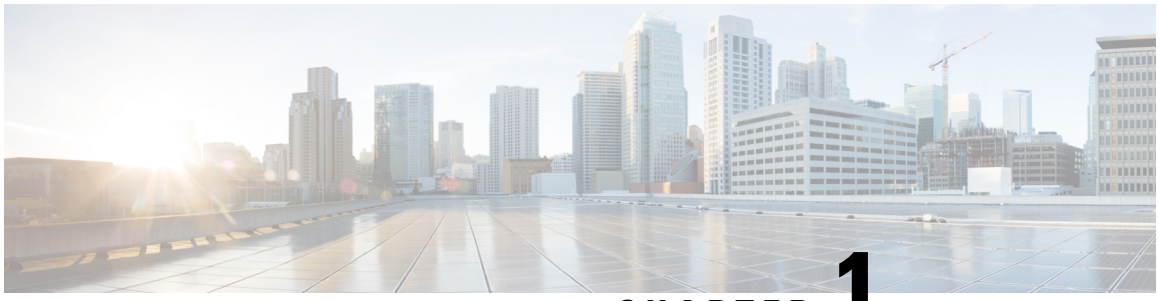
Cisco NCS 2000 Series SVO Configuration Guide, Release 12.3.x

First Published: 2022-02-02

Last Modified: 2023-09-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco SVO Setup and Installation

Table 1: Feature History

Feature Name	Release Information	Feature Description
Cisco SVO Installation	Cisco NCS 2000 Release 12.3	The following installation methods are introduced to ease SVO installation: • **The `svoTools-12.3.sh` script is introduced to simplify system deployment in the server. You can use the script to install, uninstall, extract, and load the SVO images.** • IPv4 Port Forwarding allows to save one IPv4 address of the management network for each running Admin Plane. When Port Forwarding is enabled, Admin Plane can share the same IPv4 address assigned to the host NIC. • Standalone configuration enables you to install the SVO instances in standalone mode for lab and development usage.

Feature Name	Release Information	Feature Description
Layer 3 Management Network Connectivity through BGP	Cisco NCS 2000 Release 12.3.1	Management interconnection for servers or VMs in different locations is now supported at Layer 3 through the Border Gateway Protocol (BGP). This simplifies the management of the Admin Plane servers by using core routers, which use the BGP applications in the VMs to route to the correct SVO instances. This approach allows you to configure the same management subnet for the SVO instances and different management subnets for distributed servers or VMs. Unlike in L2, which uses multiple protocols, the L3 management network needs only the BGP protocol to improve the performance of the network.

Overview

Cisco NCS 2000 Shelf Virtualization Orchestrator (SVO) supports different modes of deployment in the optical network. This chapter provides information related to the installation and configuration of the SVO software application on external servers or virtual machines (VMs).

SVO is a Docker-based application that leverages a complex networking configuration. The SVO application supports both IPv4 and IPv6 scenarios through different Docker networks created during the installation. The extreme flexibility of the SVO software solution and its network architecture allows satisfying any requirement with proper configuration.

IPv4 Port Forwarding

IPv4 port forwarding allows saving one IPv4 address of the management network for each running admin plane (two IPv4 addresses in a high availability setup). The admin plane application shares the same IPv4 address assigned to the host NIC.

Note IPv4 port forwarding can be used in the server only.

Use the **svoTools-12.3.1.sh** script described in Install SVO in the External Server Using the Installation Script, on page 23 to enable IPv4 Port Forwarding.

Note When preparing the network configuration YAML file, the same IPv4 address must be assigned to the `adminplane` and `host-nic` fields in the management IPv4 section.

For information on how to create the network YAML configuration file, see Network Configuration File, on page 13.

Layer 3 Management Interconnection for Geo Redundancy

Layer 3 management interconnection between servers for Geo redundancy allows you to avoid stretching the Layer 2 subnet between the two locations where the servers are installed.

Layer 3 management interconnection solution is based on the Border Gateway Protocol (BGP). Servers or VMs in different locations establish a BGP neighbor relationship with a core router. The SVO Admin Plane in the servers or VMs advertises the routes that are related to itself and each SVO instance running in Active mode to the core router.

Layer 3 management interconnection is implemented with goBGP 3.0.0. goBGP is an Open Source BGP implementation that can be downloaded from https://github.com/osrg/gobgp. We recommend goBGP 3.0.0 for better compatibility.

goBGP is available as an archive file. It includes a daemon and a client. After you download and extract the files in the local device, it is necessary to create a configuration file. The following examples show the configuration files for IPv4 setup and IPv4/IPv6 setup.

gobgp_ipv4.yml

```
global:
  config:
    as: 65001
    router-id: "192.168.85.2"
neighbors:
- config:
    peer-as: 65001
    neighbor-address: "192.168.85.1"
    auth-password: "cisco"
```

gobgp_ipv4_ipv6.yml

```
global:
  config:
```

```
    as: 65001
    router-id: "192.168.85.2"
neighbors:
- config:
    peer-as: 65001
    neighbor-address: "fd00::192:168:85:1"
    auth-password: "cisco"
- config:
    peer-as: 65001
    neighbor-address: "192.168.85.1"
    auth-password: "cisco"
```

Note The field **auth-password** is optional, remove it if authentication is not a requirement.

When the configuration file is ready, you can execute the goBGP daemon with administrative privileges via command line (or configuring it as a service).

Use the following command for executing the **gobgp_ipv4.yml** file:

```
[gacrux@arturo-vm3 gobgp]$ sudo ./gobgpd -t yaml -f ./gobgp_ipv4.yml
```

Use the following command for executing the **gobgp_ipv4_ipv6.yml** file:

```
[gacrux@arturo-vm3 gobgp]$ sudo ./gobgpd -t yaml -f ./gobgp_ipv4_ipv6.yml
```

To connect to the SVO Installation Tool remotely, its route must be manually advertised with the goBGP client. This operation must be done on the local and remote servers using the following commands. The example commands contain the details of the local machine that must be substituted for the following custom configuration and the next-hop addresses:

- IP address of Admin Plane / SVO Installation Tool
- IP address of the server management network

Example

```
[gacrux@VM1]$ sudo./gobgp global rib -a ipv4 add 10.58.253.2/32 nexthop 192.168.85.2
[gacrux@VM2]$ sudo./gobgp global rib -a ipv4 add 10.58.253.3/32 nexthop 172.16.16.2
```

For information on how to create the network YAML configuration file, see Network Configuration File, on page 13. Refer to Deployment of Servers in Different Locations (L3 Interconnection), on page 29 for details about SVO software application running with Layer 3 management interconnection and Use Case 3 - Dislocated Servers (L3 Interconnection), on page 34 for use case example.

Using svoTools.sh Script

Use the **svoTools-12.3.1.sh** script described in Install SVO in the External Server Using the Installation Script to enable Layer 3 Management Interconnection.

Running goBGP Daemon as a Service

After you download, extract the files, and create the configuration file as described in the previous section, you can configure the goBGP Daemon as a service.

Create the service file with the following content (substitute the highlighted parts with the correct path where you extracted gobgpd and with the path of the configuration file):

```
[gacrux@arturo-vm3 ~]$ cat /usr/lib/systemd/system/gobgpd.service
[Unit]
```

```
Description=goBGP 3.0 server daemon
Documentation=www.gobgp.com
After=network.target

[Service]
Type=exec
ExecStart=/home/gacrux/gobgp-3.0/gobgpd -t yaml -f /home/gacrux/gobgp-3.0/gobgp_ipv4.yml
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartSec=2s

[Install]
WantedBy=multi-user.target
```

Enable the Service

To enable the service, use the following command:

```
[gacrux@arturo-vm3 ~]$ sudo systemctl enable gobgpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/gobgpd.service to
/usr/lib/systemd/system/gobgpd.service.
[gacrux@arturo-vm3 ~]$
```

Start the Service

To start the service, use the following command:

```
[gacrux@arturo-vm3 ~]$ sudo systemctl start gobgpd.service
```

Check the Status of the Service

To check the status of the service, use the following command:

```
[gacrux@arturo-vm3 ~]$ sudo systemctl status gobgpd.service
● gobgpd.service - goBGP 3.0 server daemon
   Loaded: loaded (/usr/lib/systemd/system/gobgpd.service; enabled; vendor preset: disabled)

   Active: active (running) since Fri 2022-03-18 16:32:01 CET; 8s ago
 Main PID: 28139 (gobgpd)
    Tasks: 10
   Memory: 8.5M
   CGroup: /system.slice/gobgpd.service
           └─28139 /home/gacrux/LG/gobgp-3.0/gobgpd -t yaml -f
/home/gacrux/LG/gobgp-3.0/gobgp_ipv4.yml

Mar 18 16:32:01 arturo-vm3 systemd[1]: Started goBGP 3.0 server daemon.
Mar 18 16:32:01 arturo-vm3 gobgpd[28139]: {"level":"info","msg":"gobgpd
started","time":"2022-03-18T16:32:01+01:00"}
Mar 18 16:32:01 arturo-vm3 gobgpd[28139]: {"Topic":"Config","level":"info","msg":"Finished
 reading the config file","time":"2022-03-18T16:32:01+01:00"}
Mar 18 16:32:01 arturo-vm3 gobgpd[28139]:
{"Key":"192.168.85.1","Topic":"config","level":"info","msg":"Add
Peer","time":"2022-03-18T16:32:01+01:00"}
Mar 18 16:32:01 arturo-vm3 gobgpd[28139]:
{"Key":"192.168.85.1","Topic":"Peer","level":"info","msg":"Add a peer
configuration","time":"2022-03-18T16:32:01+01:00"}
Mar 18 16:32:06 arturo-vm3 gobgpd[28139]:
{"Key":"192.168.85.1","State":"BGP_FSM_OPENCONFIRM","Topic":"Peer","level":"info","msg":"Peer
 Up","time":"2022-03-18T16:32:06+01:00"}
[gacrux@arturo-vm3 ~]$
```

Stop the Service

To stop the service, use the following command:

```
[gacrux@arturo-vm3 ~]$ sudo systemctl stop gobgpd.service
```

Disable the Service

To disable the service, use the following command:

```
[gacrux@arturo-vm3 ~]$ sudo systemctl disable gobgpd.service
```

Recommended Hardware

The hardware recommendation is based on the Cisco UCS configuration with the VMWare ESXi-7.0U1c.

Note In VMWare ESXi, configure the Security Policy of virtual switches as follow:

```
Allow promiscuous mode: yes
Allow forged transmits: yes
Allow MAC changes: yes
```

- Cisco UCS-C220-M5SX
- 32 CPUs (2x Intel Xeon Gold 5218 CPU @ 2.30GHz)
- 256GB RAM
- 2x 480GB SSD (Raid)
- MLOM NIC for additional network interfaces

Recommended Software

Table 2: Feature History

Feature Name	Release Information	Feature Description
Support for Hosting SVO Server on Red Hat Enterprise Linux	Cisco NCS 2000 Release 12.3	This feature allows you to host SVO on an external server running Red Hat Enterprise Linux 7.9.

The following are the recommended OS versions.

- CentOS Linux release 7.9.2009 (Docker Engine 20.10.9)
- Red Hat Enterprise Linux 7.9 (Docker Engine 20.10.9)

Recommended Resource for Virtual Machines

The following sections provide information on the resources that are required to define SVO instances.

In case of high availability, it is recommended to have the same resources on both the VMs.

Release 12.3.1

Release 12.3.1 introduces effective resource management, which has a significant impact on resource optimization. As a reference of load, a VM created on a UCS server with 64 virtual CPUs, 240 GB RAM and 400 GB of available disk space, can accommodate admin plane and 90 SVO instances (the verification is done with 60 percent of ROADM instances and 40 percent of OLA instances).

- **CPU**

  Seven virtual CPUs for 10 SVO instances (including admin plane)

- **Memory**
  - 2 GB for admin plane
  - 2.1 GB for each node, irrespective of the SVO type such as ROADM and OLA

Note We recommend you to use 80 percent of the total available memory of the server or VM to create SVO instances, and use the remaining 20 percent as shared resources to accommodate memory peaks during heavy operations.

- **Disk Space**

  2.5 GB for each SVO instance

Note SVO application stores data in the root (/) filesystem (`/var` and `/misc` folders). It is in charge of the administration of the server/VM to apply the proper partition (advanced disk options during installation).

Release 12.3 and Earlier

- **CPU**
  - One virtual CPU for each ROADM node
  - One virtual CPU for every three OLA, DGE, or TXP nodes
- **Memory**
  - 2 GB for admin plane
  - 3 GB for each OLA, DGE, TXP, or ROADM with 2, 3 or 4 degrees
  - 4 GB for each ROADM with 5, 6, 7 or 8 degrees

- 8 GB for each ROADM with more than 8 degrees

- **Disk Space**

  5 GB for each SVO instance

Required Network Resources

Network resources that must be planned in the design phase are related to three different subnets.

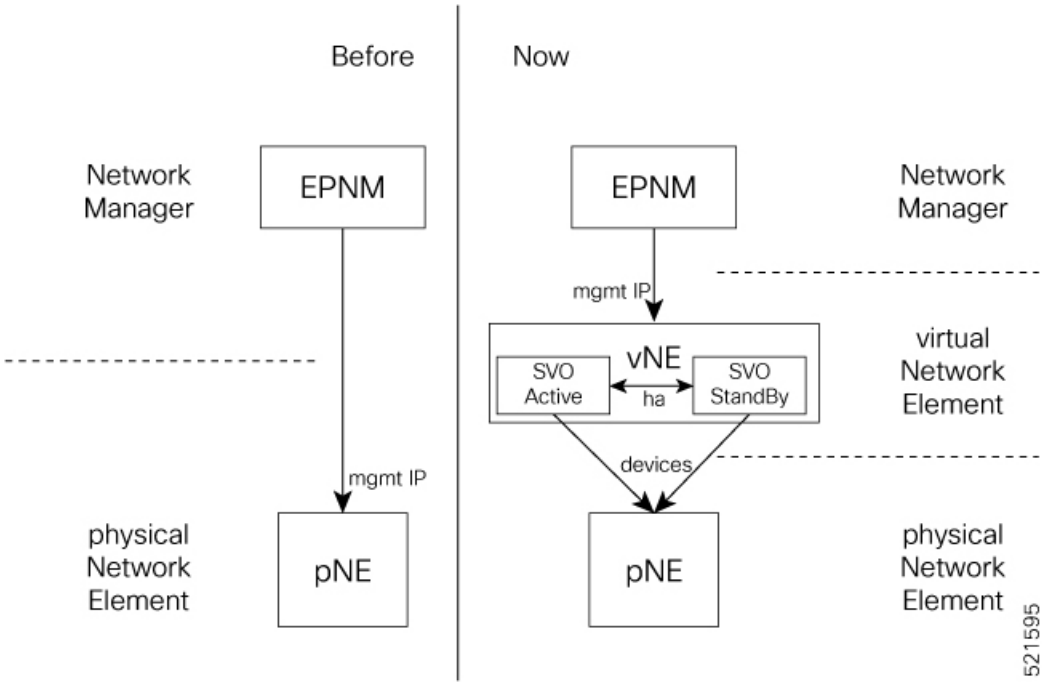
The following table describes the different networks.

Table 3: Network Type

Network	Network Type	Description
mgmt	Management network	Offers Netconf NBI and Web UIs for admin plane and SVO instances (used by users)
ha	High availability network	For data replication **Note** Used only between two servers or VMs
devices	Network to reach NCS 2000 devices	Communicate with NCS 2000 devices **Note** Used only between the servers or VMs and the NCS 2000 devices

The following figure illustrates the management of an NE before and after the introduction of SVO.

Figure 1: Network Element Before and After SVO



Note For each virtual NE, represented by a SVO instance, there is a single management IP address. The status of the management interface, Up or Down, is aligned with the status of the SVO, active or standby.

If SVO is active, the management interface is Up. If SVO is standby, the management interface is Down.

The status, active or standby, is orchestrated by admin plane.

In the following table, the data to define the size of the subnets to set up HA network and the description of each network and its usage.

Network	No. of IP Addresses	Description
management	One for each gateway Two for each host NIC Two for each admin plane One for each SVO instance	Must be the same subnet on both the servers or VMs. On this subnet, SVO software application offers Netconf NBI and Web UIs. When used from the customer DCN, this network becomes visible and routable in the customer DCN. Admin planes work in active/active status, that is, on each server or VM, when an admin plane is running, it is possible to connect to the Web UI through the management IP address (https://*mgmt-ip*). Each SVO instance works in active/standby status. The instances share the same management IP address. **Note** The network interface is Down on the standby side.

Network	No. of IP Addresses	Description
HA	One for each gateway Two for each host NIC Two for each admin plane Two for each SVO instance	In release 12.1, HA network must have the same subnet on both the servers or VMs. From release 12.2, HA network can have different and routable subnets. Allows data replication between active and standby SVO instances. It is the primary communication channel between admin planes.
Devices	One for each gateway Two for each host NIC Two for each admin plane Two for each SVO instance	In release 12.1, Devices network must have the same subnet on both the servers and the VMs. From release 12.2, the subnets can be different. Devices shall be routable towards NCS 2000 network. Used by SVO instances to communicate with NCS 2000 devices. It is the secondary communication channel between admin planes.

Bandwidth and Latency Requirements

The bandwidth required for the high availability (HA) networks ranges from 255 to 977 Mbps, depending on the workload of the server.

The latency requirements are:

- EPNM from and to SVO is < 80 ms
- SVO servers from and to NCS 2000 devices is < 80 ms
- SVO servers high availability is < 100 ms

Install Docker Engine

Use this task to install the docker engine.

Note During the installation on RHEL, the following error message could be generated during the execution of the command `sudo yum install docker-ce-<version> ...`:

```
**************************************************************************
yum can be configured to try to resolve such errors by temporarily enabling
disabled repos and searching for missing dependencies.
To enable this functionality please set 'notify_only=0' in
/etc/yum/pluginconf.d/search-disabled-repos.conf
**************************************************************************
```

Edit the file `/etc/yum/pluginconf.d/search-disabled-repos.conf` and set **notify_only=0**, then execute again the command.

Procedure

Step 1 Check repositories for available package updates.

```
[gacrux@arturo-vm3 ~]$ sudo yum check-update
Loaded plugins: fastestmirror
Determining fastest mirrors
 * base: ams.edge.kernel.org
 * extras: ams.edge.kernel.org
 * updates: ams.edge.kernel.org
...
```

Step 2 Install the required dependencies from the Docker repositories.

```
[gacrux@arturo-vm3 ~]$ sudo yum install -y yum-utils device-mapper-persistent-data lvm2
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ams.edge.kernel.org
 * extras: ams.edge.kernel.org
 * updates: ams.edge.kernel.org
Resolving Dependencies
--> Running transaction check
---> Package device-mapper-persistent-data.x86_64 0:0.8.5-3.el7 will be updated
---> Package device-mapper-persistent-data.x86_64 0:0.8.5-3.el7_9.2 will be an update
---> Package lvm2.x86_64 7:2.02.187-6.el7 will be updated
...
Installed:
  yum-utils.noarch 0:1.1.31-54.el7_8


Dependency Installed:
  libxml2-python.x86_64 0:2.9.1-6.el7.5      python-chardet.noarch 0:2.2.1-3.el7
python-kitchen.noarch 0:1.1.1-5.el7

Updated:
  device-mapper-persistent-data.x86_64 0:0.8.5-3.el7_9.2                    lvm2.x86_64
7:2.02.187-6.el7_9.3

Dependency Updated:
  device-mapper.x86_64 7:1.02.170-6.el7_9.3                    device-mapper-event.x86_64
 7:1.02.170-6.el7_9.3
  device-mapper-event-libs.x86_64 7:1.02.170-6.el7_9.3           device-mapper-libs.x86_64
 7:1.02.170-6.el7_9.3
  lvm2-libs.x86_64 7:2.02.187-6.el7_9.3
```

```
Complete!
```

Step 3 Set up the Docker repository.

```
[gacrux@arturo-vm3 ~]$ sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
Loaded plugins: fastestmirror
adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
grabbing file https://download.docker.com/linux/centos/docker-ce.repo to
/etc/yum.repos.d/docker-ce.repo
repo saved to /etc/yum.repos.d/docker-ce.repo
```

Step 4 Install the 20.10.9 version of Docker engine and containerd.

```
[gacrux@arturo-vm3 ~]$ sudo yum install docker-ce-20.10.9 docker-ce-cli-20.10.9 containerd.io
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
Resolving Dependencies
--> Running transaction check
---> Package containerd.io.x86_64 0:1.4.10-3.1.el7 will be installed
--> Processing Dependency: container-selinux >= 2:2.74 for package:
containerd.io-1.4.10-3.1.el7.x86_64
---> Package docker-ce.x86_64 3:20.10.9-3.el7 will be installed
...
Installed:
  containerd.io.x86_64 0:1.4.10-3.1.el7                docker-ce.x86_64 3:20.10.9-3.el7
              docker-ce-cli.x86_64 1:20.10.9-3.el7

Dependency Installed:
  container-selinux.noarch 2:2.119.2-1.911c772.el7_8      docker-ce-rootless-extras.x86_64
 0:20.10.9-3.el7       docker-scan-plugin.x86_64 0:0.8.0-3.el7
  fuse-overlayfs.x86_64 0:0.7.2-6.el7_8                    fuse3-libs.x86_64 0:3.6.1-4.el7
                        slirp4netns.x86_64 0:0.4.3-4.el7_8

Complete!
```

Step 5 Start the Docker engine.

```
[gacrux@arturo-vm3 ~]$ systemctl start docker
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to manage system services or units.
Authenticating as: gacrux
Password:
==== AUTHENTICATION COMPLETE ===
```

Step 6 Enable the Docker engine.

```
[gacrux@arturo-vm3 ~]$ systemctl enable docker
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: gacrux
Password:
==== AUTHENTICATION COMPLETE ===
Created symlink from /etc/systemd/system/multi-user.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: gacrux
Password:
==== AUTHENTICATION COMPLETE ===
```

Step 7 Add the user to the Docker group.

```
[gacrux@arturo-vm3 ~]$ sudo usermod -aG docker $USER
```

Step 8 Exit the command line.

```
[gacrux@arturo-vm3 ~]$ exit
```

Step 9 Disconnect and reconnect to refresh user permissions.

Network Configuration File

Network configuration file defines all the information that is related to the servers and the networking infrastructure that is required to set up the SVO functionalities. See Required Network Resources section to define the networks.

The *network.yml* configuration file starts with the **server-name** field. The **server-name** field refers to the **name** field of the server in which the installation executes.

The configuration files that are used for the installation in high availability networks on two servers or VMs contain different values in the **server-name** field for the respective servers.

The *network.yml* configuration file contains two main sections, one for each server or VM of the cluster.

For each server section, there are three fields:

- name—Server name (editable)
- mgmt-port—Not editable (value is 443)
- ha-agent-port—Not editable (value is 5480)

SVO network architecture is based on four networks. Each section in a *network.yml* file defines the following networks:

- **Management**—The management ports of the admin plane and SVO instances belong to this network.
- **High Availability**—This network is used for SVO database replication and communication between the admin planes.
- **Private HA Network**—This network is used only for communicating between the admin plane and the local SVO instances in certain processes such as node activation. It doesn't use external networking resources.
- **Devices**—This network is used for connecting the NCS 2000 devices. The devices must be reachable through this subnet. If the admin plane is unable to communicate with its peer server on the primary high availability network, it uses a link on this network as an alternative way to communicate.

The **Private HA Network** is local to the server or VM. The other three networks are exposed outwards and they must have three different subnets.

Note Ensure that IP addresses from the *172.16.xx.xx/16* subnet are not specified in *.yml* files as this subnet is reserved for Docker's internal use.

The following table describes the fields in the *network.yml* configuration files.

Field	Value	Editable	Description
server-name	—	Yes	Name of the server to which the file is applied.
mgmt-address-family	IPv4 IPv4_IPv6 IPv6	Yes	IP address family of the management network.
name	management hanetwork haprivate devices	No	Name of the network
mgmt-port	443	No	Port that is used for admin plane web UI
ha-agent-port	5480	No	Port that is used for internal communication between the admin plane and SVO
host-nic-name	—	Yes	(Optional) Interface that is used in docker network **Note** Only in **management**, **hanetwork**, and **devices**
ha-port	10001 10002	Yes	Port used for admin plane high-availability on the specific network (primary path) **Note** Only in **HA** and **Devices.**
IPv4			
ip	—	Yes	Subnet
prefix	—	Yes	Mask
gateway	—	Yes	Gateway
host-nic	—	Yes	(Optional) IPv4 address that is assigned to the host interface **Note** Only in **management**, **hanetwork**, and **devices**
adminplane	—	Yes	IPv4 address that is assigned to the admin plane
IPv6: (Optional)			
ip	—	Yes	Subnet
prefix	—	Yes	Mask
gateway	—	Yes	Gateway
host-nic	—	Yes	(Optional) IPv6 address that is assigned to the host interface **Note** Only in **management**, **hanetwork**, and **devices**

Field	Value	Editable	Description
adminplane	—	Yes	IPv6 address that is assigned to the admin plane

The following sections contain one example of *network.yml* file for IPv4 configuration and one for IPv6 configuration.

To create the configuration file, use one of the following templates.

IPv4 Network YAML Configuration File Sample

```
server-name: VM1

servers:
  - name: VM1
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens192
      ipv4:
        ip: 10.58.233.0
        prefix: 24
        gateway: 10.58.233.1
        host-nic: 10.58.233.75
        adminplane: 10.58.233.76
    ha:
      name: hanetwork
      host-nic-name: ens224
      ha-port: 10001
      ipv4:
        ip: 192.168.1.0
        prefix: 24
        gateway: 192.168.1.1
        adminplane: 192.168.1.4
        host-nic: 192.168.1.2
    haprivate:
      name: haprivate
      ipv4:
        ip: 192.168.3.0
        prefix: 24
        gateway: 192.168.3.1
        adminplane: 192.168.3.2
    devices:
      name: devices
      host-nic-name: ens256
      ha-port: 10002
      ipv4:
        ip: 192.168.2.0
        prefix: 24
        gateway: 192.168.2.1
        adminplane: 192.168.2.4
        host-nic: 192.168.2.2

  - name: VM2
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens192
      ipv4:
```

```
    ip: 10.58.233.0
    prefix: 24
    gateway: 10.58.233.1
    host-nic: 10.58.233.77
    adminplane: 10.58.233.78
ha:
  name: hanetwork
  host-nic-name: ens224
  ha-port: 10001
  ipv4:
    ip: 192.168.1.0
    prefix: 24
    gateway: 192.168.1.1
    adminplane: 192.168.1.5
    host-nic: 192.168.1.3
haprivate:
  name: haprivate
  ipv4:
    ip: 192.168.3.0
    prefix: 24
    gateway: 192.168.3.1
    adminplane: 192.168.3.2
devices:
  name: devices
  host-nic-name: ens256
  ha-port: 10002
  ipv4:
    ip: 192.168.2.0
    prefix: 24
    gateway: 192.168.2.1
    adminplane: 192.168.2.5
    host-nic: 192.168.2.3
```

IPv6 Network YAML Configuration File Sample

Networking infrastructure requires all the *network.yml* files with IPv6 section to have an IPv4 section.

In the following example, the IPv6 section has been configured for the three networks: management, high availability, and devices.

It is not mandatory that all networks must be configured in IPv6. Each network is independent of others.

Table 4: Network Types

Network Types	Description
Management	**Dual stack (IPv4+IPv6)**—User wants to use both IPv4 and IPv6 addresses. It is required that the same IPv4 subnet is used between the two servers **IPv6 only**—User wants to use only IPv6 addresses. Use different private IPv4 subnets between the two servers, to avoid any conflict In both scenarios, the IPv4 information are required by the networking infrastructure.

Network Types	Description
High availability and devices	When IPv6 information are available, IPv4 information are not used directly by the SVO application but are anyway required by the networking infrastructure. The suggestion is to use different private IPv4 subnets between the two servers, to avoid any conflict.
Private HA Network	It is a local network. You must use the IPv4 information as required by the networking infrastructure. There is no reason to add IPv6 section.

```
server-name: VM1

servers:
  - name: VM1
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens192
      ipv4:
        ip: 10.58.233.0
        prefix: 24
        gateway: 10.58.233.1
        adminplane: 10.58.233.72
      ipv6:
        ip: 2001:420:4491:2004::233:0
        prefix: 112
        gateway: 2001:420:4491:2004::233:2
        host-nic: 2001:420:4491:2004::233:70
        adminplane: 2001:420:4491:2004::233:72
    ha:
      name: hanetwork
      host-nic-name: ens224
      ha-port: 10001
      ipv4:
        ip: 192.168.80.0
        prefix: 24
        gateway: 192.168.80.1
        adminplane: 192.168.80.2
      ipv6:
        ip: 2001:db8:abc:111::0
        prefix: 64
        gateway: 2001:db8:abc:111::1
        adminplane: 2001:db8:abc:111::4
        host-nic: 2001:db8:abc:111::2
    haprivate:
      name: haprivate
      ipv4:
        ip: 192.168.3.0
        prefix: 24
        gateway: 192.168.3.1
        adminplane: 192.168.3.2
    devices:
      name: devices
      host-nic-name: ens256
      ha-port: 10002
      ipv4:
```

```
      ip: 192.168.81.0
      prefix: 24
      gateway: 192.168.81.1
      adminplane: 192.168.81.2
    ipv6:
      ip: 2001:db8:abc:222::0
      prefix: 64
      gateway: 2001:db8:abc:222::1
      adminplane: 2001:db8:abc:222::4
      host-nic: 2001:db8:abc:222::2

- name: VM2
  mgmt-port: 443
  ha-agent-port: 5480
  mgmt:
    name: management
    host-nic-name: ens192
    ipv4:
      ip: 10.58.233.0
      prefix: 24
      gateway: 10.58.233.1
      adminplane: 10.58.233.73
    ipv6:
      ip: 2001:420:4491:2004::233:0
      prefix: 112
      gateway: 2001:420:4491:2004::233:2
      host-nic: 2001:420:4491:2004::233:71
      adminplane: 2001:420:4491:2004::233:73
  ha:
    name: hanetwork
    host-nic-name: ens224
    ha-port: 10001
    ipv4:
      ip: 192.168.83.0
      prefix: 24
      gateway: 192.168.83.1
      adminplane: 192.168.83.3
    ipv6:
      ip: 2001:db8:abc:111::0
      prefix: 64
      gateway: 2001:db8:abc:111::1
      adminplane: 2001:db8:abc:111::5
      host-nic: 2001:db8:abc:111::3
  haprivate:
    name: haprivate
    ipv4:
      ip: 192.168.3.0
      prefix: 24
      gateway: 192.168.3.1
      adminplane: 192.168.3.3
  devices:
    name: devices
    host-nic-name: ens256
    ha-port: 10002
    ipv4:
      ip: 192.168.84.0
      prefix: 24
      gateway: 192.168.84.1
      adminplane: 192.168.84.3
    ipv6:
      ip: 2001:db8:abc:222::0
      prefix: 64
      gateway: 2001:db8:abc:222::1
```

```
        adminplane: 2001:db8:abc:222::5
        host-nic: 2001:db8:abc:222::3
```

IPv4 Port Forwarding Network YAML Configuration

```
...

servers:
  - name: VM1
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens192
      ipv4:
        ip: 10.58.233.0
        prefix: 24
        gateway: 10.58.233.1
        host-nic: 10.58.233.75
        adminplane: 10.58.233.75
    ha:
      name: hanetwork
      host-nic-name: ens224
      ha-port: 10001
      ipv4:
        ip: 192.168.1.0
        prefix: 24
        gateway: 192.168.1.1
        host-nic: 192.168.1.2
        adminplane: 192.168.1.4

    ...
```

L3 Management Interconnection Network YAML Configuration

Layer 3 management interconnection between servers simplifies Geo redundancy deployment.

Note A new field is added in the *network.yml* file to configure the management interconnection at Layer 3. The following field is an optional field with the default value set as **LAYER2**.

```
mgmt-interconnection: LAYER3
```

The following *network.yml* file contains the IP addresses used in the Use Case 3 - Dislocated Servers (L3 Interconnection), on page 34 section.

```
server-name: VM1
mgmt-address-family: IPv4_IPv6
mgmt-interconnection: LAYER3
servers:
  - name: VM1
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens161
      ipv4:
        ip: 10.58.253.0
        prefix: 27
        gateway: 10.58.253.1
        host-nic: 192.168.85.2
```

```
      adminplane: 10.58.253.2
    ipv6:
      ip: 2000::10:58:253:0
      prefix: 123
      gateway: 2000::10:58:253:1
      host-nic: fd00::192:168:85:2
      adminplane: 2000::10:58:253:2
  ha:
    name: hanetwork
    host-nic-name: ens224
    ha-port: 10001
    ipv4:
      ip: 192.168.85.32
      prefix: 27
      gateway: 192.168.85.33
      host-nic: 192.168.85.34
      adminplane: 192.168.85.35
    ipv6:
      ip: fd00::192:168:85:20
      prefix: 123
      gateway: fd00::192:168:85:21
      host-nic: fd00::192:168:85:22
      adminplane: fd00::192:168:85:23
  haprivate:
    name: haprivate
    ipv4:
      ip: 192.168.85.96
      prefix: 27
      gateway: 192.168.85.97
      adminplane: 192.168.85.98
  devices:
    name: devices
    host-nic-name: ens256
    ha-port: 10002
    ipv4:
      ip: 192.168.85.64
      prefix: 27
      gateway: 192.168.85.65
      host-nic: 192.168.85.66
      adminplane: 192.168.85.67
    ipv6:
      ip: fd00::192:168:85:40
      prefix: 123
      gateway: fd00::192:168:85:41
      host-nic: fd00::192:168:85:42
      adminplane: fd00::192:168:85:43

- name: VM2
  mgmt-port: 443
  ha-agent-port: 5480
  mgmt:
    name: management
    host-nic-name: ens161
    ipv4:
      ip: 10.58.253.0
      prefix: 27
      gateway: 10.58.253.1
      host-nic: 172.16.16.2
      adminplane: 10.58.253.3
    ipv6:
      ip: 2000::10:58:253:0
      prefix: 123
      gateway: 2000::10:58:253:1
      host-nic: fd00::172:16:16:2
```

```
    adminplane: 2000::10:58:253:3
ha:
  name: hanetwork
  host-nic-name: ens224
  ha-port: 10001
  ipv4:
    ip: 172.16.16.32
    prefix: 27
    gateway: 172.16.16.33
    host-nic: 172.16.16.34
    adminplane: 172.16.16.35
  ipv6:
    ip: fd00::172:16:16:20
    prefix: 123
    gateway: fd00::172:16:16:21
    host-nic: fd00::172:16:16:22
    adminplane: fd00::172:16:16:23
haprivate:
  name: haprivate
  ipv4:
    ip: 172.16.16.96
    prefix: 27
    gateway: 172.16.16.97
    adminplane: 172.16.16.98
devices:
  name: devices
  host-nic-name: ens256
  ha-port: 10002
  ipv4:
    ip: 172.16.16.64
    prefix: 27
    gateway: 172.16.16.65
    host-nic: 172.16.16.66
    adminplane: 172.16.16.67
  ipv6:
    ip: fd00::172:16:16:40
    prefix: 123
    gateway: fd00::172:16:16:41
    host-nic: fd00::172:16:16:42
    adminplane: fd00::172:16:16:43
```

Prepare the Network Configuration

Use this task to prepare the network configuration for the external server model or the SVO card model.

Before you begin

See Network Configuration File, on page 13.

Procedure

Step 1 Create a configuration file (*network.yml)* for each server with the networking configuration data. This file is uploaded during the installation.

Step 2 Cable and configure the related network interfaces (physical or virtual).

Both the configuration files are identical and contain the data for both the servers in HA. The only difference is the *server-name* attribute that contains the name of the server to which the file is applied.

Standalone SVO Configuration

From Release 12.3, you can configure and install SVO in Standalone mode. Independent of IPv4 or IPv6 configuration, the network YAML file contains information of a single server, instead of the local and remote instances.

Limitation of Standalone Mode

An SVO installed in Standalone mode cannot be upgraded to high availability. The SVO application must be re-installed with a standard network YAML file containing the information of both servers.

Installation of SVO

The SVO application can be installed in the following setups:

- Install SVO Card, on page 22
- Install the External Server, on page 23

The SVO software installation for the external server can be separated in different steps:

- Creation of the VM and resource allocation
- Installation of OS and Docker packages
- Installation of SVO software

VM Creation and Resource Allocation

Create a VM allocating the proper resources, in terms of CPU, memory and disk space.

Installation of OS and Docker packages

Installation steps described in the following sections refer to CentOS 7.9.2009 and RHEL 7.9.

Install SVO Card

Note The SVO card model comes pre-installed with the required software packages. You need to power up the card and start the configuration.

Use this task to install the SVO application using the SVO card.

Before you begin

Ensure following recommendations are met:

- Recommended Hardware, on page 6
- Recommended Software, on page 6
- Recommended Resource for Virtual Machines, on page 7
- Required Network Resources, on page 8

Procedure

Step 1 Power up the SVO card.

Step 2 Run the SVO installation tool. See Bring Up Admin Plane with the SVO Installation Tool, on page 26.

Install the External Server

Before you begin installing the SVO application using the installation script or manual installation, ensure the following recommendations are met.

- Recommended Hardware, on page 6
- Recommended Software, on page 6
- Recommended Resource for Virtual Machines, on page 7
- Required Network Resources, on page 8
- Install Docker Engine, on page 10

You can install the SVO application in the following methods:

- Install SVO in the External Server Using the Installation Script, on page 23

  This method enables you to install the SVO application using the **svoTools-12.3.1.sh** script. When you install the SVO application using the installation script, you can skip the manual installation procedure.

- Install SVO in the External Server Manually, on page 25

  This method enables you to install the SVO application using the CLI commands and docker images.

Install SVO in the External Server Using the Installation Script

The **svoTools-12.3.1.sh** script enables automatic installation of the SVO application in the server for Release 12.3.1. You need not use the Docker engine to install the SVO application. The script is available for download within **svo-utilities-12.3.0.tar** file that is located in the Utilities folder of SVO Release 12.3.1 at the Cisco Software Downloads page. The tar archive file contains the related signed RPM with instructions to extract the actual script file. This utility script simplifies the following operations:

1. Extracts and loads SVO images
2. Brings up and starts SVO installation tool

3. Uninstalls SVO

Note **svoTools-12.3.1.sh** script can be used to install the SVO application in the server only.

Note If any compatibility issue arises between the selected operating system and the script, manually install the SVO application.

Note If the management network configuration is **IPv4/IPv6** or **IPv6-only**, the **svoTools-12.3.1.sh** script requires subnet, mask, and gateway for both the stacks.

The difference between the **IPv4/IPv6** and **IPv6-only** configurations is the IPv4 information. For the IPv4/IPv6 dual stacks management network, the same public IPv4 subnet network information must be used between the two servers. For an IPv6-only management network, two different private IPv4 subnet network information must be used between the two servers.

Procedure

Run the `sudo ./svoTools-<version>.sh` command as an admin.

```
[gacrux@arturo-vm2 LG]$ sudo ./svoTools-12.3.1.sh
 ========================================================================
 ========================================================================

               SVO Tools 1.3 (compatible with SVO 12.3.1)


 Cisco Systems, Inc.                                        Copyright 2022
 ========================================================================

 Welcome to the SVO Tools

 This script simplifies the following operations:
   * Load SVO images from SW release (ncs2k-server-12.3.1_REL.tar)
   * Start SVO Installation Tool
   * Uninstall SVO

 In any moment you can abort the operation pressing CTRL-C
 ------------------------------------------------------------------------

 Enter your choice:

1) Load SVO images
2) Start SVO
3) Uninstall SVO
4) Exit
#?
```

Type the number of your choice.

Load SVO images require downloading the SVO software release from Cisco.com (as a TAR archive file) in the same folder where the script is executing.

Start SVO option allows starting the SVO Installation Tool. After selecting the **Start SVO Tool** option, see Bring Up Admin Plane with the SVO Installation Tool, on page 26 about how to connect via browser to the tool.

Uninstall SVO allows uninstalling the SVO files.

Note From Release 12.3.1, the **svoTools-12.3.1.sh** allows you to choose between **`Layer2`** and **`Layer3`** management interconnection. Select **`Layer3`** option to enable Layer 3 Management Interconnection solution when the following prompt appears:

```
Select management interconnection between servers at Layer2 or Layer3:
1) Layer2
2) Layer3
#? 2
```

Install SVO in the External Server Manually

Note If you successfully completed the SVO application installation using the Install SVO in the External Server Using the Installation Script, on page 23 procedure, you can skip the following procedure.

Use this task to install the external server.

Procedure

Step 1 Create the network configuration. See Prepare the Network Configuration, on page 21.

Step 2 Obtain the admin plane (es-admin-plane) and SVO (svo-dos) docker images. Perform these steps:

- Get the `ncs2k-server-12.1.0_REL.tar` file and extract its contents.

```
> tar xvf ncs2k-server-12.1.0_REL.tar
> cd SIGNED_RPM; ls
NCS2K-S-1210.020K.2311.x86_64.rpm
es-admin-plane-12.1.0.B0582.x86_64.rpm
svo-dos-12.1.0.R0582.x86_64.rpm
> rpm2cpio es-admin-plane-12.1.0.B0582.x86_64.rpm | cpio -D <OUTDIR> -idmv
> rpm2cpio svo-dos-12.1.0.R0582.x86_64.rpm | cpio -D <OUTDIR> -idmv
```

- Load the admin plane and SVO images.

```
docker load -i es-admin-plane.tgz
docker load -i svo-dos.tgz
```

- Verify the images using the **docker images** command.

Step 3 Create the configuration folder */misc/disk1/data/adminplane*. The folder path need to used as a parameter the next step.

Step 4 Create a text file called *installer.properties* inside the configuration folder. Add the the following line to the file.

```
server.address=<adminplane-mgmt-ip>
installer.remote-connection=true
```

The `adminplane-mgmt-ip` is the IP address that is assigned to the admin plane in the management network.

Step 5 Create a docker network using any one of the following commands:

- **IPv4**

```
docker network create -d macvlan --attachable --subnet <subnet>/<mask> --gateway <gw>
-o parent=<mgmt-interface> management
```

```
docker create --name adminplane --network management --ip <adminplane-mgmt-ip> -m 2g
--memory-swap 2g --cap-add NET_ADMIN --restart
always -v /misc/disk1/data:/misc/disk1/data -v /var/run/docker.sock:/var/run/docker.sock
 -v /misc/disk1/data/adminplane:/opt/config es-admin-plane:<version>
```

- **IPv4 and IPv6**

```
docker network create -d macvlan --attachable --subnet <subnet>/<mask> --gateway <gw>
--ipv6 --subnet <ipv6-subnet>/<prefix> --gateway <ipv6-gw> -o parent=<mgmt-interface>
management
```

```
docker create --name adminplane --network management --ip <adminplane-mgmt-ip> --ip6
<adminplane-mgmt-ipv6> -m 2g --memory-swap 2g --cap-add NET_ADMIN --restart
always -v /misc/disk1/data:/misc/disk1/data -v /var/run/docker.sock:/var/run/docker.sock
 -v /misc/disk1/data/adminplane:/opt/config es-admin-plane:<version>
```

Step 6 Start the application using the following command:

```
docker start adminplane
```

Step 7 Run the SVO installation tool. See Bring Up Admin Plane with the SVO Installation Tool, on page 26.

Bring Up Admin Plane with the SVO Installation Tool

Use this task to bring up the Admin Plane with the SVO installation tool for the external server model or the SVO card model.

Note In the SVO card model, the user created is the superuser in all the SVO instances created later.

Procedure

Step 1 Start the SVO installation tool using the IP address as follows:

- **External server model**—Use the management IP address, http://*adminplane-mgmt-ip*.
- **SVO card model**—Use the pre-defined IP address, http://192.168.0.66.

  Note The client must be connected to the SVO craft port using an ethernet cable.

Step 2 In the **Credentials** area, perform these steps:

a. Enter a username in the **Username** field.

b. Enter a password in the **Password** field.

   The password must be a minimum of eight characters, and it can be a maximum of 127 characters. The password must have at least one uppercase letter, one lowercase character, one number, and one special character.

c. Retype the password in the **Retype Password** field.

Step 3 In the **Networks** area, perform these steps:

a. Click **Browse** to select the *network.yml* configuration file **Configuration File** field.

   For more information about the configuration file (*network.yml*), see Prepare the Network Configuration, on page 21.

Step 4 Click **Submit**.

The system creates the credentials, verifies the network configuration file and brings up the system. You are now able to connect to Cisco SVO admin plane login page at *https://adminplane-mgmt-ip*. See Log into the Cisco SVO Admin Plane, on page 42.

Deployment

The SVO networking architecture offers a degree of flexibility that meets all requirements.

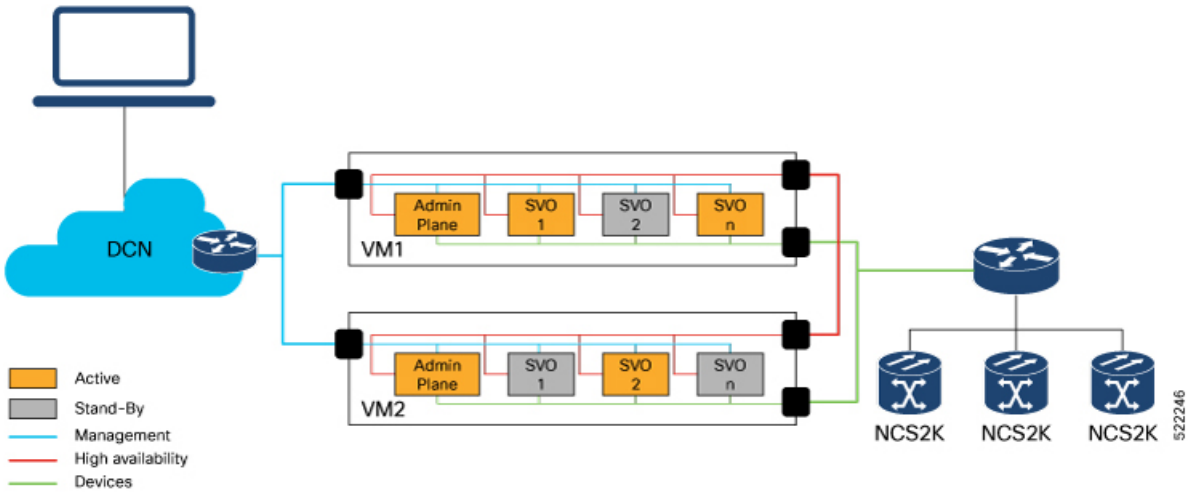
The following list describes the types of deployment:

- Deployment of Colocated Servers
- Deployment of Servers in Different Locations (L2 Interconnection)

Deployment of Colocated Servers

Deployment of the colocated servers is simple. In this deployment, both the servers or VMs share the same subnets for all three networks. The following image displays the schema of the networks and the connections.

Figure 2: Deployment of Colocated Servers



Deployment of Servers in Different Locations (L2 Interconnection)

Deployment of servers in different locations is complicated. This deployment needs more attention in the design and more checks in the existing subnet.

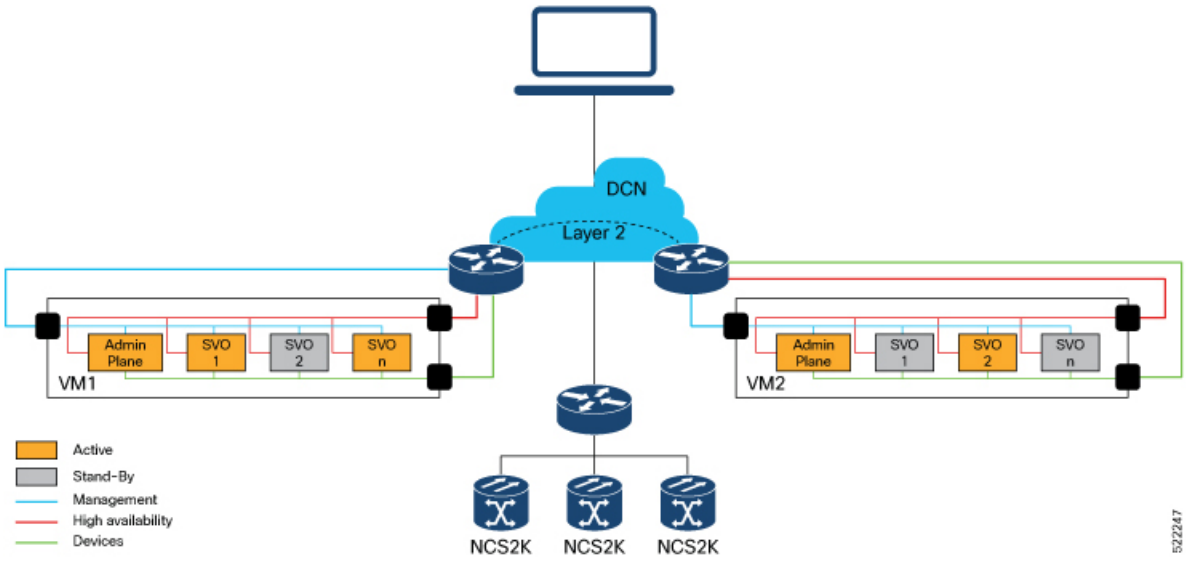
Management subnet reaches the servers in different locations. A Layer 2 connection is required for both the servers and VMs in different locations. The valid Layer 2 connections are L2VPN, L2TPv3, VXLAN, or a similar solution.

In Release 12.1, some limitations can generate more complexities for this kind of deployment. The **high availability** networks on the two servers must be in the same subnets. The same limitation impacts the **devices** networks on the two servers. Cisco recommends following the same approach that is selected for the **management** network. It is valid for both **high availability** and **devices** networks.

From Release 12.2, the high availability and devices networks can be configured in different routable subnets.

The following figure shows the schema of the networks and the connections.

Figure 3: Deployment of Servers in Different Locations



Deployment of Servers in Different Locations (L3 Interconnection)

From Release 12.3.1, deployment of servers in different locations with L3 management interconnection is supported. It enables a Layer 3 management interconnection between servers or VMs that are deployed in different locations.

A single and common **management** subnet is used only by the SVO Admin Plane. The management network interfaces of the servers or VMs have IP addresses on different subnets.

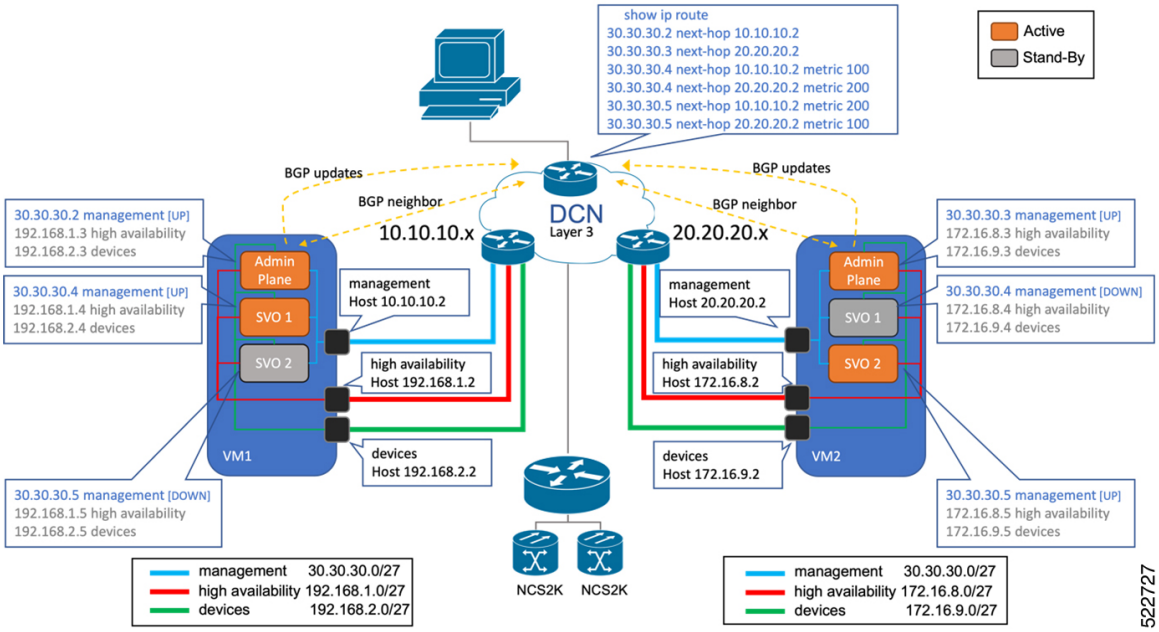
The two servers or VMs establish a BGP neighbor relationship with a core router.

SVO Admin Plane advertises the route that is related to itself and each SVO instance running in Active mode on the local server, with next-hop address pointing to the local server host management IP address.

The IP addresses of the servers are not visible to you, only the SVO management subnet is visible. In the following example, the management subnet is **30.30.30.0/27**.

The following image displays the schema of connections, BGP relationships, and networks advertisements.

Figure 4: Deployment of Servers in Different Locations (L3 Interconnection)



Admin Planes constantly monitor the BGP daemon running on each server and exchange information between themselves about the BGP neighbor relationship status. The status is displayed on the SVO Admin Plane Web UI (near the high availability bell icon) with two colored dots over a router icon.

In case of failure in the BGP neighbor relationship on one server, a switchover of all Active SVO instances is triggered toward the server where the BGP neighbor relationship is still established.

You can configure BGP communities per server through the Web UI or through the configuring file. For configuration in Web UI, refer to Modify Admin Plane Properties.

Note You can configure the BGP communities in the `adminplane.properties` file from the `/misc/disk1/data/adminplane/adminplane.properties` path. Enter a list of elements that are separated by commas as shown in the following example:

```
adminplane.bgp.advertiser.communities=100,102
```

Disaster Recovery

This section explains the analysis of what happens during a disaster, where a server or VM failed, disconnected, became unreachable or unavailable, and the details of the behavior of SVO instances connected to NCS 2000 devices.

The following lists the implementation of high availability:

- SVO instances use a **high availability** network for database synchronization.

- Admin Planes use a **high availability** network as the primary path and **devices** network as the secondary path. Admin Plane continuously monitors the connectivity between an SVO instance and the associated NCS 2000 device.

Consider there are multiple SVO instances created. Each SVO instance is associated with an NCS 2000 device. Some SVO instances are Active on one server or VM, and other SVO instances are Active on the peer server or VM.

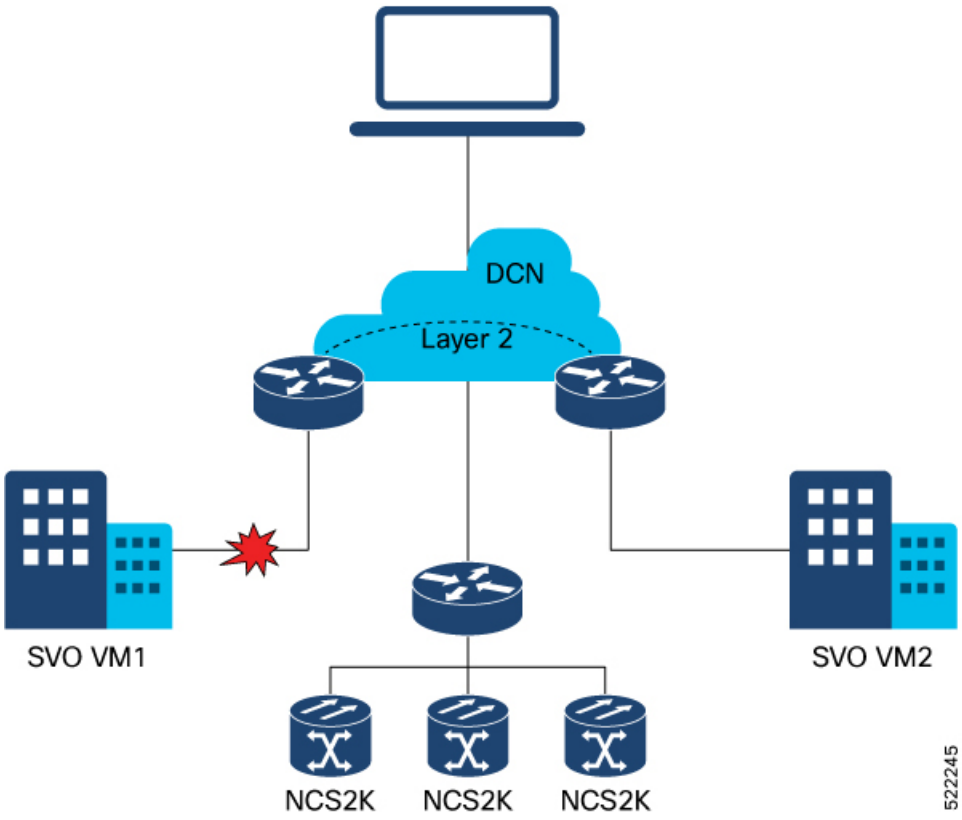
Data Center Restoration

Admin Plane and SVO instances periodically verify the communication channels for high availability.

When network connectivity restores, the SVO recognizes the networks in any order. The SVO can recognize the **devices** network first and then the **high availability** network, or vice versa.

Based on the order of recognition, there can be a transient (less than a minute) delay where an SVO instance is in an Active/Active state. Irrespective of the order, the Admin Planes manage all the situations, assigning the roles.

Figure 5: Data Center Restoration



Sudden Data Center Disconnection

Admin Plane and SVO Instances running on one server are not more able to communicate with the peers.

SVO Instances in Stand-By move to None because they are not able to communicate with the Active.

Admin Plane running in the disconnected data center, detects SVO Instances are not able to communicate with NCS 2000 devices, and aware of the high availability issue, move all the SVO Instances from Active to None.

Admin Plane running in the working data center is not able to communicate with the peer Admin Plane on both primary and secondary paths, it verifies SVO Instances are able to communicate with NCS 2000 devices, then moves SVO Instances from Stand-By to Active.

Use Cases

The following is the list of use cases for the SVO application setup.

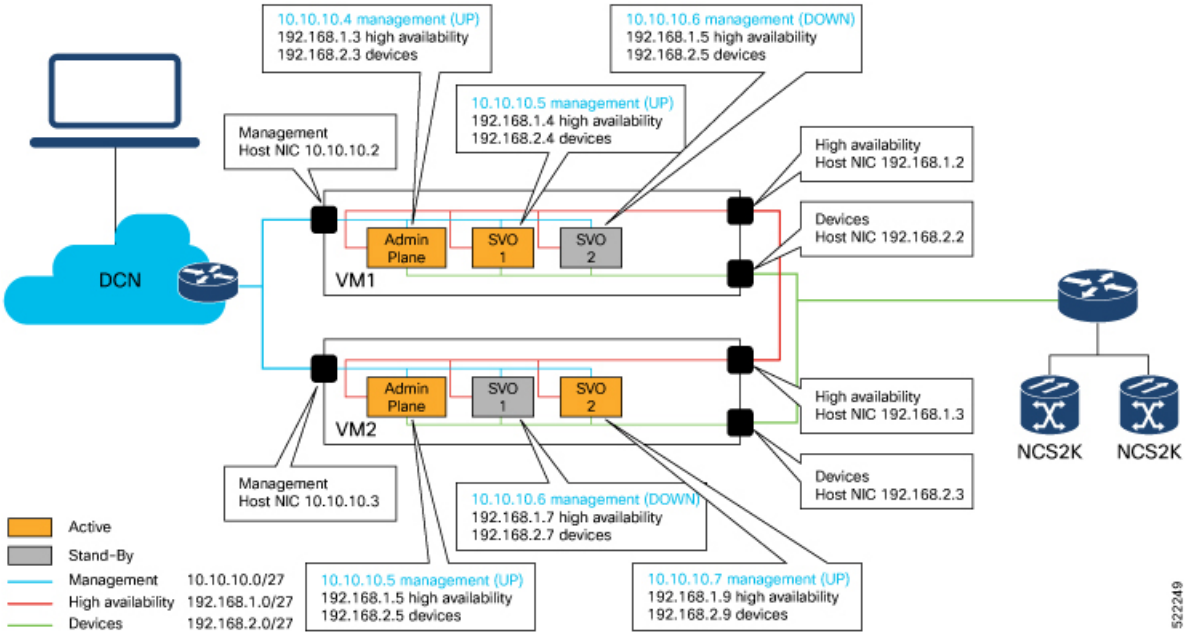
- Use Case 1 - Colocated Servers, on page 32
- Use Case 2 - Dislocated Servers (L2 Interconnection), on page 33

Use Case 1 - Colocated Servers

The following image displays typical use case of servers or VMs colocated in the same location, it shows an example of IP addresses assignment for host NICs, Admin Planes, and SVO instances.

From Release 12.1, the management, high availability, and devices networks are the same on both the servers or VMs.

Figure 6: Colocated Servers



Note Host NIC IP addresses (text in black) can be configured on the server or VM, before continuing with the SVO installation.

IP addresses in gray are automatically assigned by the Admin Plane during SVO creation.

Use Case 2 - Dislocated Servers (L2 Interconnection)

The following image displays the typical use case of servers or VMs distributed in different locations. It describes the IP addresses assigned for the host NICs, Admin Planes, and SVO instances.

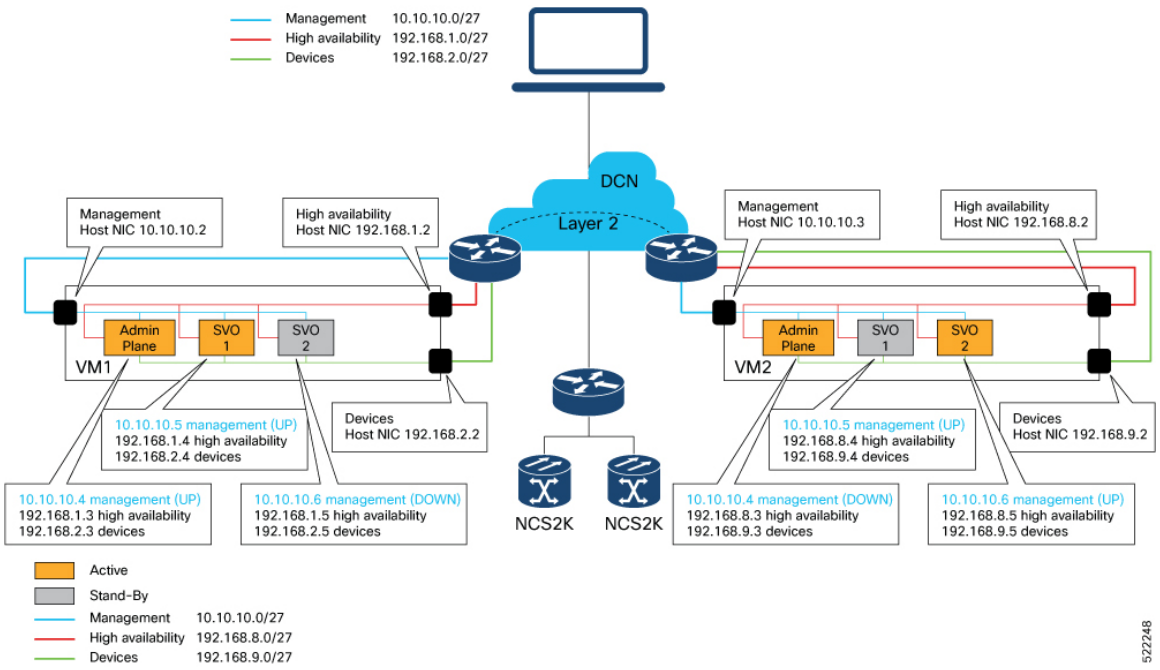
From Release 12.2, the management network is common for both the servers and VMs in different locations. However, the high availability and devices networks are different for both the servers and VMs in different locations.

Note To implement the Layer 2 connection for the router interfaces, use the IP addresses of the **management** subnet from the end. The valid Layer 2 connections are L2VPN, L2TPv3, VXLAN, or a similar solution.

The following lists the IP addresses to use for router interfaces on a specific **management** subnet:

- For the 10.10.10.0/27 subnet, use 10.10.10.29 and 10.10.10.30 IP addresses.
- For the 10.10.10.0/24 subnet, use 10.10.10.253 and 10.10.10.254 IP addresses.

Figure 7: Dislocated Servers



Note Host NIC IP addresses (text in black) can be configured on the server or VM before continuing with the SVO installation.

IP addresses in gray are automatically assigned by the Admin Plane during SVO creation.

Use Case 3 - Dislocated Servers (L3 Interconnection)

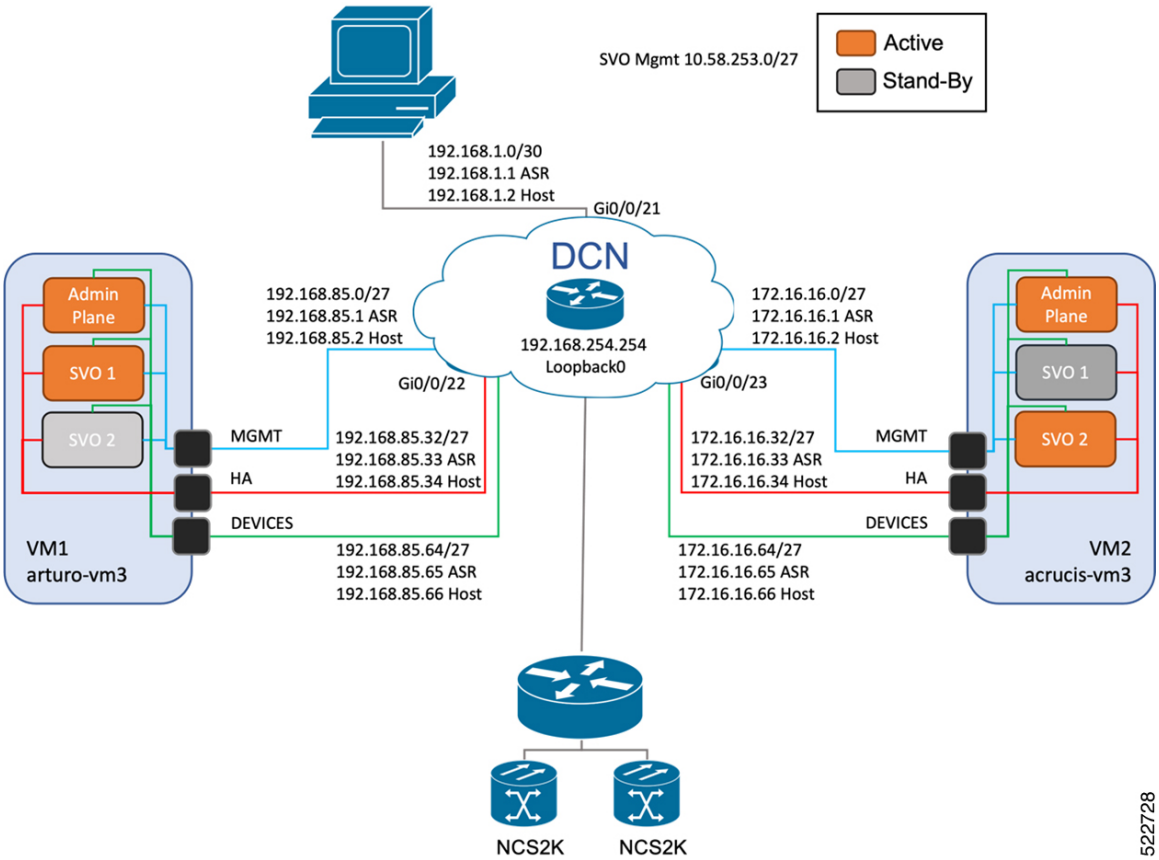
The following images display the typical use case of servers or VMs dislocated in different locations. It shows an example of IP addresses assignment for host NICs, Admin Planes, and SVO instances.

In this use case, the management interconnection at Layer 3 exists between the servers or VMs. The Layer 3 interconnection is the difference between this use case and the previous use cases.

From Release 12.3.1, the management, high availability, and devices networks are different for both the servers and VMs in different locations. However, the SVO applications share the same management subnet between the servers or VMs in different locations.

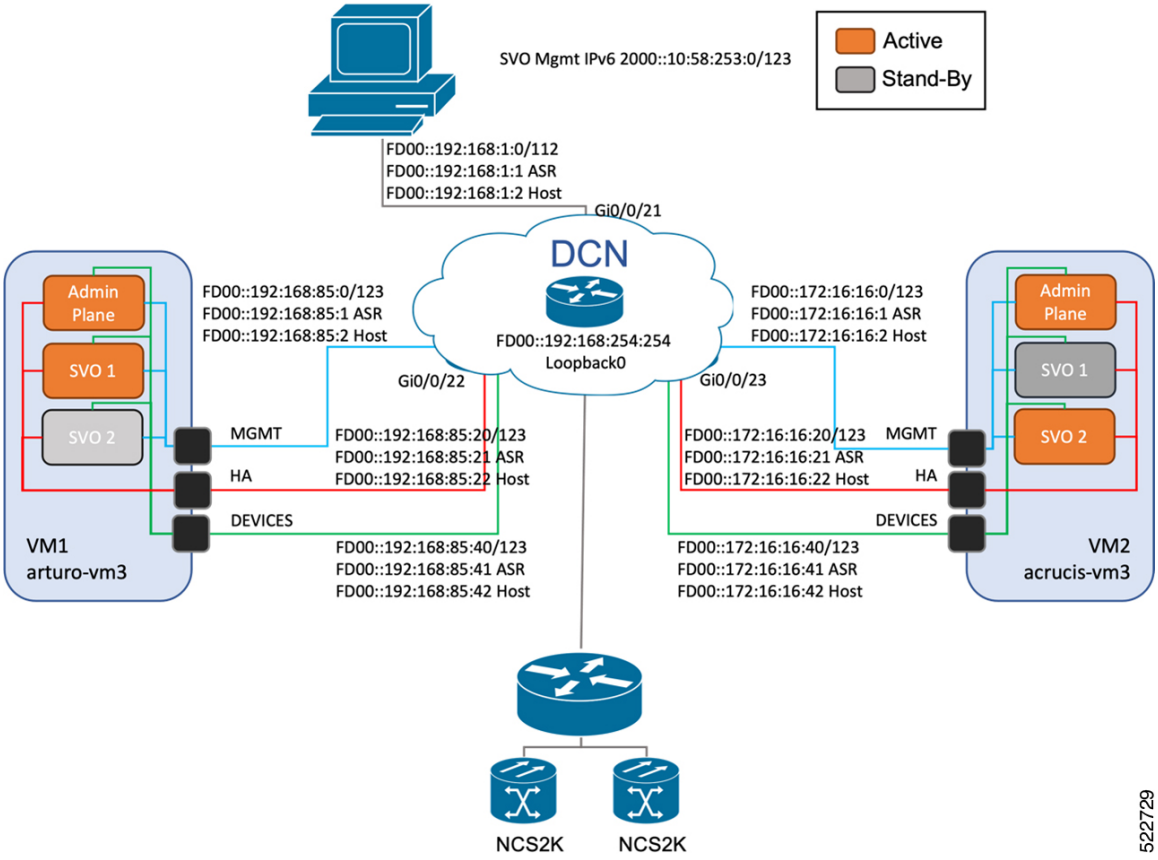
The following image displays the L3 interconnection with IPv4 addresses assigned to the server NICs. The SVO configured management subnet is **10.58.253.0/27**.

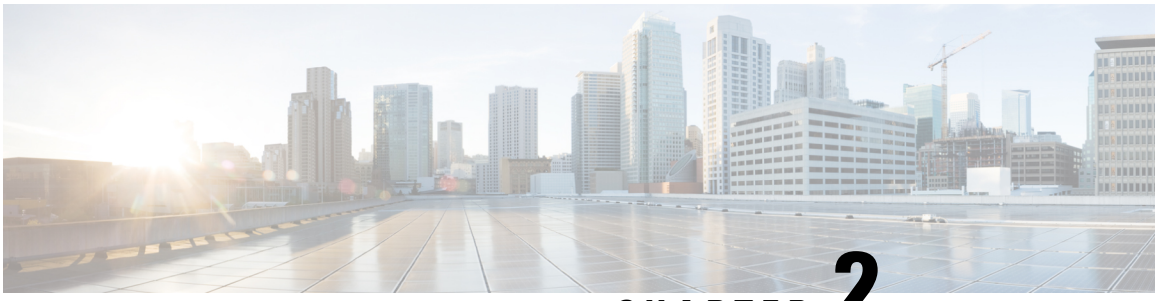
Figure 8: Dislocated Servers (L3 Interconnection) - IPv4 Configuration



The following image displays L3 interconnection with the IPv6 addresses assigned to the server NICs. The SVO configured management subnet is **2000::10:58:253:0/123**.

Figure 9: Dislocated Servers (L3 Interconnection) - IPv6 Configuration





CHAPTER 2

Cisco SVO Admin Plane

This chapter describes the admin plane that used in Cisco NCS 2000 SVO and its related tasks.

Table 5: Feature History

Feature Name	Release Information	Feature Description
Admin Plane UI Enhancements	Cisco NCS 2000 Release 12.2	The following admin plane UI enhancements are done to improve the user experience: • Flexible memory reservation replaces memory profiles. This enhancement allows the user to assign desired memory for an SVO instance. • **IP Assignment Policy** page replaces IP Filtering page. This change enables the user to modify IP addresses in the allowed list and denied list. In case of conflicting entries, the allowed IP address is preferred. • **SVO Runtime Status** page simplifies troubleshooting and allows the user to extract detailed information about the runtime environment of both the local and remote SVO instances. • **Admin Plane Restart** button replaces Reset to Factory Default button in the **Utilities** page. This enhancement enables the user to restart the admin plane when required. • **Certificates** page is introduced to check the details of SVO admin plane. The **Renew Certificate** button can be used to extend the lifetime of self-signed admin plane certificates by five years.

Feature Name	Release Information	Feature Description
Admin Plane UI Enhancements	Cisco NCS 2000 Release 12.3	The following admin plane UI enhancements are done to improve the user experience: • **Statistics** menu is introduced to present the memory details of the SVO instances in a table. The **SVO Instances Statistics** page contains **SVO Instance Memory Statistics** icon to view the memory details and **Download Memory Statistics** icon to download the memory details. • **SVO Instance Details** page is updated with **Restart SVO Container**, **Force local SVO Container**, and **Delete SVO Container** icons to troubleshoot both the local and remote SVO instances. • **Certificates** page is updated with **Upload Certificate** button. The **Upload Certificate** button can be used to upload a customized certificate by providing Key and Certificate files in .PEM format. • **Scripts** menu is introduced to upload custom scripts provided by Cisco. The custom scripts provide access to a few object models of the application.

Feature Name	Release Information	Feature Description
Admin Plane UI Enhancements	Cisco NCS 2000 Release 12.3.1	The following admin plane UI enhancements are done to improve the user experience: • SVO containers now have the limit memory besides the reseved memory. The limit memory is a threshold that is set by the Admin Plane at 2 GB higher than the reserved memory. When you configure the reserved memory, the Admin Plane automatically assigns the limit memory that is shared by the SVO containers. The limit memory acts a buffer to absorb the temporary peak memory requirements. • In **IP Assignment Policy** page, you can enter multiple IP addresses using Range, List, and Wildcard inputs. This approach reduces the tedious and error-prone task of manually typing multiple IP addresses. • **Troubleshooting** menu is introduced to perform on-demand health checks on the network infrastructure and identify the common misconfiguration. You can view the report in the **Network Troubleshooting** page. • The new **Properties** menu enables you to easily modify and customize multiple admin plane properties. This menu reduces the task of manually editing each property file in the local system.

- Cisco SVO Admin Plane Overview, on page 41
- Log into the Cisco SVO Admin Plane, on page 42
- SVO Admin Plane Home Page, on page 43

Cisco SVO Admin Plane Overview

Cisco SVO admin plane is responsible for turning up the shelf virtualization orchestration services for the network elements (NE). It is a web user interface that facilitates the installation of the SVO software and configures the NE instances and orchestrates high availability (HA) services.

The admin plane is supported both on the external server and the SVO card. The admin plane allows you to create, update, manage, and delete SVO NE instances.

To achieve high availability for the exernal server, the SVO software is installed on two servers in local and remote locations. In the case of the SVO card, two SVO line cards are installed in two different chassis of the ROADM node. The two external servers or two SVO cards are connected by two intercommunication links—through the HA network (primary link) and through the devices network (secondary link). Both links are used for the communication between the admin planes. The primary link is also responsible for replicating all the configuration transactions that are performed on each active SVO instance to the related standby SVO instance.

All the networking configuration data required by the admin plane is present in a file shared by both the SVO cards or external servers. When creating a new SVO instance, you can configure the management interface address, while the other parameters are automatically selected by the admin plane based on the constraints defined in the configuration file.

The admin planes coordinate to automatically assign active and standby roles to the SVO instances. The admin planes can also perform an automatic switchover that promotes the standby instance to active when software or hardware faults affect the active instance.

The Cisco SVO admin plane allows you to:

- Create the super user for the SVO card model or the admin user for the external server model.
- Create, update, or delete SVO instances of type ROADM, OLA, DGE, or TXP. You can also view the details of the SVO instances.

Note The first SVO instance created on the SVO card is always a ROADM instance. Subsequent SVO instances can be OLA, DGE, or TXP.

- Control, monitor, and performs health checks of the SVO instances.
- Auto switch SVO instances during a software or hardware fault in the SVO cards or servers.

- Force a manual switch between the active and standby SVO instances.
- View parameters of the network configuration file.
- View a list of allowed and blocked IP addresses
- Troubleshoot using diagnostics. A zip file containing the log files from the admin plane can be downloaded.
- Reset the SVO card to factory defaults. This action erases all containers and configurations on the SVO card.

The following table highlights the differences between the two types of system installation.

SVO Card Model	External Server Model
The super user must be created to log in to the admin plane.	The admin user must be created to log in to the admin plane.
Only IPv4 addresses can be configured.	IPv4 or IPv6 addresses can be configured independently for the three networks (Management, HA, and Devices) during the installation.
Only one ROADM SVO instance can be created. Subsequent instances must be of type OLA, DGE, or TXP.	Any number of ROADM, OLA, DGE, or TXP SVO can be created.
The SVO card can be reset to its default values.	—

Log into the Cisco SVO Admin Plane

Use this task to log in to the Cisco SVO admin plane.

Procedure

Step 1 In the browser URL field, enter the IP address of the admin plane (https://*IP_address*/login).

The login page appears.

Step 2 Enter the username and password.

In an SVO card system, only the superuser is allowed to log in to the Cisco SVO admin plane.

Step 3 Click **Login**.

The SVO Instances page is displayed.

SVO Admin Plane Home Page

Table 6: Feature History

Feature Name	Release Information	Feature Description
Device Synchronization and Alarm Status Icon	Cisco NCS 2000 Release 12.3	The device synchronization and alarm status icon indicates the status of the device and alarm synchronization with varying colors. The colors in the synchronization status icon are: • Green • Orange • Red

Side Menu Items

In the SVO Admin Plane home page, the menu items are present in the left panel. The menu items allow you to monitor and troubleshoot SVO instances, view certificates, and restart admin plane. The following list describes the menu items.

- **Instances**—Instances menu enables you to create, edit, and monitor SVO instances.
- **Diagnostics**—Diagnostics menu allows you to download log files to troubleshoot SVO instances.
- **Networks**—Networks menu enables you to configure networks and assign IP addresses.
- **Certificates**—Certificates menu enables you to view and renew the self-signed admin plane certificates.
- **Utilities**—Utilities menu allows you to restart the admin plane.

Device Synchronization and Alarm Status Icon

The device synchronization and alarm status are indicated as a summary icon with changing colors close to the bell icon.

Note The icon appears only when you synchronize a device.

The icon indicates the device synchronization and alarm status with respective colors. The icon color changes from lower to a higher priority. The icon statuses are:

- **Green**—All the defined devices are connected and synchronized. The device status is alarm-synchronised.
- **Orange**—One or more devices are disconnected or locked by the user. The device status changes as sync-not-started, sync-configuration, and sync-operational.
- **Red**—One or more devices have sync-error, sync-not-completed, or out-of-sync-alarms.

Router Icon (BGP Status)

Each Admin Plane constantly monitors its BGP daemon, exchanging information with its peer about the BGP service and neighbor relationship status.

Note The icon appears only when SVO is installed with management interconnection at Layer 3.

A router icon with two colored dots over it indicate the neighbor relationship status of the servers or VMs with the core router. The first dot represents the local status, and the second dot represents the remote status. The dots statuses are:

- **Green**—Server or VM has established BGP connection.
- **Red**—Server or VM has lost or not yet established BGP connection.

Bell Icon (HA Status)

The icon on the top right of the SVO home page indicates the status of high availability network (primary link) and devices network (secondary link). The icon statuses are:

- **Green**—Both the primary and secondary links are up. High availability is working successfully.
- **Yellow**—A warning that the primary link is up but the secondary link is down.
- **Red**—There are two cases:
  - **Small red icon**—The primary link is down but the admin planes are able to communicate because the secondary link is up.
  - **Large red icon**—Both the primary and secondary links are down and the server is functioning in standalone mode.

User Profile Icon

The user profile icon displays the username and the log out option for the user to exit the current SVO session.

SVO Instances

An SVO instance is a software virtualization of the physical NCS 2000 node that has been configured to manage. SVO instances are of types—ROADM, OLA, DGE, and TXP. In an SVO card model, you can configure a maximum of one ROADM SVO instance and up to 30 OLA DGE, or TXP SVO instances.

In an external server model, you can configure any number of ROADM, OLA, DGE, or TXP SVO instances.

You can create, update and delete SVO instances using the admin plane. Each SVO instance runs as an active instance on one server and as a standby instance on the other server. It is also possible to manually switch the roles of the SVO instance between active and standby.

The peer admin planes that are running on the local and remote server respectively have two intercommunication links, one through the HA network (primary link) and the other through the devices network (secondary link).

The table displays the SVO instances that were created. Each row has two entries relating to the local and remote SVO card or server. In each row, the first entry is the local instance and the second entry is the remote instance. The details are:

- **Name**—Name of the SVO instance.
- **IP Address**—The IP address of the SVO instance. It is IPv4 for the SVO card model, and IPv6 or IPv4 for the external server model.
- **SW version**—SW version on the server.
- **State**—State of the SVO instance.
- **App State**—State of the SVO application that is running on the SVO instance.
  - During a manual switching process, the **App State** field displays different statuses such as SWITCHING, SWITCH_DONE, or UP.
  - The **App State** field displays ACTIVATING or ACTIVATE_RESTART only after the SVO web UI has requested the admin plane to orchestrate the activation process.
- **Role** —Role of the SVO instance. The roles are ACTIVE, STANDBY, NONE, and UNKNOWN. In case of issues or specific SVO states, special tags are displayed such as NOT_RESPONDING, STARTING,STOPPED, or BAD_CLUSTER.

Note The green icon indicates the reachability of the SVO instance to the connected NCS 2000 device. If the active SVO instance is unable to reach the NCS 2000 device due to a network segregation, it performs an auto-switch.

- **Up Time**—Up time of the SVO instance.
- **Type**—Label for the SVO instance.
- **Action**—A set of actions can be performed on the SVO instance:
  - **Details of the SVO instance—**Click this icon to view the summary of the local and remote SVO instance.
  - **Edit SVO Instance**—Click this icon to edit the memory size of the SVO instance.
  - **Switch SVO Instance**—Click this icon to manually switch the SVO instance between servers.

Note A switch operation is possible only if both the SVO instances are up and running and the role of the instances are Active and Standby.

- **Delete SVO Instance**—Click this icon to delete an SVO instance.

Note This icon is disabled when a switch operation is in progress.

Create an SVO Instance

Use this task to configure an SVO instance.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click the + button at the top-left of the SVO Instances page.

The SVO Instance Configuration page appears.

Step 2 In the **General Info** area, perform these steps:

a) Enter the name for the new SVO instance in the **Name** field.

The name is mandatory and must be unique among the SVO instances managed by the admin plane. It can contain a minimum of two characters and a maximum of 64 characters. It can include numbers, uppercase letters, lowercase letters, dashes (-), or underscores (_).

b) Choose the version from the **Software Version** drop-down list.

c) Choose the type of the SVO instance from the **TDM Terminology** drop-down list.

The two options are ANSI and ETSI.

d) Choose the label of the SVO instance from the **Type** drop-down list.

The four options are ROADM, OLA, DGE, and TXP. The type indicates the role of the SVO instance in the network.

Note When Type is selected, a default value for memory size is displayed in the **Reserved Memory GB** field.

e) Choose the memory size to be allocated to the SVO instance from the **Reserved Memory GB** field.

The user is allowed to reserve the SVO container memory in steps of 0.1GB. This value is visible and summarized at server level in the SVO instances table.

Note In addition to the reserved memory, SVO container allocates the Limit Memory. SVO solution automatically sets the Limit Memory with a threshold value of 2 GB higher than the configured Reserved Memory. This threshold acts as a buffer to absorb the temporary peak memory requirements. Docker engine kills the operations that cross the Limit Memory threshold due to Out-of-Memory (OOM).

If the reserved memory is alloted more than the server or VM memory, the docker engine fails the allocation. Allocate only up to 80 percent of the server or VM memory for the Reserved Memory.

Step 3 In the **Admin User** area, perform these steps:

a) Enter the username in the **Username** field.

The values "admin," "oper," "private," or, "public" cannot be used as the admin username.

b) Enter the password in the **Password** field.

The password must be a minimum of eight characters. The password must contain at least an uppercase letter a number, and a special character. The special characters supported are ! $ % ^ ( ) [ ] _ - ~ { } . +

c) Enter the password again in the **Retype Password** field.

Step 4 In the **Management Network** area, the system suggests the management subnets to be used in the **IPv4 Address** or the **IPv6 Address** fields, depending on the type of addressing defined during the installation. The system checks for constraints defined in the network configuration file and ensures that the IP addresses that are assigned are not in use.

a) Enter the IPv4 Address in the **IPv4 Address** field in a SVO card model.

or

b) Enter the IPv4 or the IPv6 Address in the **IPv4 Address** or **IPv6 Address** field respectively in an external server model.

Step 5 Click **Create**.

Step 6 A message is displayed indicating the creation of the SVO instance.

Step 7 Click **OK**.

The SVO Instances page appears. The table displays the new SVO instance.

The SVO instance can now be accessed through a web browser.

View Details of an SVO Instance

Use this task to view the details of an SVO instance.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Choose the SVO instance you want to view.

Step 2 Click **Details of SVO Instance**.

The **SVO Instance Details** page is displayed. See SVO Instance Details, on page 49.

Edit Reserved Memory of an SVO Instance

Use this task to edit the memory size of the SVO instance.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Choose the SVO instance that you want to edit.

Step 2 Click **Edit SVO Instance**.

The SVO Instance Edit page is displayed.

Step 3 Choose the memory size to allocate to the SVO instance from the **Reserved Memory GB** field.

Note After upgrading the SVO solution to R12.31, you should adjust the containers memory to default 2.1GB. Allocate only up to 80 percent of the server or VM memory for the Reserved Memory. Enough free Host memory must be available to set the Limit Memory.

Step 4 Click **Edit**.

Switch SVO Instances

Use this task to manually switch between active and standby SVO instances.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Choose the SVO instance you want to switch.

Step 2 Click **Switch SVO Instances**.

A dialog box is displayed asking for confirmation.

Step 3 Click **Confirm**.

During the switching process, the **App State** field displays different statuses such as SWITCHING, SWITCH_DONE, and UP. The **Role** field displays NONE, ACTIVE, and STANDBY.

Delete an SVO Instance

Use this task to delete an SVO instance.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Choose the SVO instance you want to delete.

Step 2 Click **Delete SVO Instances**.

A dialog box is displayed asking for confirmation of deletion.

Step 3 Click **Confirm**.

SVO Instance Details

The SVO Instance Details page provides information on the various properties of both local and remote SVO instances. The Admin & Troubleshooting property includes a set of action icons for both SVO instances. The action icons enable you to troubleshoot the SVO instances. The actions are:

- **Get local SVO Runtime Status**—Click this icon to extract detailed information about the runtime status of both local and remote SVO applications.
- **Restart Container**—Click this icon to restart the target SVO container.
- **Delete local SVO container**—Click this icon to delete the target SVO container.
- **Force as Active the local SVO container**—Click this icon to force the local SVO container to become the active instance.

Retrieve SVO Runtime Status

Use this task to retrieve the runtime information of local or remote SVO instances.

Procedure

Step 1 Click the heartbeat icon next to the required instance.

The **SVO Runtime Status** page is displayed.

Step 2 Expand the related sections to view the details of the SVO instances.

The sections are NCS Status, HA Agent, and NCS Launcher.

Step 3 Click the hyperlink above the expandable sections to view the details in separate window as plain text.

Restart SVO Container

Use this task to restart the required SVO instance.

Procedure

Click the reload icon next to the desired instance.

You are redirected to the SVO Instances page.

The SVO instance reloads.

Delete SVO Container

Use this task to delete the required SVO instance.

Procedure

Step 1 Click the trashcan icon next to the required instance.

A warning dialog box appears.

Step 2 Click **Confirm**.

Success message appears.

Step 3 Click **OK**.

You are redirected to the SVO Instances page.

Force Active the Local SVO Container

Use this task to force a local SVO instance as ACTIVE. This action must be performed only when the admin plane fails to assign a role to the local instance.

Procedure

Click the go-forward icon next to the local instance.

You are redirected to the SVO Instances page.

The status of the local SVO instance changes from NONE to ACTIVE.

IP Assignment Policy

The IP Assignment Policy page displays two sets of IP addresses:

- Allowed List—Contains a list of available IP addresses.
- Denied List—Contains a list of blocked IP addresses.

The list of allowed and denied IP addresses displayed on this page are stored in two separate files on the file system of the local and remote server.

The IP lists are applicable only to the devices network. During the creation of the SVO instance, the denied list prevents the admin plane from selecting any IP address that is on the list for the IPv4 and IPv6 addresses whereas the allowed list permits the admin plane to select any IP address that is in the list.

The IP list can be modified on this page at runtime.

To view these IP addresses in the admin plane:

Before you begin

Log into the Cisco SVO Admin Plane, on page 42.

Procedure

Step 1 Click **Networks** in the left panel and choose **IP Assignment Policy**.

Step 2 Enter the needed IP addresses in the **Allowed IP addresses list** and **Denied IP addresses list** columns.

Use one of the following methods to enter multiple IP addresses:

- **List**—For Example, 192.168.1.**1,4** becomes [192.168.1.1, 192.168.1.4].

  Use comma to enter a list of IP addresses.

- **Range**—For example, 192.168.1.**1-4** becomes [192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4].

  Use hyphen to define a range of IP addresses.

- **Wildcard**—For example, 192.168.1.***** becomes [192.168.1.1,..... , 192.168.1.255].

  Use asterisk to enter all the possible IP addresses in the subnet.

Step 3 Click **Apply**.

When you apply the changes, all the shortcuts expand and join into the final list.

Note If conflicting entries exist, the allowed IP address has the precedence.

Restart Admin Plane

Use this task to restart the SVO admin plane.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click **Utilities** in the left panel.

The Utilities page appears.

Step 2 Click **Restart Admin Plane**.

All the SVO instances and configurations available on the SVO card are restarted.

A **Warning!** dialog box appears.

Step 3 Click **Confirm**.

Warning Proceeding with confirmation may interrupt any running procedure.

Manage Certificate

Certificates are required to enable security protocols for the SVO application. Use this task to generate a self-signed certificate or upload your own certificate for the admin plane.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42.

Procedure

Step 1 Click **Certificates** in the left panel.

The **Certificates** page displays the certificate details.

Step 2 To manage the certificates, perform one of the following actions:

- In the case of a **self-signed certificate**, click **Generate Selfsigned Certificate**.
- In the case of an **own certificate**, perform the following steps:
  - **a.** Click **Upload Certificate**.

    The **Custom Certificate Configuration** dialog box appears.
  - **b.** In **Key file**, click the **Add** icon to upload the key file in .pem format.
  - **c.** In **Certificate file**, click the **Add** icon to upload the certificate file in .pem format.
  - **d.** Click **Generate Certificate**.

    Your certificate is uploaded.

SVO Instances Statistics

SVO instances statistics table is a collection of memory resource details for each SVO instance. The table periodically collects details such as allocation and consumption of memory for each SVO instance. The statistics table is similar to the SVO instances table with a **Memory** column.

You can view and download the statistical data of the SVO instances using the icons in the **Actions** column. Each SVO instance runs as an active instance on one server and as a standby instance on the other server.

The table displays the created SVO instances and the associated memory details. Each row has two entries relating to the local and remote SVO card or server. In each row, the first entry is the local instance and the second entry is the remote instance. The details are:

- **Name**—Name of the SVO instance.
- **IP Address**—The IP address of the SVO instance. It is IPv4 for the SVO card model, and IPv6 or IPv4 for the external server model.
- **SW version**—SW version on the server.
- **Role**—Role of the SVO instance.

Note The green icon indicates the reachability of the SVO instance to the connected NCS 2000 device. If the active SVO instance is unable to reach the NCS 2000 device due to a network segregation, it performs an auto-switch.

- **Type**—Label for the SVO instance.
- **Memory (GB) Min/Max/Actual**—Minimum and maximum memory allocated for each instance and actual memory utilized by each instance.
- **Actions**—A set of actions performed on the SVO instance. The actions are:
  - **Memory Statistics Graph**—Click this icon to view the summary of the local and remote SVO instance.
  - **Download Local Statistics File**—Click this icon to download all the statistics files of the local SVO instance as a zip package.

View Memory Statistics Graphical Summary

Use this task to view the memory details of local and remote SVO instances in graphical format.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click **Statistics** in the left panel.

The **Statistics** page appears.

Step 2 Click **Memory Statistics Graph** for an SVO instance.

The **SVO Instance Memory Statistics** page appears displaying memory statistics for both local and remote instances.

Note The **Memory Statistics** graph displays a fine-grained collection of memory usage of the SVO instance in the last few days. Memory limits defined at creation time are also displayed for reference. The **Historical Daily Statistics** graph displays the daily memory details such as average memory usage and maximum memory usage of the SVO instances since creation.

Step 3 (Optional) Click the calender icon to view the statistics for the required period.

Step 4 Click the table icon to export the data as plain text in a new window.

Download Local SVO Instances Memory Files

Use this task to download the local SVO instances memory files.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click **Statistics** in the left panel.

The **Statistics** page appears.

Step 2 Click **Download Local Statistics File** for an SVO instance.

A confirmation message appears.

Step 3 Click **OK**.

The statistics files for the local SVO instance downloads as a zip package.

Download Diagnostic Log Files

Use this task to download the diagnostic log files.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click **Diagnostic** in the left panel.

The Diagnostic page appears.

Step 2 Click **Download Log Files**.

A zip file that contains the admin plane logs is downloaded.

Custom Scripts

Custom scripts are quick solutions that are specific to each feature. The scripts provide access to the full application object model to extend the capabilities of the admin plane at runtime

The custom scripts let you do the following actions and more:

- Add UI- and REST-based custom actions
- Define in a declarative way web input forms for action parameters
- Export data in different text formats
- Add custom validation logic, for example, when creating a new SVO instance
- Perform custom tasks on application events, for example, when the HA role changes
- Define scripted HA services that can communicate through the Admin Plane GRPC channels

The scripts table displays the added scripts and the relevant script details. The following list describes the table items.

- **Name**—Name of the custom script
- **Type**—Type of the custom script
- **Target**—Target GUI of the SVO admin plane
- **Status**—Status of the custom script
- **Version**—Version of the custom script added
- **Lifetime**—Duration of the script in the admin plane in **dd:hh:mm:ss** format
- **Action**—Action to delete the added script

Add Custom Scripts

Use this task to add custom scripts to the SVO admin plane, for example, **importInstancesCSV** file.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click **Scripts** in the left panel.

The Scripts page appears.

Step 2 Click **Add new SVO script**.

An explorer window opens.

Step 3 Select a custom script and click **Open**, for example, **importInstancesCSV** file.

A Success message appears.

Step 4 Click **OK**.

The **importInstancesCSV** script is added to the scripts table.

Step 5 Check the SVO Instances table in the admin plane for the **Import CSV** button.

The **Import CSV** button allows you to import the SVO instances using a CSV file.

Modify Admin Plane Properties

Admin plane is customizable through several configuration properties. A few of the admin plane properties are useful in particular contexts or for troubleshooting. From Release 12.31, some "expert only" settings are modifiable directly from the Admin Plane web UI.

Use this task to modify the admin plane properties.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click **Tools** in the left panel and choose **Properties**.

The **Properties** page appears to display the admin plane properties, current values, and edited values.

Table 7: Properties Table

Label	Description
Property	Displays the customizable admin plane properties
Current Value	Displays the current values of each admin plane property
Edited Value	This field is editable. Enter the values for the admin plane properties.

Step 2 To modify the values for the admin plane properties, perform one of the following actions:

Tip When you hover over a property, a tooltip appears to explain the property purpose.

- In **Edited Value**, enter the needed values for the properties that you want to customize.
- Click **Reset to default** to restore the default settings for all the properties.

Step 3 Click **Apply** to apply the modified values.

A **Warning!** message appears.

Step 4 Click **Continue**.

A **Success!** message appears.

Step 5 Click **OK**.

Step 6 Restart the admin plane to commit the modified values in the properties files. See Restart Admin Plane, on page 51.

Remember Modified properties are not automatically propagated to the peer server. Make the same changes on the peer server to align the properties files with the host server.

Troubleshoot Networks

SVO requires proper configurations of management, high availability, and devices networks. The **Networks Troubleshooting** page allows performing general health-checks and identifying some common misconfiguration in the network infrastructure. It performs extra reachability checks when you specify an optional device IP address of any relevant network device.

Use this task to initiate the troubleshooting report of the network infrastructure or a target device.

Before you begin

Log into the Cisco SVO Admin Plane, on page 42

Procedure

Step 1 Click **Networks** in the left panel and choose **Troubleshooting**.

The **Networks Troubleshooting** page appears.

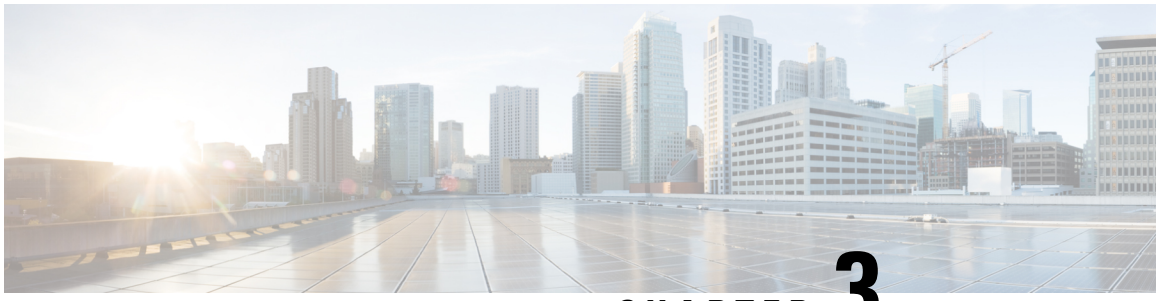
Step 2 Click **Troubleshooting** to initiate checks on the network infrastructure.

Network troubleshooting report appears in the pane below the **Troubleshooting** button.

Step 3 (Optional) In **Device IP address:** field, enter the IP address of the device and click **Troubleshooting**.

Note Enter only the IP address of a device that is reachable without adding any IP route.

Troubleshooting report for the target device appears in the pane below the **Troubleshooting** button.



CHAPTER 3

Cisco Light Web User Interface

This chapter describes the Cisco Light Web User Interface that is used to bring up a remote node.

Cisco Light Web User Interface Overview

The Cisco Light Web User Interface (UI) is a new standalone solution and is used when:

- Installing networks in order bring up a remote node
- A remote node where there is DCN or OSC connectivity, to initiate networking with SVO hosts

The remote nodes are connected through optical fibers through OSC interfaces. These OSC interfaces must be turned on to connect to the SVO web UI.

After the OSC interfaces are up and functional, you can use the SVO web UI to manage the NCS 2000 network elements.

The light web UI runs on the browser without the need to download any JAR or Java files. The UI can be used across multiple operating systems and browsers.

The light web UI allows you to:

- View the summary of an existing remote node such as device, network, and OSC configurations.
- Provision new control card parameters for the remote node.
- View the diagnostics.

During bring up, you must:

- Insert a control card in the remote node. For more information on the control card installation, see Installing the TNC, TNCE, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card, on page 146.
- Power on the remote node and connect an Ethernet interface.
- Configure the remote node using the light web UI to provision new control card parameters and turn on OSC interfaces.

- Check the diagnostics if the OSC interfaces are up and functional.

Now you can connect the SVO web UI to manage the NCS 2000 network elements.

Log into the Remote Node Light Web User Interface

Use this task to log into the remote node light web UI.

Procedure

Step 1 In the browser URL, enter *https://<ipv4/ipv6-address>/light-ui* for for secure nodes or *http://<ipv4/ipv6-address>/light-ui*.

The NCS 2000 Device Management login page appears.

The IP address to be used is the factory default unless you have changed it during the installation of the control card. New control cards are shipped with 192.1.0.1.

Only IPv4 address is supported.

Step 2 Enter the username and password:

When you log into the light web UI for the first time, the system prompts you to change the default password and set a new password.

- For a brand-new factory card, the default user is **tornado** and the password is **password**.
- For a card after the reset factory default procedure, the username is **CISCO15** and password is **otbu+1**.

The NCS 2000 Device Management page appears.

Provision Control Card Parameters

Use this task to provision new control card parameters.

Procedure

Step 1 Click the **Provisioning** tab.

The **Provisioning** page appears.

Step 2 Click the **Device Configuration** area.

Step 3 From the **System Mode** drop-down list, choose ANSI or ETSI.

Step 4 Click **Submit**.

A confirmation message appears.

Step 5 Click **Ok**.

Step 6 In the **Network Configuration** area:

a. **Device Name**—Enter the name for the device.

b. **IPv4 Address**—Enter the network address.

c. **TNC Front Port Role**—Select the port role from the **TNC Front Port Role** drop-down list. The available options are Access or Trunk.

d. **Subnet Mask Length**—Enter the length of the subnet mask.

e. **Gateway IP Address**—Enter the IP address of the Gateway.

f. **LAN OSPF Area-id**—Enter the area ID of the LAN OSPF.

g. **Gateway Settings**—Click the **Enable SOCKS** check box to configure SOCKS Proxy server on NCS 2000 nodes.

Choose one of the following options:

- External Network Element (ENE)—Choose this option when the node is not connected to a LAN but has DCC connections to other nodes.
- Gateway Network Element (GNE)—Choose this option when the node is connected to a LAN and has DCC connections to other nodes.
- SOCKS Proxy Only—Choose this option when the node is connected to a LAN and the LAN is separated from the node by a firewall.

h. **Enable IPv6**—Click the **Enable IPv6** check box to enable IPv6. When IPv6 is enabled, SOCKS Proxy server configuration is mandatory.

Enter the following information:

- **IPv6 Address**—Enter the IPv6 node network address.
- **Subnet Mask Length**—Enter the subnet mask of the network.
- **IPv6 Default Router**—Enter the IPv6 address of the default router.
- **Disable IPv4 access for IPv6 enabled ports**—Check **Disable IPv4 access for IPv6 enabled ports** check box. This option is enabled only for nodes in single mode.

Step 7 Click **Submit**.

A confirmation message appears.

Step 8 Click **Ok**.

Step 9 In the **OSC & UDC/VOIP Configuration** area to add the OSC interface configuration:

In the **OSC Config** area:

a. **Shelf Number**—Select from the **Shelf Number** drop-down list. The available option is 1.

b. **Slot Number**—Select from the **Slot Number** drop-down list. The available options depend on the slot number in the chassis.

c. **Port Number**—Select from the **Port Number** drop-down list. The available options are 1 or 2.

d. **Payload**—Select payload from the **Payload** drop-down list. The available options depend on the system mode selected.
   - STM-1 (ETSI) or OC-3 (ANSI)
   - FE
   - ONE-GE

e. **OSPF Area-id**—Enter the OSPF area ID for the OSC interface.

f. Click **Add** to add the OSC interface configuration.

   A confirmation message appears.

g. Click **Ok**.

In the **UDC/VOIP Config** area:

a. **1-1 (Slot-1) (STM-1)**—Click the **1-1 (Slot-1) (STM-1)** radio button to select the 1-1 STM-1 slot.

b. **Service Type**—Select the service type from the **Service Type** drop-down list.
   - UDC
   - VOIP

c. Click **Apply**.

Step 10 In the **OSC Configuration** area, to delete the OSC interface configuration:

a. Select the payload from the **Payload** drop-down list.

b. Select the OSPF area ID from the **OSPF Area-id**.

Step 11 Click **Delete**.

A confirmation message appears.

Step 12 Click **Ok**.

Note The drop-down list displays only options for cards and pluggables equipped in the chassis.

To delete the shelf, slot, and port numbers, you must remove the pluggable from the chassis.

Verify Control Card Parameters

In the **Summary** page, you can verify the new or existing control card configuration of the remote node.

Procedure

Step 1 Click the **Device Configuration** area to view the new or existing **Device** configuration.

- **Device Mode**—Displays whether the device mode is ANSI or ETSI.

Step 2 Click the **Network Configuration** area to view the following new or existing network configuration.

In the **IPv4** table:

- **IPv4 Address**—Displays the IPv4 node network address.
- **Subnet Mask Length**—Displays the subnet mask of the network.
- **Gateway IP Address**—Displays the IP address of the gateway.
- **LAN OSPF Area-id**—Displays the area ID of the LAN OSPF. If there is no value appearing in this field, then it is configured to default.
- **Device Name**—Displays the device node name.
- **TNC Front Port**—Displays whether the TNC front port is Access or Trunk.
- **IPv4 Access on IPv6 enabled ports**—Displays whether the IPv4 access set on IPv6-enabled port is true or false. By default IPv4 is enabled (true) when IPv6 is enabled and node has both the IPv4 and IPv6 addresses, but in single shelf mode it is possible to disable IPv4 (false).
- **Gateway Network Element**—Displays whether the gateway network element is enabled.

In the **IPv6** table:

- **IPv6 Address**—Displays the IPv6 node network address.
- **Subnet Mask Length**—Displays the subnet mask of the network.
- **IPv6 Default Router**—Displays the IPv6 address of the default router.
- **Gateway Network Element**—Displays whether the gateway network element is enabled.

Step 3 Click the **OSC & UDC/VOIP Configuration** area to view the new or existing OSC configuration.

- **Slot**—Displays the slot number of the chassis.
- **Port**—Displays the port number through which the OSC interface is configured.
- **Payload**—Displays the configured payload mode of the system.
- **OSPF Area-id OSC**—Displays OSPF area ID configured on the OSC interface.
- **Service Type**—Displays the service type. The service types are NONE, UDC, or VOIP.

View Diagnostics

Use this task to view the diagnostics of the remoteLA node.

Procedure

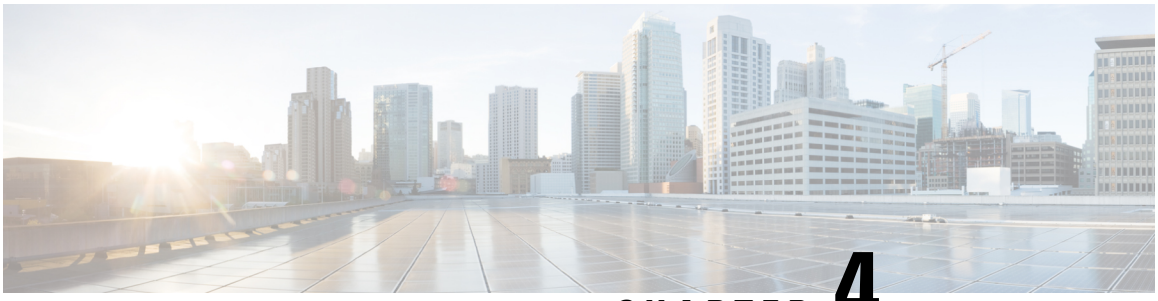
Step 1 Click the **Diagnostics** tab.

The **Diagnostics** page appears.

Step 2 In the **Diagnostics** page, click the **Live Diagnostics** button.

The following information is displayed:

- Power details such as EID, AID, power on the OSC interface, laser bias, Tx, and Rx power.
- Routing information
- OSPF area trace details
- OSPF routing table information
- OSPF external routing table information
- OSPF global, virtual, and neighbor configuration information
- OSPF topology details
- Network details



CHAPTER 4

SVO Web User Interface

This chapter describes the web user interface used in Cisco NCS 2000 SVO and its related tasks.

Understanding Shelf Virtualization Orchestrator

Table 8: Feature History

Feature Name	Release Information	Feature Description
SVO extends card provisioning on the NCS 2002 Chassis	Cisco NCS 2000 Release 12.3.1	This release enables you to provision the control cards on slot 1 and the following service cards on the slots 2 and 3 of the NCS 2002 chassis: • Transponder and muxponder cards • Optical service channel cards • Optical amplifier cards • Optical add/drop cards • Reconfigurable optical add/drop cards You can set operating mode, and provision features that are supported on these cards. You can also monitor performance, view fault monitoring details, and download and activate the latest available software package for SVO.

Shelf Virtualization Orchestrator (SVO) is a node-level software solution that addresses multishelf scalability issues and provides node aggregation functions. The SVO solution runs on the SVO card that is installed in the NCS 2006 or NCS 2015 chassis.

The SVO solution introduces a NETCONF interface with Cisco YANG models and a SVO web user interface from R12.0. The web user interface is also referred to as the nodal craft.

The NETCONF/YANG interface is used by network management systems such as Cisco Evolved Programmable Network Manager (EPNM) whereas the SVO web user interface is used to install and troubleshoot.

The SVO solution works in high availability (HA) mode. Each SVO card can have combination of SVO instances that can be in primary or secondary mode. The card running the SVO ROADM primary instance is the main card that monitors and handles the SVO admin plane, networking, and so on.

The SVO solution provides a mechanism for collecting alarms from the subtended NCS 2006 and NCS 2015 nodes and then forwards them to the NETCONF interface. The alarms that are generated by SVO provide the actual root cause of the failure to the end user.

The SVO solution supports:

- One ROADM SVO instance with up to 50 NCS 2006 chassis and 20 NCS 2015 chassis

- 15 OLA SVO instances in Release 12.3 and earlier
- 20 OLA SVO instances in Release 12.3.1

SVO Web User Interface

The SVO web user interface (UI), also called the nodal craft, is designed to manage the NCS 2000 network elements and replaces CTC. The SVO web UI runs on the browser without the need to download any JAR or Java files. The SVO web UI can be used across multiple operating systems and browsers.

The SVO web UI performs the following functions:

- Manages the chassis, cards, and passive devices
- Manages alarms, faults, and conditions
- Manages users and user profiles
- Administers devices
- Troubleshoots issues
- Provides a seamless user experience with Cisco Evolved Programmable Network Manager (EPNM)

Note When multiple web UI sessions are open, and there are changes in the card status, it is possible that these changes are not updated correctly in some of the web UI sessions. In such situations, you can refresh the web UI page, and confirm if the expected and actual card states are the same.

Log into the SVO Web Interface

Use this task to log into the SVO web interface (SVO instance).

Procedure

Step 1 In the browser URL field, enter the IP address of the SVO instance.

The IP address to be used is the management IP address that is configured in the Create an SVO Instance, on page 46 task.

The SVO login page appears.

Step 2 Enter the username and password.

Note Use the credentials (configured in the Create an SVO Instance, on page 46 task) to log into a SVO instance.

Step 3 Click **Login**.

Log into the SVO Web Interface Using EPNM

From R12.0.1 onwards, SVO provides single sign-on (SSO) support when accessed from EPNM.

For releases before R12.0.1, if the SVO has not configured an SSO server, EPNM users can launch SVO web interface, but users must enter the username and password to log into the SVO web UI.

From R12.0.1 onwards, SVO enables you to configure SSO authentication for some predefined users to add an SSO user and enable SSO authentication. For more information, see Add an SSO User, on page 68 and Enable SSO, on page 69. EPNM users whose SSO is configured can open the SVO web UI without logging in again.

From R12.1 onwards, SVO web user interface allows you to configure Single Sign On (SSO) capability from EPNM. This allows you to redirect from EPNM to SVO without additional sign-on request. For example, if you have a specific alarm present in EPNM and when you click that alarm from EPNM, you can directly navigate to that specific alarm page or global alarm page of SVO. Ensure that the EPNM is configured for SVO navigation pages and SSO is enabled on SVO.

Use this task to start SVO from EPNM.

Before you begin

Enable SSO, on page 69

Procedure

Step 1 From the left sidebar of EPNM, choose **Inventory** > **Device Management** > **Network Devices**.

The **Network Devices** page appears.

Step 2 From the **Network Devices** list, click the SVO instance you want to start.

The SVO web interface dashboard appears directly without prompting for SVO login credentials.

Add an SSO User

Use this task to add an SSO user. Only an admin or superuser can add SSO users.

Ensure that both SSO users and other users must be different.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **SSO** tab.

The SSO Configuration dialog box appears.

Step 3 In the **SSO Users** area, perform these steps:

a) Click the + button.

The **SSO Users** dialog box appears.

b) Enter the username in the **Username** field.
c) Choose the user group from the **User Group** drop-down list.

The options are Viewer and Editor. The Viewer when mapped for SSO, can only view the SVO configurations. The Editor when mapped for SSO, can configure devices.

Step 4 Click **Apply**.

A confirmation message appears.

Step 5 Click **Yes**.

Enable SSO

Use this task to enable SSO. Only an admin or superuser can enable SSO.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **SSO** tab.

The SSO Configuration dialog box appears.

Step 3 In the **SSO** page, perform these steps:

a) Check the **Enable SSO** check box to enable SSO on SVO.
b) Enter the EPNM server IP address in the **IP Address** field.
c) The default port number is 443. You can change the port number using the **Port** field, .

Step 4 Click **Apply**.

A confirmation message appears.

Step 5 Click **Yes**.

SVO Views

The SVO Topology page helps you access the topology in two different views:

- The Logical or Tree View (default)
- The Tabular or Table View

The logical or tabular view allows you to view and manage the NCS 2006 and NCS 2015 nodes connected to the SVO controller.

You can access the tabular view by clicking the **Table** toggle button in the logical view. You can access the logical view by clicking the **Tree** toggle button in the Tabular View.

You can display or hide the left panel in either view by using the toggle button on the top-right of the SVO topology page.

Both views allow you to add additional racks to the topology by clicking **Add Rack**.

Logical View

The left panel of the logical view contains the list of racks and the SVO cards. You can navigate to the nodes in the network by clicking the node or chassis name from the expanded rack view in the left panel or by clicking the node from the logical view. When you hover over a node in the logical view, the chassis type and alarm details are displayed. You can zoom in or zoom out the view by clicking the + and - symbols.

Tabular View

The tabular view displays two lists:

- The Chassis List table lists the IDs of the nodes, chassis type, Rack ID, and Description.
- The SVO List table lists the SVO ID, Chassis ID, Chassis type, Rack ID, and State.

You can navigate to the nodes in the network by clicking the chassis name from the expanded rack tree view in the left panel or by clicking the ID of the chassis in the Chassis List or the Chassis ID in the SVO List.

Note When you navigate between the rack or chassis view, especially on larger nodes and low connection speeds, the information on the right panel of the alarms pane displays before the images on the left panel. The loading spinner is only present until the information on the right panel displays. However, the SVGs (images) on the left panel takes some more time to display the racks and cards.

Note In conditions panel while fetching conditions, sometimes *Applying configuration* follows the fetching data spinner, even though there is no configuration change happening.

Note From R12.3.1 onwards, you can view the NCS 2002 chassis and panels with names. You can add a card to the chassis and delete the existing card in the chassis.

Open the Card View

Use this task to open the card view.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Navigate to the chassis view using any one of the following steps:

- Click the chassis icon in the logical view.
- Click the ID in the Chassis List or the Chassis ID in the SVO List in the tabular view.
- Click the rack ID in the left panel to open the rack view and identify the chassis of interest.
- Click the chassis name in the expanded rack tree view in the left panel.

Step 3 Click the slot that contains the card, and click **Open Card**.

The card view appears.

Card and Port Status LED

This chapter describes the different LED colors available on a card and a port for indicating status.

Table 9: Feature History

Feature Name	Release Information	Feature Description
Card and Port Status LED	Cisco NCS 2000 Release 12.3.1	You can now accurately identify the status of a card and a port through different LED colors. A card has following color indicators: • Green- active; represents card is operational • Red- inactive; represents hardware issue • Amber- inactive; represents signal fail and loss of frame In addition to the gray color, which indicates the inactive state of a port, A port has following color indicators: • Green- active • Red- inactive; represents availibility of major alarms • Yellow- active; represents availibility of minor alarms

Card LED and Port LED

Card LED

Each card faceplate has following three card-level LED indicators:

LED Color	Card Status
Green	Active (ACT LED)
Amber	Inactive; represents a signal failure (SF) or conditions such as loss of frame and high bit error rate
Red	Inactive; represents a hardware failure (FAIL LED)

Port LED

For a port, the available color indicators are:

LED Color	Port Status
Green	Active

LED Color	Port Status
Yellow	Active with minor alarms
Red	Inactive with major alarms and conditions

Create a Rack

Use this task to add a rack.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click **Add Rack**.

The Add rack dialog box appears.

Step 3 Enter a rack ID in the **Rack ID** field.

You can enter any value from 1 through 32767.

Step 4 Click **Apply**.

The rack is added to the left panel.

Add a Chassis

Use this task to add a chassis to the rack. The chassis types are:

- NCS2015-ANSI
- NCS2015-ETSI
- NCS2006-ANSI
- NCS2006-ETSI
- NCS2K-MF-6RU
- NCS2K-MF10-6RU

The NCS2K-MF-6RU and NCS2K-MF10-6RU types are passive chassis.

Before you begin

- Log into the SVO Web Interface, on page 67
- Create a Rack, on page 73-Complete this task if no racks are available in the left panel or the existing racks are full.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel, where you want to add the chassis.

The rack view appears.

Step 3 Left-click an empty slot in the rack.

Step 4 Click **Add Chassis**.

Step 5 From the **Select Device** drop-down list, choose the node.

Step 6 From the **Select Chassis** drop-down list, choose the chassis to add to the rack.

Step 7 From the **Enter Chassis ID** drop-down list, choose the chassis ID.

Step 8 (Optional) Enter a name for the chassis in the **Display Name** field.

Step 9 Click **Provision**.

The chassis is added to the rack.

Add a Card to the Chassis

Use this task to add a card to the NCS 2006 or NCS 2015 chassis.

The following table lists the cards supported by the latest release of SVO.

TNCS	OPT-AMP-C	CFP-LC
TNCS-O	OPT-EDFA-17	MR-MXP
TNCE	OPT-EDFA-24	10x10G-LC
TSCE	100GS-CK-C	100G-CK-C
TNCS-2	200G-CK-C	16-AD-CCOFS
TNCS-2O	400G-XP	20-SMRFS
TNC	100G-LC-C	9-SMR17FS
9-SMR24FS	9-SMR34FS	20-SMRFS-CV
RAMAN-CTP	RAMAN-COP	EDRA1-26C

EDRA1-35C	EDRA2-26C	EDRA2-35C
1.2T-MXP	40E-MXP-C	40EX-MXP-C
40ME-MXP-C	80-WXC-C	OPT-PRE
OPT-BST	OTU2-XP	OPT-AMP-17C
OPT-EDFA-35	OSC-CSM	RMN-CTP-CL
40-SMR1-C	40-SMR2-C	6AD-DD-CFS
OPT-BST-E	OPT-AMP-17-C	PSM

Before you begin

- Log into the SVO Web Interface, on page 67
- Add a Chassis, on page 73

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the empty slot in the chassis where you want to add the card.

Step 4 From the **Slot** drop-down list, choose the card that you want to provision.

Step 5 Click **Provision** to add the card to the chassis.

Reposition a Chassis

This topic describes how you can change the location of a chassis in a rack.

Table 10: Feature History

Feature Name	Release Information	Feature Description
Reposition a Chassis	Cisco NCS 2000 Release 12.3	This topic describes the procedure required to reposition a chassis in a rack.

Repositioning a Chassis

Use this task to reposition a chassis in a rack.

Before you begin

Log into the SVO Web Interface, on page 67

Add a Chassis, on page 73

Procedure

Step 1 Select the chassis you want to reposition.

A dialog box appears.

Step 2 Select **Cut** from the dialog box.

The selected chassis is ready to be pasted in a new position.

Step 3 **Paste** the selected chassis in the appropriate rack.

You can paste the chassis inside the same rack or in a different rack.

Note If required space is not available in the position where you want to paste the chassis, the **Paste** button will be disabled and you will receive **Not enough space to paste this element** message.

If you wish to stop the operation in the middle, press the ESC key on your keyboard.

Inventory

The **Inventory** tab lists the inventory information of all the racks and chassis used on the network.

View Inventory Information

Use this task to view inventory information.

If the user attempts to navigate to the **Inventory** tab immediately after login, the Inventory tab might be empty. Refresh the table to retrieve the inventory information.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Perform this step, as needed.

a) To view inventory information of all the racks and chassis used on the network, perform this step:

1. Click the hamburger icon at the top-left of the page, and select **Inventory**.

b) To view inventory information of the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.
2. Click the rack in the left panel.

   The rack view appears.
3. Select the **Inventory** tab.

c) To view inventory information of the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.
2. Click the rack in the left panel.

   The rack view appears.
3. Left-click the chassis, and select **Open**.

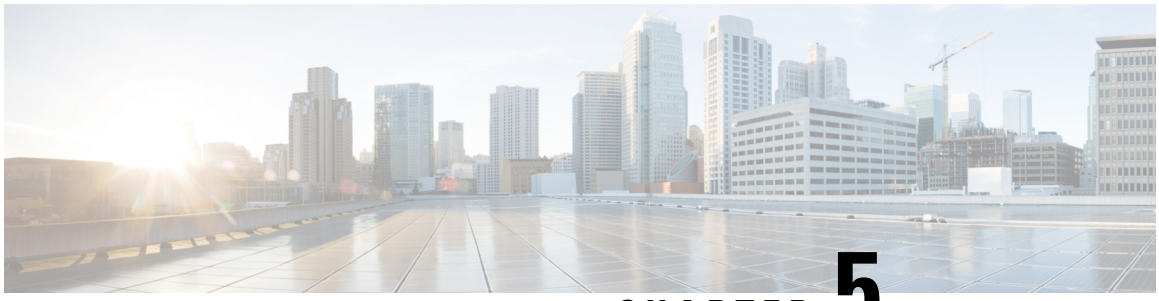
   The chassis view appears.
4. Select the **Inventory** tab.

The Inventory page appears. You can view the following inventory details.

- **Location**—Identifies where the equipment is installed.
- **UID**—Displays the unique identifier of each component.
- **Display Name**—Displays the display name of each component.
- **Eqpt Type**—Displays the type of equipment.
- **Eqpt State**—Displays the state of each component.
- **Admin State**—Displays the current administrative state of each component.
- **Service State**—Displays the current service state of each component.
- **Connected To**—Displays the passive unit associated with the USB port of the chassis.
- **Actual Eqpt Type**—Displays the specific card name.
- **Serial No**—Displays the equipment serial number.
- **Product ID**—Displays the manufacturing product identifier.
- **HW Part No**—Displays the hardware part number.
- **CLEI Code**—Displays the Common Language Equipment Identifier (CLEI) code.
- **Version ID**—Displays the manufacturing version identifier.
- **HW Rev**—Displays the hardware revision number.

- **Boot ROM Rev**—Displays the boot read-only memory (ROM) revision number.

Step 2 (Optional) Click the **Export to Excel** icon to download the inventory information to an Excel sheet.



CHAPTER 5

Manage Users

This chapter describes the different types of users in Cisco NCS 2000 SVO. This chapter also describes the tasks to manage users.

Table 11: Feature History

Feature Name	Release Information	Feature Description
View Users	Cisco NCS 2000 Release 12.2	This feature allows an admin or superuser to view the details of users who have successfully logged into SVO.

User Groups

User groups are system-defined. The users in each group have certain levels of privileges and permissions and can perform a defined set of tasks.

The system-defined user groups are:

- Superuser—A user assigned to this group has special permissions to perform any action on the system. The superuser has access to the SVO Admin Plane and the SSH interface. Superusers can create, modify, and delete users. Only one superuser can be created.
- Admin—A user assigned to this group has read and write permissions. An admin can create, modify, and delete users.
- Editor—A user assigned to this group has limited read and write permissions. An editor does not have permissions to create and manage users.

- Viewer—A user assigned to this group has only read permission. A viewer cannot perform any action on the device.

Role-Based Access Control

Table 12: Feature History

Feature Name	Release Information	Feature Description
Role-Based Access Control	Cisco NCS 2000 Release 12.3	The Role-Based Access Control (RBAC) feature allows the users belonging to the Editor, Admin, and Viewer groups to access and operate certain SVO panes.

Role-Based Access Control (RBAC) restricts or authorizes system access for users by setting permissions and privileges. Users are assigned roles depending on the resources to which they need access.

RBAC allows users belonging to the Editor, Viewer, and Admin groups to access and operate certain SVO panes as detailed below:

- **Viewer group**: You can
  - Refresh a page or pane.
  - Export reports.
  - View options in panes.

Note However, the changes cannot be applied.

- **Viewer and Editor groups**: You can perform all operations except for viewing the **Users & Access** menu when the hamburger icon at the top-left of the page is clicked.
- **Viewer and Admin groups**: Access is restricted based on the instance type. In the TXP instance:
  - For the **Node Configuration** > **Optical Configuration** menu, the **Connection Verification**, **OTDR**, **Internal Patch Cords**, **OSC**, **Optical Degree**, **Optical Degree Power Monitoring**, **Span Loss**, **Expected Input Power**, and **Fiber Attributes** tabs are not accessible.
  - The **Node Configuration** > **APC** tab is not accessible.
  - The **Provisioning** > **Raman Amplifier** tab in the card view is not accessible.

External Authentication Users for SVO

In SVO, the following users are created to manage SVO provisioning activities:

- Local users (local authentication)—Specifies users created to manage SVO instances.

- External users (external authentication)—Specifies users created on the external authentication servers.

The local and external users are mutually exclusive, for example, if there is a local user as **user1** configured on SVO, then another external user with same name **user1** is not allowed to login.

The RADIUS or TACACS user who is created on the RADIUS or TACACAS server should have the *Cisco-AVPair* reply attribute that is configured for each user on SVO to authenticate.

The following table lists the server attribute mapped to user privileges supported on SVO.

Table 13:

Cisco-AVPair Reply Attribute	Value mapped in RADIUS Server	Value mapped in TACACAS Server
shell:priv-lvl=	3	3
shell:priv-lvl=	0	0
shell:priv-lvl=	1	1

Create Users

Use this task to create users. Only an admin or superuser creates new users. Superusers cannot be created using this task.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, click **Create**.

The Create User dialog box appears.

Step 3 Enter the following details.

a) **User Name**—Type the user name. The user name must be a minimum of six and a maximum of 40 characters. It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot).

b) **Password**—Enter the password which will be used by the user while logging into the system. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters. The minimum number of characters in the password is eight and the maximum number is 127. The password must not contain the user name.

c) **Retype Password**—Retype the password.

d) **Full Name**—Enter the full name of the user.

e) **Expiry Time (days)**—Enter the time period in days before which the user needs to change the password. For example, if the user has set the expiry time to be 20 days, the user must change the password before 20 days are over.

The user is automatically moved to the Change Password group after the time period in the Expiry Time field elapses. The user must change the password before performing any other action.

f) **Warning Before Expiry (days)**—Enter the number of days the user is warned of the expiry of the password.
g) **Max Retry Number**—Enter the number of maximum retries for the user. The user is logged out of the system if the password is incorrectly entered after this number of attempts is reached.
h) **Group**—Select the group from the drop-down list. The available options are admin, editor, and viewer.

Step 4 Click **Create**.

The new user is added to the list.

Change Password

Use this task to change password for the user. Only an admin or superuser can change the password.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, check the check box corresponding to the user you want to change the password, and click **Reset Password**.

The **reset** *Username* **password** dialog box appears.

Step 3 Enter the new password in the **New Password** field.

The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters. The minimum number of characters in the password is eight and the maximum is 127. The password must not contain the user name.

Step 4 Retype the same password in the **Retype Password** field.

Step 5 Click **Reset Password**.

A confirmation message appears.

Step 6 Click **OK**.

View Users

Use this task to view users. Only an admin or superuser can view the activities of users.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, click **Login**.

The **Last Successful Logins** dialog box appears.

Step 3 View the displayed details in the **Last Successful Logins** tab.

- **Login ID**—Displays the session ID.
- **User**—Displays the user name.
- **Last Login Date**—Displays the date and time on which the user had last logged in.
- **Last Logout Date**—Displays the date and time on which the user had last logged out.
- **Interface**—Displays the interface type that the user used to last log in. The interface types are web UI, CLI, NETCONF, and Unknown.

Delete Users

Use this task to delete users. Only an admin or superuser can delete users.

Note Superusers cannot be deleted.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, check the check box corresponding to the user you want to delete and click **Delete User**.

A confirmation message appears.

Step 3 Click **Yes**.

Modify User Settings

Use this task to change the user settings.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the User icon at the top-right of the page, and select **Users & Access**.

The **User Login Details** and **User Configurations** tabs appear.

Step 2 View the displayed details in the User Login Details tab.

- **Last Login Date**—The date on which the user had last logged in.
- **Last Logout Date**—The date on which the user had last logged out.
- **Last Login Interface**—The interface used for last login.
- **Number of Failed Login Attempts**—The number of times the user has had failed login attempts before the current login.
- **Last Failed Login Message**—The reason for the last login failure.
- **Warning Message**—The message displays the number of days remaining for the expiry of the current password.

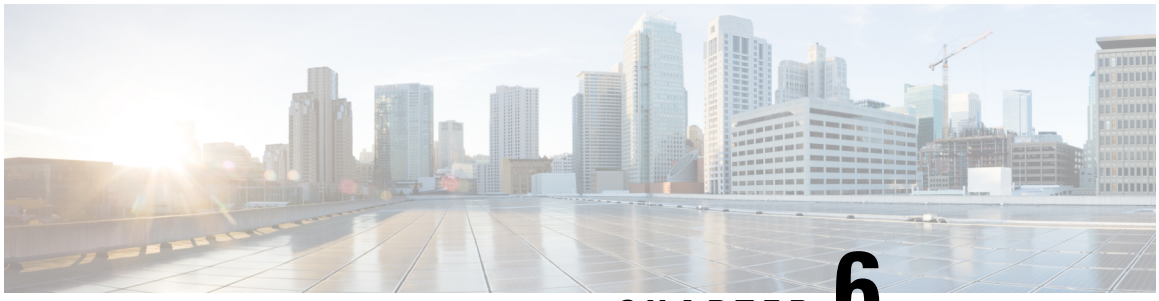
Step 3 To change the user attributes, go to the **User Configurations** tab. The following attributes can be changed by a superuser or an admin user except the user name.

- **User Name**—Displays the user name.
- **Group**—The original group a user was created in. An admin or a superuser can change the group to which a user belongs. Also, when a user has reached the set **Expire Time**, the user is moved automatically to the Change Password user group. The user must change the password before performing any other action on the system.
- **Full Name**—Displays the full name of the user.
- **Max Retry Number**—The number of times the user can attempt to login. The default value is 3.
- **Expire Time (days)**—The number of days the current password is valid. The default value is 180.
- **Warning Before Expire (days)**—The user is warned about the number of days remaining before the expiry of the current password. The value entered for this field must be lesser than the value entered for the **Expire Time** field. The default value is 14.

Step 4 Click **Apply**.

A confirmation message appears.

Step 5 Click **Yes**.



CHAPTER 6

Manage External Authentication

This chapter describes the tasks related to external authentication in Cisco NCS 2000 SVO.

Manage External Authentication

From 12.1 onwards, SVO supports RADIUS and TACACS modes of external authentication. Ensure that you enable and use either RADIUS or TACACS authentication method. You can add a maximum of up to ten servers for each of RADIUS or TACACS on SVO.

There should be at least one RADIUS or TACACS authentication server that is configured for authentication to be enabled. In order to delete the last RADIUS or TACACS server, you must disable the external authentication first, and then delete the RADIUS or TACACS server.

When your login to SVO with the external authentication enabled, SVO first tries with the configured list of servers. If external authentication servers are not reachable, then SVO uses local authentication provided the local authentication is enabled on SVO.

To manage SVO, the following users are created:

- Local users (local authentication)—Specifies users who are created to manage SVO instances.
- External users (external authentication)—Specifies users who are created on the external authentication servers.

For more information related to users, see External Authentication Users for SVO, on page 80.

The following table lists some external authentication scenarios that describe some possible authentication errors, causes, and actions.

Table 14: External and Local Authentication Scenarios

External and Local Authentication Combination	Possible Authentication Scenario	Possible Cause	Action to be Taken
• External Authentication Enabled and Local Authentication Disabled	Server denies authentication	External username or password is incorrect	Enter the correct username and password to log in to the system
	Server not reachable	IP address, shared secret or port number is not configured correctly although username or password could be correct	You are locked out of the system. Ensure that you have configured correct IP address, shared secret, and port number
• External authentication enabled and Local authentication enabled	Server denies authentication (although location authentication is enabled)	External username or password is incorrect	Enter the correct username and password to log in to the system Local authentication only works when the RADIUS or TACACS external servers are not reacheable
	Server not reachable (Local authentication is enabled)	IP address, shared secret, port number is not configured correctly although username or password could be correct	Use local authentication credentials to log in to SVO

Limitations for RADIUS or TACACS Authentication

- In Release 12.1, an external user list is maintained with username and its respective group (admin, editor, or viewer). The user list is populated whenever a new username is successfully authenticated. This user list is limited to 500 users. The delete (-) button available under the **External Authentication** tab is activated when 450 users limit is reached. Whenever you click the delete (-) button, the external users are cleared. In the user list, if the user limit is reached (500 users), then the new external user (501^{th} external user) cannot login to SVO.

  If you are logged in as external user and cleared the list, ensure that you must relogin on all the logged-in sessions. If you do not relogin, the system might not respond properly and information might not appear properly.

- In Release 12.1 external authentication is applicable only on SVO web user interface. External authentication using logging into the Netconf console is not supported.

RADIUS Authentication

Use the following tasks to manage RADIUS authentication on SVO.

Note Only an admin or superuser can manage RADIUS authentication on SVO.

1. Create RADIUS Server Entry on SVO, on page 89
2. Enable RADIUS Authentication, on page 90
3. Modify RADIUS Server Parameters, on page 90
4. Disable the RADIUS Authentication, on page 91
5. Delete the RADIUS Server from SVO, on page 91

Create RADIUS Server Entry on SVO

Use this task to create RADIUS server entry on SVO. Only an admin or superuser can add RADIUS server.

Before you begin

Log into the SVO Web Interface, on page 67

Ensure that you have added SVO instances with RADIUS IP addresses in the Cisco Secure ACS server.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, perform the following steps:

a) Click the + button.

The **Create RADIUS server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the RADIUS server.
- **IP Address**—IPv4 or IPv6 address of the RADIUS server.
- **Authentication Port**—1812 is default for RADIUS. The range is from 0 to 65535. RADIUS server must be running on the port that is configured.
- **Shared Secret**—Shared secret configured on the RADIUS server.
- **Confirm Shared Secret**—Confirm the above shared secret for the RADIUS server.

c) Click **Add**.

The RADIUS server is added to the RADIUS server list on SVO.

Enable RADIUS Authentication

Use this task to enable RADIUS authentication. Only an admin or superuser can enable RADIUS authentication. You can add upto ten RADIUS servers on SVO.

Before you begin

- Log into the SVO Web Interface, on page 67
- Create RADIUS Server Entry on SVO, on page 89

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, perform the following steps:

a) Check the **Enable RADIUS Authentication** check box to enable RADIUS server on SVO.

b) Check the **Enable node as final authentication when RADIUS server is reacheable** check box to enable the RADIUS server as a final authentication option.

Note When you enable external authentication, local authentication is enabled by default to avoid lock out scenarios (such as configuration errors). Until external authentication is enabled, local authentication can be enabled or disabled based on your requirement.

c) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the RADIUS server before retrying to contact the server.

d) In the **Attempts** field, enter the number of attempts to contact the first RADIUS server in the authentication list. If there is no response after the allotted number of attempts, then SVO tries to contact the the next RADIUS server in the list.

Step 4 Click **Apply**.

Modify RADIUS Server Parameters

Use this task to modify RADIUS authentication settings. Only an admin or superuser can modify RADIUS server settings.

Before you begin

Log into the SVO Web Interface, on page 67 and Create RADIUS Server Entry on SVO, on page 89

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, select the RADIUS server to edit from the list of available RADIUS servers and perform the following tasks:

a) Click the edit icon.

The **Modify RADIUS server** dialog box appears.

b) Edit the following fields:

- **IP Address**
- **Authentication Port**
- **Shared Secret**
- **Confirm Shared Secret**

c) Click **Save**.

Disable the RADIUS Authentication

Use this task to disable RADIUS authentication.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the External Authentication tab.

The External Authentication window appears.

Step 3 In the RADIUS Configuration area, perform the following steps:

a) Uncheck the **Enable RADIUS Authentication** check box to disable RADIUS authentication on SVO.

b) Uncheck the **Enable node as final authentication when RADIUS server is reacheable** check box to disable the RADIUS server as a final authentication option.

Note When external authentication is disabled, then local authentication is disabled by default.

Step 4 Click **Apply**.

Delete the RADIUS Server from SVO

Use this task to delete the RADIUS server entry from SVO.

Before you begin

Disable the RADIUS Authentication, on page 91

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **RADIUS Configuration** area, select the RADIUS server to delete and click the **-** button.

A confirmation message appears.

Step 4 Click **Yes**.

Dual Factor Authentication

SVO external authentication is enhanced to support challenge-response based authentication using RSA Secure login with the Cisco Secure ACS server. The dual factor authentication provides secure way of authentication using passcode and token system. RSA provisioning is performed on the RADIUS server and the user-level access privileges are configured and maintained on the RADIUS server.

Note RSA configuration is not supported on the TACACS server.

Challenge Response RSA Authentication

In the SVO login page, enter username and passcode or token passcode, and click **Login**.

Based on scenarios (whether the user logged in for the first time or has been locked out), and if a **Challenge/Response** dialog box appears, then you must enter the new soft token PIN in the **Response** field and then click **Ok**.

If username is configured for RSA authentication, then RADIUS passes on user information to the RSA server.

RSA server validates the User ID and associated token. RADIUS passes info to SVO and user can log in through SVO with token and the username.

RSA Authentication Scenarios

RSA Authentication Using the New PIN Mode

To log in to SVO using new PIN mode, follow the procedure:

1. For a user with the dual factor authentication configured on the Cisco Secure ACS server, enter username and token code (code that is generated by the RSA token code generator) (without a PIN as the PIN is not generated).
2. Once you click the **Login** button, the **Challenge/Response** dialog box appears. In the **Challenge/Response** dialog box, enter the PIN based on the policy that is configured on the RSA server.

3. Once the PIN is sent, then there is an additional confirmation dialog box appears. Renter the same PIN and you can log into SVO.

RSA Authentication Using the New Token Mode

Next Token mode is applied when the authentication process requires an additional verification of the token code. In this mode, you are notified to enter the next token code. For example, you must wait for the number that is displayed on the passcode or token code generator to change, and then enter the new number (without the PIN).

To log in to SVO using the new token mode, follow the procedure:

1. Enter the user ID.
2. Enter the passcode (enter your PIN, Press Next arrow button, and the passcode appears on the token generator).
3. Wait until your token code changes. When prompted, enter the new token code.

RSA Authentication Using the Normal Login Mode

To log in to SVO using the normal login mode, follow the procedure:

1. PIN is generated. Enter the username and the PIN in the passcode generator.
2. Copy the passcode code and paste the passcode code in the password field of SVO, and click **Login**.

TACACS Authentication

Use the following tasks to manage TACACS authentication.

Note Only an admin or superuser can manage TACACS authentication on SVO.

1. Create TACACS Server Entry on SVO, on page 93
2. Enable TACACS Authentication, on page 94
3. Modify TACACS Server Parameters, on page 95
4. Disable the TACACS Authentication, on page 96
5. Delete the TACACS Server from SVO, on page 96

Create TACACS Server Entry on SVO

Use this task to create TACACS server entry on SVO. Only an admin or superuser can add TACACS server. You can add upto ten TACACS server.

Before you begin

Log into the SVO Web Interface, on page 67

Ensure that you have added SVO instances with TACACS IP addresses in the Cisco Secure ACS server.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS** Configuration area, perform the following steps:

a) Click the **+** button.

The **Create TACACS server Entry** dialog box appears.

b) Enter the following fields:

- **Name**—Name of the TACACS server.
- **IP Address**—IP address of the TACACS server.
- **Authentication Port**—49 is default for TACACS. TACACS server must be running on the port that is configured.
- **Shared Secret**—Shared secret configured on the TACACS server.
- **Confirm Shared Secret**—Confirm the above shared secret for the TACACS server.

c) Click **Add**.

The TACACS server is added to the TACACS server list on SVO.

Enable TACACS Authentication

Use this task to enable TACACS authentication.

Before you begin

- Log into the SVO Web Interface, on page 67
- Create TACACS Server Entry on SVO, on page 93

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, perform the following steps:

a) Check the **Enable TACACS Authentication** check box to enable TACACS server on SVO.

b) Check the **Enable node as final authentication when TACACS server is reacheable** check box to enable the TACACS server as a final authentication option.

Note When you enable external authentication, local authentication is enabled by default to avoid lock out scenarios (such as configuration errors). Until external authentication is enabled, local authentication can be enabled or disabled based on your requirement.

c) In the **Timeout (seconds)** field, enter the time interval (seconds) to wait for a response from the TACACS server before retrying to contact the server.

d) In the **Attempts** field, enter the number of attempts to contact the first TACACS server in the authentication list. If there is no response after the allotted number of attempts, then SVO tries to contact the the next RADIUS server in the list.

Step 4 Click **Apply**.

Modify TACACS Server Parameters

Use this task to modify TACACS authentication settings. Only an admin or superuser can modify TACACS server settings.

Before you begin

Log into the SVO Web Interface, on page 67 and Create TACACS Server Entry on SVO, on page 93

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External** Authentication tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, select the TACACS server to edit from the list of available TACACS servers and perform the following tasks:

a) Click the edit icon.

The **Modify TACACS server** dialog box appears.

b) Edit the following fields:

- **IP Address**
- **Authentication Port**
- **Shared Secret**
- **Confirm Shared Secret**

c) Click **Save**.

Disable the TACACS Authentication

Use this task to disable TACACS authentication.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, perform the following steps:

a) Uncheck the **Enable TACACS Authentication** check box to disable TACACS authentication on SVO.

b) Uncheck the **Enable node as final authentication when TACACS server is reacheable** check box to disable the TACACS server as a final authentication option.

Note When external authentication is disabled, then local authentication is disabled by default.

Step 4 Click **Apply**.

Delete the TACACS Server from SVO

Use this task to delete the TACACS server entry from SVO.

Before you begin

Disable the TACACS Authentication, on page 96

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Access Configuration**.

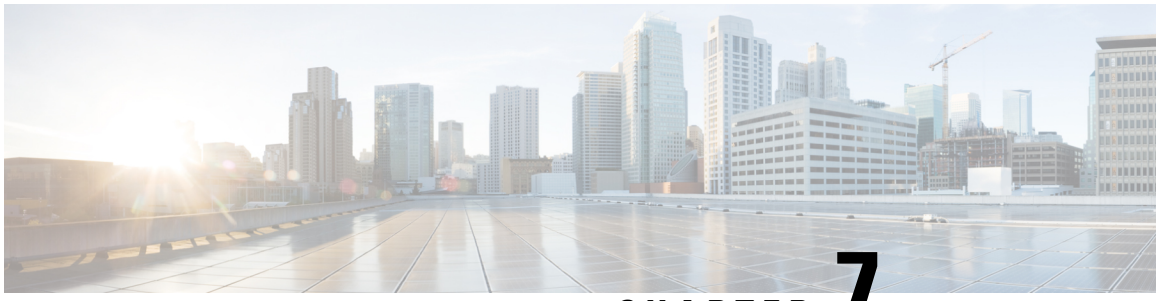
Step 2 In the **Access Configuration** window, click the **External Authentication** tab.

The **External Authentication** window appears.

Step 3 In the **TACACS Configuration** area, select the TACACS server to delete and click the **-** .

A confirmation message appears.

Step 4 Click **Yes**.



CHAPTER 7

Configure Devices

This chapter describes the tasks related to device configuration in Cisco NCS 2000 SVO.

Manage Authorization Groups

Use this task to create, edit, or delete authorization groups for devices.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

Step 2 Click the **Authorization Group** tab.

A table appears that lists the authorization groups.

Step 3 Perform these steps, as needed:

a) To create a new authorization group, perform these steps:

1. Click the **Add Auth Group** icon.

   The **Add Authorization Group** dialog box appears.

2. Enter the Auth Group Name, Remote User Name, and Remote Password in their respective fields.

3. Click **Add**.

   The new auth group is added to the table.

b) To edit an authorization group, perform these steps:

1. Check the check box that is next to the auth group you want to edit.
2. Click the **Edit Auth Group** icon.

   A warning message appears informing the user that there may be loss in device communication.
3. Click **OK**.

   The **Edit Authorization Group** dialog box appears.
4. Edit the fields, as needed.

   Note The auth group name cannot be edited.
5. Click **Edit**.

   The details are updated.

c) To delete an authorization group, perform these steps:

1. Check the check box that is next to the auth group you want to delete.
2. Click the **Delete Auth Group** icon.

   A confirmation message appears.
3. Click **OK**.

   The auth group is deleted from the table.

Manage Devices

Use this task to add, synchronize, or delete devices.

Note Only one NCS 2000 device can be added to an SVO instance.

Note SVO line card is automatically added as a device. It is listed as svo-primary in the non-high availability mode, and as svo-primary and svo-secondary in the high availability mode.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

Step 2 Click the **Devices** tab.

A table appears that lists all the devices that are configured.

Step 3 Perform these steps, as needed:

a) To create a new device, perform these steps:

1. Click the **Add Device** icon.

   The Add Device dialog box appears.

2. Choose the **Device Type** from the drop-down list.
3. Enter the Device Name and IP Address in their respective fields.
4. Select an auth group from the drop-down list.
5. Click **Add**.

   The new device is added to the table.

b) To delete a device, perform these steps:

1. Check the check box that is next to the device you want to delete.
2. Click the **Delete Device** icon.

   A confirmation message appears.

3. Click **OK**.

   The device is deleted from the table.

c) To synchronize a device, perform these steps:

1. Check the check box that is next to the device you want to sync.
2. Click the **Sync Selected Devices** icon.

   The **Sync Status** field displays one of the following statuses:

   - sync-not-started—Device is waiting for the start of the synchronization process.
   - full-sync-requested—A full data synchronization of the device is requested by the user to recover from an error.
   - sync-configuration—Device is synchronizing the configuration parameters.
   - sync-operational—Device is synchronizing the operational parameters.
   - sync-completed—Device is fully synchronized.
   - sync-mea—Device cannot be synchronized because it is different from the SVO topology.

Note The **Sync Status** field does not display the status of the SVO card.

SOCKS Proxy

Table 15: Feature History

Feature Name	Release Information	Feature Description
SOCKS Proxy	Cisco NCS 2000 Release 12.2	Socket Secure (SOCKS) is a standard proxy protocol for IP-based applications developed by IETF. SOCKS Proxy feature allows the SVO node to access remote NCS 2000 nodes using SOCKS Proxy server.

Socket Secure (SOCKS) is a standard proxy protocol for IP-based applications developed by IETF. SOCKS Proxy feature allows the SVO node to access remote NCS 2000 nodes using SOCKS Proxy server. You can set the SOCKS proxy server as an External Network Element (ENE) or a Gateway Network Element (GNE).

Benefits

- SOCKS Proxy is used when the SVO node cannot connect directly to the remote NCS 2000 node through DCN.
- It is mandatory to use SOCKS Proxy if IPv6 is enabled on NCS 2000 nodes.
- OSPF need not be enabled to propagate the routes as routing to the remote node is done by the SOCKS Proxy server.
- SOCKS Proxy allows the SVO node to connect to remote nodes behind the firewall of a GNE.

Limitations

- A SOCKS Proxy server must be used only to connect to small remote nodes (OLA nodes).
- A SOCKS Proxy server must serve only up to five NCS 2000 nodes.

Configure External Switch

Use this task to configure the external switch in the ROADM or OLA instance in the SVO card model. You can add up to a maximum of two external switches. External server model does not support the external switches.

Before you begin

- To view the network configuration in the admin plane:
  - Log into the Cisco SVO Admin Plane, on page 42.
  - Click **Network** in the left panel and choose **Configuration**.
  - Ensure that the IP address of the external switch to be added, is in the subnet of the HOST NIC IP address that is present in the Devices Network section of the network.yml configuration file. If the switch IP address is not in the subnet, reset the SVO card to factory default, using the task Restart Admin Plane, on page 51, reinstall the SVO software, and upload the proper network.yml configuration file.
- Ensure that the external switches have appropriate initial configuration and cabling.
- Log into the SVO Web Interface, on page 67.
- Create Authorization group for the external switches and NCS 2000 devices. See Manage Authorization Groups, on page 99.
- Add the External Switches. See Manage Devices, on page 100.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

Step 2 Click the **Networking** > **Switch Configuration** tabs. There are three options available in the drop-down list.

a. Managed—The switch is present and managed.

b. Not Managed—The switch is present and not managed.

c. None—The switch is not present and managed.

a) (Only ROADM instance) Choose **Managed** from the drop-down list:
b) (Only OLA instance) Choose **Not Managed** from the drop-down list:
c) Click **Apply**.

A confirmation message appears.

d) Click **Yes**.

Step 3 (Only ROADM instance) Click the **External Switch Configuration** tab.

a) Click the **Add** icon.

The **Add External Switch** dialog box appears.

b) Select the switch that you added from the **Device** drop-down list.
c) Enter the **IP Address** and the **Subnet Address Mask**.
d) Click **Add**.

A confirmation message appears.

e) Click **Yes**.
f) Repeat the above steps for all the external switches added.

The external switches are added to the table.

Step 4 Click the **Devices Gateway** tab.

a) Click the **Add** icon.
b) In the **Add Device Gateway** dialog box, enter the subnet in CIDR notation, with or without mask, in the **Subnet** field.

The subnet can be in IPv4 or IPv6 format.

c) Enter the IP address of the **Gateway**.
d) Click **Add**.

Note After adding the Gateway, you can edit only the gateway IP address.

Step 5 (Optional) Click the **Socks Server** tab to add SOCKS Proxy servers so that SVO can reach the remote nodes.

a) Click the **Add** icon.
b) In the **Add Socks Server** dialog box, enter the IPv4 or IPv6 addresses in the **Address** field.
c) Click **Add**.

When you add SOCKS Proxy servers, the proper device gateways are automatically added in the **Devices Gateway** tab.

Step 6 (Only ROADM instance) Click the **OSPF** tab.

a) Enter the subnet in the **Subnet** field.
b) Enter the OSPF bits in the**Wild card Mask** field.
c) Enter the area ID in the **Area ID** field.
d) Click **Apply**.

A confirmation message appears.

e) Click **Yes**.

Step 7 (Only ROADM instance) Click the **Configure Switch** tab.

a) Click **Configure** to apply the configuration to the switch.

Note The **Configure** button is enabled only if you have chosen "Managed" in the **Switch Configuration** tab.

This configuration takes some minutes. After the configuration is completed, the message "Configuration completed" appears.

Step 8 Click the **Devices** tab.

Step 9 Add NCS 2000 devices. See Manage Devices, on page 100.

Wait until the Sync Status of the NCS 2000 device becomes "sync-completed".

Step 10 (Only ROADM instance) Configure the NTP server. See Configure Timing, on page 171.

Retrieve Device Diagnostics

Use this task to retrieve and download the device diagnostic logs.

Note The system retrieves the diagnostics of the selected device. The progress and errors are displayed at the top of the table.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

Step 2 Click the **Diagnostics** tab.

A table that lists the configured devices is displayed.

Step 3 Check the check box that is next to the device whose diagnostics you want to retrieve.

The check boxes in the Device Audit Log, Node Diagnostics, OBFL, and OBFL standby columns are checked by default.

Step 4 Click **Retrieve**.

A confirmation message appears.

Step 5 Click **Yes** to proceed.

A **Request Accepted** message appears.

Step 6 Click **OK**.

A message appears when the diagnostic action is completed.

Step 7 To download the logs, check the check box whose diagnostics you want to download and click **Download**.

A zip file containing the logs is downloaded.

Configure IPv4 Settings

Use this task to configure IPv4 settings.

Caution Verify that the IPv4 addresses assigned to the node are unique in the network. Duplicate IP addresses in the same network cause issues in managing the node.

Note The Name and MAC Address fields are display-only fields.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

Step 2 Click the **Configuration** > **IPv4 Settings** tabs.

Step 3 Click **Edit** corresponding to the IP settings of the device you want to change.

The **Edit IPv4 Settings** dialog box appears.

Step 4 Complete the following information in the Edit IPv4 Settings dialog box.

- **IP Address**—Type the IPv4 address for the device.
- **Subnet Prefix Length**—Type the subnet mask length (decimal number representing the subnet mask length in bits)
- **Default Gateway**—If the node is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the node cannot directly access.

Step 5 Click **Apply**.

A confirmation message appears.

Step 6 Click **OK**.

Change the Cooling Profile Control

Use this task to change the cooling profile control of the NCS 2006 node from automatic to manual or the other way round.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Device Configuration**.

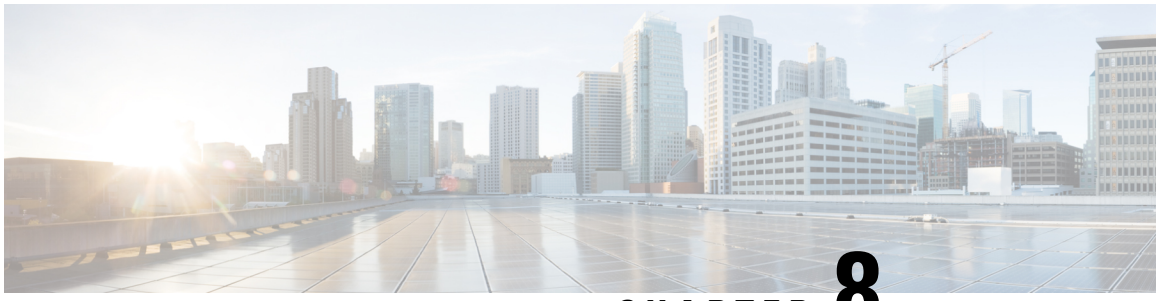
Step 2 Click the **Configuration** > **Device Settings** tabs.

Step 3 Choose the control from the **Cooling Profile Control** drop-down list.

Step 4 Click **Apply**.

A confirmation message appears.

Step 5 Click **Yes**.



CHAPTER 8

Configure the Node

This chapter describes the tasks related to node configuration in Cisco NCS 2000 SVO.

Internal Patch Cords

Internal patchcords provide virtual links between two termination points of the network. A termination point may be an OSC port, a transponder or muxponder trunk port, a line port, or a passive device port.

Manage Internal Patch Cords

Use this task to create, modify, view, or delete internal patchcords in the node.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **Internal Patch Cords** tabs.

Step 3 Perform these steps, as needed.

a) To add a new internal patch cord, perform these steps:

1. Click the + button.

   The **Create Internal Patch Cord** dialog box appears. It displays the **From** and **To** columns indicating the two termination points.

2. Choose the **Type** of the patch cord from the drop-down list. The options are chassis or passive unit.

3. Choose the **UID**, **Slot**, and **Port** types from the drop-down lists.

   Note If the selected Type in the previous step is a passive unit, the Slot field is not displayed.

4. Check the **Bi-directional** check box if you want to make the patch cord bidirectional.

5. Click **Apply**.

   The internal patch cord is created and added to the table that displays the following information:

   - **From**—Specifies the location from where the connection originates.
   - **To**—Specifies the location where the connection terminates.
   - **Type**—Specifies the type of internal patch cord. Possible values are Transport and Add-Drop.

b) To delete the internal patch cords, perform these steps:

1. Check the check boxes corresponding to the internal patch cords you want to delete.

2. Click the - button to delete the selected patch cord.

   A confirmation message appears.

3. Click **Yes**.

   The internal patch cord is deleted from the table.

Step 4 (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

Connection Verification

The connection verification feature measures power levels and verifies the optical cables and patchcords in a node for the following:

- Connectivity: Checks whether the cable is connected.
- Insertion Loss: Checks whether the cable loss is within expected value.

A 1567-nm connectivity check signal is generated and transmitted into the DMUX input port of the 20-SMRFS-CV card by a dedicated laser source. This signal is detected by an embedded photo diode to complete the connection verification.

Supported Cards and Passive Devices

The cards and passive devices that support connection verification are as follows:

- 16-AD-CCOFS
- 20-SMRFS-CV
- MF-DEG-5 and MF-DEG-5-CV
- MF-MPO-16LC and MF-MPO-16LC-CV
- MF-UPG-4 and MF-UPG-4-CV
- 100GS-CK-LC, 200G-CK-LC, and 400G-XP

The passive devices require loopback caps on unused ports. The CV version of the passive devices is shipped with loopback caps.

Prerequisites

The connection verification feature works only if the following conditions are met:

- Flex nodes must be present.
- Loopback caps must be installed on all the unused ports of the passive devices.
- At least one 20-SMRFS-CV card must be present in the node.
- All sides of the node must have the 20-SMRFS-CV card to test all the cables and patchcords.
- All passive devices must be connected with a USB cable and associated, so that power readings can be calculated.

Running the Connection Verification

The connection verification runs automatically at the following time intervals and events:

- 20 minutes after boot or reboot of the first shelf controller
- One minute after enabling the connection verification
- Ten minutes after creation or deletion of patchcords
- Ten minutes after creation or deletion of circuits
- Every six hours

Benefits

The benefits of connection verification feature are as follows:

- Validates the 20-SMRFS-CV card connectivity with local Add/Drop or other ROADM elements.
- Detects any incorrect cabling in the ROADM network element.

- Collects insertion losses of each optical path inside the network element to detect possible failures.

Verify Connections in Optical Cables

Use this task to verify the optical interconnections between the optical cards inside the flex ROADM node.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **Connection Verification** tabs.

Step 3 Check the **Enable Verification** check box to enable connection verification at the node level.

Step 4 View the following information displayed in the **Connection Verification** pane:

- From—Displays the source slot for connection verification.
- To—Displays the destination slot for connection verification.
- Connectivity Verification—Displays connectivity status. This information is summarized and displayed for any patchcord in the MPO cable. The different status includes:
  - Connected—Cable or patchcord is connected.
  - Not Connected—Cable or patchcord is disconnected.
  - Disabled—Cable or patchcord is excluded from connection verification.
  - Not Measurable—Power source is not detected; cable or patchcord cannot be tested for connection verification.
  - Not Verified—Cable or patchcord is not tested for connection verification. This is the default status upon first boot.
- Connectivity Last Change—Displays the date and time when the connectivity information was previously changed.
- Loss Verification—Displays insertion loss verification status that is one of the following:
  - Not Verified—Cable or patchcord is not tested for insertion loss verification. This is the default status upon first boot.
  - Not Measurable—Power source is not detected; cable or patchcord cannot be tested for insertion loss verification.
  - OK—Cable or patchcord insertion loss is within expected value.
  - Degrade—Cable or patchcord insertion loss is degrading.

    When the insertion loss is greater than the Insertion Loss Degrade threshold and less than the Insertion Loss Fail threshold, the status of insertion loss verification is Degrade. The Insertion Loss Degrade threshold is available at the bottom of the **Connection Verification** pane.

- Fail—Cable or patchcord insertion loss crossed the fail threshold.

  When the insertion loss is greater than the Insertion Loss Fail threshold, the status of insertion loss verification is Fail. The Insertion Loss Fail threshold is available at the bottom of the **Connection Verification** pane.

- Disabled—Cable or patchcord is excluded from insertion loss verification.

- Loss Last Changed—Displays the date and time when the insertion loss verification information was previously changed.
- Excess Loss [dB]—Displays the excess loss versus the maximum specified loss for the cable under test. When the shelf controller reboots, the information in the Excess Loss column is lost.
- Last Run—Displays the date and time when the connection verification and insertion loss verification were previously run. When the shelf controller reboots, the information in the Last Run column is lost.
- Ack—Displays the alarm acknowledgment information for a specific fiber. The possible values are true or false.
- Is Reachable—Indicates whether the connectivity is available to the patchcords and MPO cables. The possible values are true or false.
- Combined Loss—Indicates whether two or more patch cords are considered as a chain from the connection verification point of view. The possible values are true or false.

Step 5 Perform these steps, as needed.

a) Click **Abort CV** to stop the connection or insertion loss verification at any point.
b) Click **Verify Connectivity** to perform connection verification on all the patchcords and MPO cables (default behavior) or choose the required patchcords and MPO cables and click **Verify Connectivity** to perform connection verification on the selected patchcords and MPO cables.

   The confirmation message appears that lists all the links or the selected links accordingly.

c) Click **Verify Loss** to perform insertion loss verification on all the patchcords and MPO cables (default behavior) or choose the required patchcords and MPO cables and click **Verify Loss** to perform insertion loss verification on the selected patchcords and MPO cables.

   The confirmation message appears that lists all the links or the selected links accordingly.

d) Click **Ack** to acknowledge the insertion loss verification result related to the selected MPO cables or patchcords. This button allows MPO cable or patch cord to operate beyond the insertion loss thresholds without raising an alarm. If all the insertion loss verification problems on the current node are acknowledged, the consequent alarm on the node is cleared.
e) Click **Clear Ack** to clear the acknowledgment on the selected MPO cable or patchcord. The insertion loss verification result becomes Fail or Degrade. This operation can raise the IPC-VERIFICATION-FAIL or IPC-VERIFICATION-DEGRADE alarm on the node.
f) Enter the Insertion Loss Fail threshold in the Fail field and the Insertion Loss Degrade threshold in the Degrade field.

   The IPC-Verification-Running condition is raised when connection or insertion loss verification is started. The default values of Insertion Loss Fail threshold and Insertion Loss Degrade threshold parameters are 4 and 1.5 dB respectively. These two default thresholds are used to generate the alarms.

g) Click **Refresh** to refresh the connection verification information.

Step 6 Click **Apply** to apply the changes.

Step 7 After connection verification, perform these steps, as needed:

If the insertion loss verification results for a patchcord are Fail or Degrade, perform these steps:

a. Remove the patchcord.

b. Clean the patch cord.

c. Install the patchcord.

d. Perform the insertion loss verification step again.

If the patchcord status is Not Connected, it raises the IPC-VERIFICATION-FAIL alarm on the node. To clear this condition, perform these steps:

a. Ensure that the patchcords are installed correctly on both the ends.

b. Perform the insertion loss verification step again.

c. Replace the patchcords if the alarm still exists.

If the IPC-LOOPBACK-MISS alarm is raised on any port, perform these steps:

a. Identify the port with IPC-LOOPBACK-MISS alarm.

b. Check whether the loopback is installed on the port.

c. If the loopback is correctly installed, perform the insertion loss verification step again.

d. Replace the loopback if the alarm still exists.

Optical Degrees

From a topological point of view, all the DWDM units that are equipped in a node belong to a side. A side can be identified by a letter, or by the ports that are physically connected to the spans. A node can be connected to a maximum of 20 different spans. Each side identifies one of the spans to which the node is connected.

Manage Optical Degrees

Use this task to create, view, modify, or delete optical degrees in the node.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **Optical Degree** tabs.

Step 3 Perform these steps, as needed.

a) To create an optical degree, perform these steps:

1. Click the + button.

   The **Create Optical Degree** dialog box appears.

2. Select the **Degree**, **Line In**, and **Line Out**, values from their respective drop-down lists.

3. (Optional) Enter a description in the **Description** field.

4. Click **Apply**.

   Note You can only create a maximum of 20 optical degrees. The optical degree is created and added to the table that displays the following information.

   - **Degree**—Specifies the optical span of the side.
   - **Description**—Specifies the description as entered while creating the optical degree.
   - **Line In**—Specifies line in settings.
   - **Line Out**—Specifies line out settings.
   - **Connected-to (IP/Degree)**—Specifies the IP address and the optical degree of the remote SVO instance that is connected on the other side of the span.
   - **Span Validation**—Specifies whether the span can be used by the GMPLS algorithm for channel routing and validation. Values are True or False.
   - **Channel Grid**—Specifies the type of grid. Values are Flexible-Grid or Fixed-Grid.
   - **Channel Spacing**—Specifies the minimum frequency spacing between two adjacent channels in the optical grid. Values are 100 or 50 GHz.
   - **Spectrum Occupancy**—Specifies a percentage of the spectral density (the ratio of the C-band used by the carrier versus the total bandwidth). The valid range is 50% to 91%.
   - **Domain Type**—Specifies the algorithm that is active on the span. Values are LOGO or LEGACY.

b) To modify any one of the optical degree parameters described below degree, perform the required step as needed:

- To modify the span validation of an optical degree, select a value from the drop-down list in the **Span Validation** column and click **Apply**.
- To enable Fixed-Grid with LOGO on an optical degree, go to the related cell in the **Channel Spacing** column, select 50 or 100 from the drop-down list, and click **Apply**.

  The **Channel Grid** value changes to Fixed-Grid and the **Domain Type** value changes to LOGO.
- To enable Flexible-Grid with LOGO on an optical degree, go to the related cell in the **Spectrum Occupancy** column, enter a valid value, and click **Apply**.

  The **Channel Grid** value changes to Flexible-Grid and the **Domain Type** value changes to LOGO.
- From R12.3, to change the **Domain Type** from Fixed-Grid with LOGO to LEGACY on an optical degree, go to the related cell in the **ChannelSpacing** column, select **NONE** from the drop-down list, and click **Apply**.

The **Domain Type** value changes to LEGACY.

- From R12.3, to change the **Domain Type** from Flexible-Grid with LOGO to LEGACY on an optical degree, perform these steps:

  1. Go to the related cell in the **ChannelSpacing** column, select 50 or 100 from the drop-down list, and click **Apply**.

     The **Channel Grid** value changes to Fixed-Grid.

  2. Go to the related cell in the **ChannelSpacing** column, select **NONE** from the drop-down list, and click **Apply**.

     The **Domain Type** value changes to LEGACY.

Step 4 (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

Fiber Attributes

The Fiber Attributes tab lists the attributes of the fibers that are connected to the optical side.

Manage Fiber Attributes

Use this task to create, view, modify, or delete fiber attributes of a span.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **Fiber Attributes** tabs.

Step 3 Perform these steps, as needed.

a) To create a fiber attribute, perform these steps:

1. Click the + button.

   The **Create Fiber Attributes** dialog box appears.

2. Enter the fiber ID in the **Fiber ID** field.

3. Select the **Fiber ID**, **Degree**, **Fiber Type**, **Length**, **PMD**, **Attenuator In**, and **Attenuator Out** from their respective scroll-lists.

4. Click **Apply**.

   The fiber attribute is created and added to the table that displays the following information.

   - **Degree**—Specifies the optical side.

- **Fiber ID**—Specifies the fiber number in the duct.
- **Fiber Type**—Specifies the type of fiber deployed.
- **Length**—Specifies the length of the optical span in kms or miles.
- **PMD**—Specifies the polarization mode dispersion (PMD) fiber coefficient in ps/sqrt (km).
- **Attenuator In**—Specifies the input attenuation in dB between the node output port (typically LINE-TX port) and the input of the fiber span. The span may include patchcords, attenuators, and patch panels.
- **Attenuator Out**—Specifies the output attenuation in dB between the node input port (typically LINE-RX port) and the output of the fiber span. The span may include patchcords, attenuators, and patch panels.

b) To modify the fiber attributes, perform these steps:

1. To modify the Fiber Type, Length, PMD, Attenuator In, Attenuator Out, or PMD values on an optical degree, go to the related cell in the related column, select a value from the drop-down list, and click **Apply**.

   A confirmation message appears. Click **Yes**.

c) To delete a fiber attribute, perform these steps:

1. Check the check box corresponding to the fiber attribute you want to delete.
2. Click the **-** button to delete the selected fiber attribute.

   A confirmation message appears.
3. Click **Yes**.

   The fiber attribute is deleted from the table.

Step 4 (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

OSC

OSC is a point-to-point communication channel that connects two consecutive nodes. The OSC carries a supervisory data channel and synchronizes clocking at network nodes. The OSC also carries a user data channel. Before provisioning OSC terminations on TNC ports carrying Fast Ethernet (FE) payloads, ensure that you set the ALS mode on these ports to Disabled.

Manage OSC

Use this task to provision OSC terminations.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **OSC** tabs.

Step 3 Perform these steps, as needed.

a) To create a OSC termination, perform these steps:

1. Click the + button.

   The **Create OSC Terminations** dialog box appears.

2. Choose the port from the **Port** drop-down list.

3. Click **Apply**.

   The OSC termination is created and added to the table that displays the following information.

   - **Port**—Specifies the control card OSC port.
   - **Service State**—Specifies the OSC service state.

b) To delete an OSC termination, perform these steps:

1. Check the check box corresponding to the OSC termination you want to delete.

2. Click the - button to delete the selected OSC termination.

   A confirmation message appears.

3. Click **Yes**.

   The OSC termination is deleted from the table.

Step 4 (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

Manage GCC Terminations

Use this task to create or delete the GCC terminations required for the network.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **GCC** tabs.

Step 3 Perform these steps, as needed.

a) To create a GCC termination, perform these steps:

1. Click the + button.

   The **Create GCC Terminations** dialog box appears.
2. Choose the **Port**, **Channel**, and **Speed (K)** from their respective drop-down lists.
3. (Optional) Enter the foreign IP in the **Foreign IP** field.
4. Choose an option from the **Enable Ospf** drop-down list.
5. Click **Apply**.

   The GCC termination is created and added to the table.

b) To delete a GCC termination, perform these steps:

1. Check the check box corresponding to the GCC termination you want to delete.
2. Click the - button to delete the selected GCC termination.

   A confirmation message appears.
3. Click **Yes**.

   The GCC termination is deleted from the table.

Step 4 (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

Optical Degree Power Monitoring

Use this task to view bar graphs of the input and output spectrum on each optical side of the node.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.
Step 2 Click the **Optical Configuration** > **Optical Degree Power Monitoring** tabs.
Step 3 Choose the **Optical Degree** from the drop-down list.
Step 4 Click **Refresh**.

Link Power Control

The Link Power Control (LPC) feature performs the following functions:

- Maintains constant per channel power when desired or accidental changes to the number of channels occur. Constant per channel power increases optical network resilience.
- Compensates for optical network degradation (aging effects).
- Simplifies the installation and upgrade of DWDM optical networks by automatically calculating the amplifier setpoints.

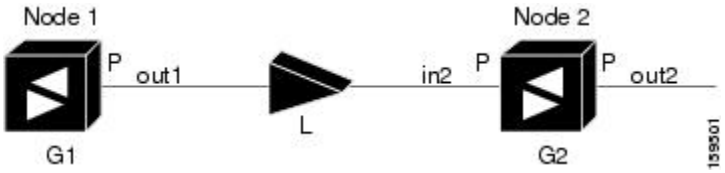
Note LPC algorithms manage the optical parameters of the line cards.

Amplifier software uses a control gain loop with fast transient suppression to keep the channel power constant regardless of any changes in the number of channels. Amplifiers monitor the changes to the input power and change the output power proportionately according to the calculated gain setpoint. The shelf controller software emulates the control output power loop to adjust for fiber degradation. To perform this function, the control card must know the channel distribution, which is provided by a signaling protocol, and the expected per channel power, which you can provision. The control card compares the actual amplifier output power with the expected amplifier output power and modifies the setpoints if any discrepancies occur.

LPC at the Shelf Controller Layer

Amplifiers are managed through software to monitor changes in the input power. Changes in the network characteristics have an impact on the amplifier input power. Changes in the input power are compensated for by only modifying the original calculated gain, because input power changes imply changes in the span loss. As a consequence, the gain to span loss established at the amplifier start-up is no longer satisfied, as shown in the following figure.

Figure 10: Using Amplifier Gain Adjustment to Compensate for System Degradation



In the preceding figure, Node 1 and Node 2 are equipped with booster amplifiers and preamplifiers. The input power received at the preamplifier on Node 2 (Pin2) depends on the total power launched by the booster amplifier on Node1, Pout1(n) (where n is the number of channels), and the effect of the span attenuation (L) between the two nodes. Span loss changes due to aging fiber and components or changes in operating conditions. The power into Node 2 is given by the following formula:

Pin2 = LPout1(n)

The phase gain of the preamplifier on Node 2 (GPre-2) is set during provisioning to compensate for the span loss so that the Node 2 preamplifier output power (Pout-Pre-2) is equal to the original transmitted power, as represented in the following formula:

Pout-Pre-2 = L x GPre-2 x Pout1(n)

In cases of system degradation, the power received at Node 2 decreases due to the change of span insertion loss (from L to L'). As a consequence of the preamplifier gain control working mode, the Node 2 preamplifier output power (Pout-Pre-2) also decreases. The goal of LPC at the shelf controller layer is simply to detect if an amplifier output change is needed because of changes in the number of channels or to other factors. If

factors other than the "changes in the number of channels" factor occur, LPC provisions a new gain at the Node 2 preamplifier (GPre-2') to compensate for the new span loss, as shown in the formula:

GPre-2' = GPre-2 (L/ L') = GPre-2 + [Pout-Pre-2 –Exp(Pout-Pre-2)]

Generalizing on the preceding relationship, LPC is able to compensate for system degradation by adjusting working amplifier gain or variable optical attenuation (VOA) and to eliminate the difference between the power value read by the photodiodes and the expected power value. The expected power values are calculated using:

- Provisioned per channel power value
- Channel distribution (the number of express, add, and drop channels in the node)
- ASE estimation

Channel distribution is determined by the sum of the provisioned and failed channels. Information about provisioned wavelengths is sent to LPC on the applicable nodes during the circuit creation. Information about failed channels is collected through a signaling protocol that monitors alarms on ports in the applicable nodes and distributes that information to all the other nodes in the network.

ASE calculations purify the noise from the power level that is reported from the photodiode. Each amplifier can compensate for its own noise, but cascaded amplifiers cannot compensate for ASE generated by preceding nodes. The ASE effect increases when the number of channels decreases; therefore, a correction factor must be calculated in each amplifier of the ring to compensate for ASE build-up.

LPC is a network-level feature that is distributed among different nodes. An LPC domain is a set of nodes that are regulated by the same instance of LPC at the network level. An LPC domain optically identifies a network portion that can be independently regulated. Every domain is terminated by two node sides residing on a terminal node, ROADM node, hub node, line termination meshed node, or an XC termination meshed node. An optical network can be divided into several different domains, with the following characteristics:

- Every domain is terminated by two node sides. The node sides terminating domains are:
  - Terminal node (any type)
  - ROADM node
  - Cross-connect (XC) termination mesh node
  - Line termination mesh node
- LPC domains are shown in the GUI.

Inside a domain, the LPC algorithm designates a primary node that is responsible for starting LPC hourly or every time a new circuit is provisioned or removed. Every time the primary node signals LPC to start, gain and VOA setpoints are evaluated on all nodes in the network. If corrections are needed in different nodes, they are always performed sequentially following the optical paths starting from the primary node.

LPC corrects the power level only if the variation exceeds the hysteresis thresholds of +/– 0.5 dB. Any power level fluctuation within the threshold range is skipped because it is considered negligible. Because LPC is designed to follow slow time events, it skips corrections greater than 3 dB. This is the typical total aging margin that is provisioned during the network design phase. After you provision the first channel or the amplifiers are turned up for the first time, LPC does not apply the 3-dB rule. In this case, LPC corrects all the power differences to turn up the node.

To avoid large power fluctuations, LPC adjusts power levels incrementally. The maximum power correction is +/– 0.5 dB. This is applied to each iteration until the optimal power level is reached. For example, a gain

deviation of 2 dB is corrected in four steps. Each of the four steps requires a complete LPC check on every node in the LPC domain. LPC can correct up to a maximum of 3 dB on an hourly basis. If degradation occurs over a longer time period, LPC compensates for it by using all margins that you provision during installation.

LPC can be manually disabled. In addition, LPC automatically disables itself when:

- A Hardware Fail (HF) alarm is raised by any card in any of the domain nodes.
- A Mismatch Equipment Alarm (MEA) is raised by any card in any of the domain nodes.
- An Improper Removal (IMPROPRMVL) alarm is raised by any card in any of the domain nodes.
- Gain Degrade (GAIN-HDEG), Power Degrade (OPWR-HDEG), and Power Fail (PWR-FAIL) alarms are raised by the output port of any amplifier card in any of the domain nodes.
- A VOA degrade or fail alarm is raised by any of the cards in any of the domain nodes.
- The signaling protocol detects that one of the LPC instances in any of the domain nodes is no longer reachable.

LPC raises the following minor, non-service-affecting alarms:

- APC Out of Range—LPC cannot assign a new setpoint for a parameter that is allocated to a port because the new setpoint exceeds the parameter range.
- APC Correction Skipped—LPC skipped a correction to one parameter allocated to a port because the difference between the expected and current values exceeds the +/– 3-dB security range.

LPC at the Amplifier Card Level

In constant gain mode, the amplifier power out control loop performs the following input and output power calculations, where G represents the gain and t represents time.

Pout (t) = G * Pin (t) (mW)

Pout (t) = G + Pin (t) (dB)

In a power-equalized optical system, the total input power is proportional to the number of channels. The amplifier software compensates for any variation of the input power due to changes in the number of channels carried by the incoming signal.

Amplifier software identifies changes in the read input power in two different instances, t1 and t2, as change in the traffic is being carried. The letters m and n in the following formula represent two different channel numbers. Pin/ch represents the input power per channel.

Pin (t1)= nPin/ch

Pin (t2) = mPin/ch

Amplifier software applies the variation in the input power to the output power with reaction time that is a fraction of a millisecond. This keeps the power constant on each channel at the output amplifier, even during a channel upgrade or a fiber cut.

The per channel power and working mode (gain or power) are set by automatic node setup (ANS). The provisioning is conducted on a per-degree basis.

Starting from the expected per channel power, the amplifiers automatically calculate the gain setpoint after the first channel is provisioned. An amplifier gain setpoint is calculated in order to make it equal to the loss

of the span preceding the amplifier itself. After the gain is calculated, the setpoint is no longer changed by the amplifier. Amplifier gain is recalculated every time the number of provisioned channels returns to zero. If you must force a recalculation of the gain, move the number of channels back to zero.

Forcing Power Correction

A wrong use of maintenance procedures can lead the system to raise the APC Correction Skipped alarm. The APC Correction Skipped alarm strongly limits network management (for example, a new circuit cannot be converted into In-Service (IS) state). The **Force Power Correction** button available in the **Node Configuration** > **APC** tab helps the user to restore normal conditions by clearing the APC Correction Skipped alarm. The **Force Power Correction** button must be used under the Cisco TAC surveillance because its misuse can lead to traffic loss.

Disable Link Power Control

Use this task to disable Link Power Control.

Caution When LPC is disabled, aging compensation is not applied and circuits cannot be activated. Disable LPC only to perform specific troubleshooting or node provisioning tasks. When the tasks are completed, enable and run LPC. Leaving LPC disabled can cause traffic loss.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select and select **Node Configuration**.

Step 2 Click the **APC** tab.

Step 3 Choose a degree and choose **force-disabled** from the **Admin Status** drop-down list.

Only degrees with Admin Status as automatic-enabled can be disabled.

Step 4 Click **Apply**.

Step 5 Verify that the **Service Status** field changes to force-disabled.

Enable Link Power Control

Use this task to enable Link Power Control.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **APC** tab.

Step 3 Choose a degree and choose **automatic-enabled** from the **Admin Status** drop-down list.

Only degrees with Admin Status as force-disabled can be enabled.

Step 4 Click **Apply**.

Step 5 Verify that the **Service Status** field changes to enabled.

Span Loss Measurement

Span loss measurements (in dB) check the span loss and are useful whenever changes to the network occur.

The span loss operational parameters are:

- **Measured By**—Displays whether the span loss is measured by the channel or Optical Service Channel (OSC). If a channel is not configured, the span loss is measured by the OSC. After a SMR-20 or SMR-9 channel is configured, the span loss is measured by the channel. An EDFA measures the span loss based on circuits.
- **Measured Span Loss**—Displays the measured span loss.
- **Measured Span Loss Accuracy**—Displays the accuracy of the span loss measurement. For example, if the measured span loss is 20 dB and the displayed accuracy value is 2.5, the actual span loss could either be 19 or 21 dB.
- **Measured Time**—Displays the time and date when the last span loss measured value is changed.

If there is a new network with SVO, the operational parameters list of span loss has two rows. The first row displays the OSC-measured span loss details. After the channel is configured, the second row is added, which displays the channel-measured span loss details. After the channel is configured, only the channel-measured span loss details are updated.

View or Modify Span Loss Parameters

Use this task to view or modify span loss parameters.

Note If a channel or OSC is not configured, span loss measurement is not reported and the operational parameters list is empty.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **Span Loss** tabs.

A table is displayed with the following information:

- **Degree**—Displays the side for which span loss information appears.
- **Measured By**—Displays whether the measurement was executed with or without channels. Values are OSC or CHANNEL.
- **Min Exp. Span Loss (dB)**—Displays the minimum expected span loss (in dB) for the incoming span.
- **Max Exp. Span Loss (dB)**—Displays the maximum executed span loss (in dB) for the incoming span.
- **Measured Span Loss (dB)**—Displays the measured span loss value.
- **Measured Accuracy (dB)**—Displays the resolution or accuracy of the span loss measurement. The resolution is +/-1.5 dB if the measured span loss is 0–25 dB. The resolution is +/-2.5 dB if the measured span loss is 25–38 dB.
- **Measured Time**—Displays the time and date when the last span loss measured value is changed.

Step 3 Select a row and click **Measure Span Loss**.

A message appears. Click **OK**.

Step 4 Refresh the table to view the updated **Measured Span Loss**, **Measured Accuracy**, and **Measured time**.

Step 5 Modify the values for **Min. Exp. Span Loss** or **Max. Exp. Span Loss** in dB. The range is from 0 to 99.

Step 6 Click **Apply**.

A confirmation message appears.

Step 7 Click **Yes**.

The span loss range is extended including the Accuracy value. A Span Loss Out of Range condition is raised when the measured span loss is higher than the extended range.

Step 8 (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

Optical Cross-connect Management

Optical cross-connect (OXC) circuits establish connectivity between two optical nodes on a specified C-band wavelength. The connection is made through the ports present on the wavelength selective switches, multiplexers, demultiplexer, and add/drop cards. In an OXC circuit, the wavelength from a source interface port ingresses to a DWDM system and then egresses from the DWDM system to the destination interface port. The OXC circuits are biredirectional in nature and are created using data models. The administrative states are:

- IS/Unlocked
- IS,AINS/Unlocked,AutomaticInService

- OOS,DSBLD/Locked,disabled

View Optical Cross-connect Circuits

Use this task to view the details of the optical cross-connects that are created for a node using data models.

Note The optical cross-connects are read-only and cannot be modified.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Select the **Optical Cross Connections** tab.

The following details are displayed for each cross-connect.

- **Connection Label**—Displays the name of the cross-connect.
- **Type**—Displays the type of cross-connect. It is bidirectional.
- **Admin Status**—Displays the admin state on the circuit.
- **Central Frequency (THz)**—Displays the spectral position of the circuit.
- **Allocation Width (GHz)**—Displays the bandwidth occupied by the service. The range is 25 to 300GHz.
- **Signal Width (GHz)**—Displays the carrier bandwidth.

  Note The payload bandwidth is lesser than the allocation bandwidth.

- **Path 1 End-points**—Displays the source and destination interfaces of the path.
- **Path 2 End-points**—Displays the source and destination interfaces of the path.

To view Path 1 or Path 2, click the + icon to expand the cross-connect. Click the down arrow on the right to view the internal details of Path 1 or Path 2. The details are:

- **Interface Name**—Displays the interface name.
- **Optical Power**—Displays the value of the optical power.
- **Power Degrade High**—Displays the threshold for a maximum power degrade.
- **Power Degrade Low**—Displays the threshold for a minimum power degrade.
- **Power Failure Low**—Displays the threshold for power failure.
- **Optical Psd Setpoint (dBm/GHz)**—Displays the optical power spectral density setpoint. This setpoint is independent of the width of the circuit.

- **Optical Power Setpoint**—Displays optical power setpoint. This setpoint is scaled to the width of the circuit and matches the value of the optical power parameter.

Step 3 (Optional) Click the **Export to Excel** button to export the information to an Excel sheet.

Import the Cisco ONP Configuration File into SVO

Table 16: Feature History

Feature Name	Release Information	Feature Description
Cisco ONP Configuration File Import Enhancement	Cisco NCS 2000 Release 12.3	SVO automatically redirects you to the Device Configuration page too add the device, if the device corresponding to the imported device configuration is not present in the system.

You can import the configuration file (NETCONF file) exported from Cisco ONP. The file contains parameters for the node, shelf, card type, port (including wavelength of the card), pluggable port module (PPM), and OTN and FEC parameters.

Caution Verify that you have the correct Cisco ONP network file before you begin this procedure. The file has an XML extension and a name that is assigned by your network planner. Check with your network planner or administrator if you have any questions.

Only the values present in XML format appear in the configuration file parameters. If the values are not in XML format, a column appears blank. The XML file values are independently reported and do not affect any configuration changes that you apply. Finally, the NETCONF file installs the ANS parameters that are calculated by Cisco ONP.

Use this task to import the Cisco ONP NETCONF file into SVO.

Before you begin

Log into the SVO Web Interface, on page 67.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click **Node Setup** tab.

Step 3 Click **Select Files**, browse and select the NETCONF file exported from Cisco ONP.

Note
- If you see an error in a pop-up window, validate the XML file and re import.
- When the device corresponding to the imported configuration is not present in the SVO, you will be redirected to the **Device Configuration** page to add the device. See Manage Devices, on page 100.

Step 4 If you want to export the XML file, click the **Download Node Configuration as XML** icon.

OTDR Support

Table 17: Feature History

Feature	Release Information	Description
OTDR Enhancements	Cisco NCS 2000 Release 12.2	The following OTDR enhancements are introduced to improve the user experience: • Choose either Hybrid or Fast mode for OTDR scan • Download OTDR scan configurations in .xls format • Print and download OTDR graph in JPEG or PNG formats • View the Event table below the graph with Event ID, Location (km), Magnitude (dB),and Type parameters

From R12.01 onwards, SVO supports TNCS-O and TNCS-2O cards for Optical Time Domain Reflectometer (OTDR) specific operations. OTDR is used to detect faults in an optical fiber link of a communication network.

The OTDR feature on the TNCS-O and TNCS-2O cards lets you do the following:

- Inspect the transmission fiber.
- Identify discontinuities or defect on the fiber.
- Measure the distance and magnitude of defects like insertion loss, reflection loss, and so on.
- Monitor variations in scan values and configured threshold values periodically.

Note OTDR does not support the placement of a bulk attenuator in its path. OTDR sends pulses of light and measures the reflected light. Bulk attenuator hinders this mechanism. The attenuator reduces the dynamic range of OTDR, limiting its capability. Another issue with bulk attenuator is that it has two reflective surfaces very close to each other which corrupts the OTDR pulses.

If a bulk attenuator is placed near the OTDR faceplate, the OTDR may not measure beyond the attenuator. If lumped attenuation is present beyond the attenuator, OTDR may erroneously declare that the fiber ends at that point. As per design, OTDR may exhibit this behavior with 5 dB or more, of lumped attenuation.

Note Once the OTDR port is initialized, it needs calibration every 24 hours for ORL measurement in Tx Direction. For this calibration, ORL training is triggered automatically by the OTDR module. ORL training is performed in hybrid mode and it lasts for just a few minutes. You cannot stop the trigger of this automatic ORL training.

OTDR Training

OTDR scan performances are improved using specific parameters of fiber such as span length, span loss, equipment insertion loss, reflection contributions, and major events on the fiber. This calibration operation is called OTDR training.

OTDR training is executed with the following rules.

- OTDR training is executed on both the Tx fiber and Rx fiber.
- OTDR training results are used to execute the composite scan.
- OTDR training is embedded in the scan operation.
- OTDR training takes up to 2 minutes in fast mode and up to 10 minutes in hybrid mode.
- OTDR training results in calibration file, fast span trace, and identification of the fiber end.

Note High reflection location is not available if detected during Optical Return Loss (ORL) training.

Provision OTDR Ports

Use this task to provision OTDR ports on the TNCS-O and TNCS-2O control cards.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page and select **Node Configuration.**

Step 2 Click the **OTDR** > **Provisioning** tabs.

Step 3 Perform these steps as needed.

a) To add an OTDR port, click +**Add**.

1. In the Create OTDR dialog box, choose the **Port**.
2. Click **Apply**.

   The OTDR port is created and added to the table that displays the following information:

   Note When you create an OTDR port, there are two entries with the status for direction Tx and the direction Rx.

   - Port—Displays the OTDR port name.
   - Direction—Displays the direction of the port (Rx or Tx).
   - Scan Status—Displays the status of the OTDR scan; for example, status-progress, status-failure, or status-idle.
   - Scan Progress—Displays the progress of the OTDR scan, in percentage.
   - OTDR Training Status—Displays the status of the OTDR training; for example, status-trained, and status-not-executed. The status is unique for each direction.
   - ORL Training Status—Displays the status of the ORL training. The status is unique for each direction.
   - Scan Failure Message—Displays the reason for the scan failure.
   - High Reflection Location—Displays the location of high reflection that is detected when the scan fails.
   - ORL Threshold— Displays the threshold of the ORL measure. There is an alarm (Excessive ORL Measure) associated with this field.
   - Refractive Index—Displays the fiber refractive index, which depends on the installed fiber.
   - Backscatter—Displays the reflective light on the fiber, which is also dependent on the installed fiber.
   - Loss Sensitivity—Displays the limit under which the loss is not considered as real loss, in dB.
   - Reflection Sensitivity—Displays the limit under which the reflection is not considered as a real reflection, in dB.

b) (Optional) If you want to delete a port, select one of the entries (Tx or Rx), and click **Delete**.

Both entries (Tx and Rx) of the port are deleted.

Step 4 To run the OTDR scan, perform these steps:

a) (Optional) Set the following values, if required.

- **Absolute Alarm Thresholds** for loss and reflection
- **Loss Sensitivity** and **Reflection Sensitivity** of the fiber

b) Choose the OTDR port on which OTDR scan has to be performed.

c) Click **Start**.

"OTDR scan started" message appears.

Note
- You can run only one scan at a time either in TX or RX direction, for each port. When you start a scan on direction TX, the column that is related to TX direction is updated, and when you start the scan on RX, the other column is updated.
- You can run scan on both ports (for example: ports 1 and 2 on TNCS-O, and ports 3 and 4 on TNCS-2O) at the same time.
- You can perform as many scans as you want, but SVO database can retain only up to two Tx scans and two Rx scans for each port. If you perform subsequent scans, the existing scan file is overwritten by the latest scan file. Hence, for each port, the web user interface displays only up to two TX scans and two RX scans.

You can view the status of the scan under the **Scan Status** column.

Step 5 To view the OTDR scan traces, perform these steps:

a) Click the **Traces** tab.

b) To set a baseline, perform these steps:

- From the **Port** drop-down list, choose one of the ports you have configured, to analyze.
- From the **Last Scan Traces** drop-down list, choose the scan file that you want to analyze.
- If the selected scan had desired results and you want to set the selected scan file as a baseline, click **Baseline**.
- Click **Yes** to confirm.
- Click **Ok** in the **Action** dialog box.

  The baseline is saved. You can have one baseline for each direction. You can use this baseline to compare with other OTDR scan results.

c) Choose the scan file and baseline file, and click the **Refresh** icon next to the **Port** drop-down list.

You can view the traces chart having Loss (dB) plotted against Distance (Km). The baseline chart is plotted in blue color, and the selected otdr scan chart is plotted in green color.

To zoom into the graph, press **Shift** key and drag the mouse pointer to select the portion of the graph.

d) Click **Download** to download the data file saved in the Standard OTDR Record (SOR) format.

The SOR file contains fiber trace data that are recorded by the OTDR instrument when testing an optical fiber.

e) Click the **Export as SVG** icon to download the traces file in SVG format.

Perform OTDR Scan

Use this task to perform the OTDR scan on a specific port.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and click **Node Configuration**.

Step 2 Click the **OTDR** tab.

Step 3 Click the **Provisioning** tab.

Step 4 Choose either **Hybrid** or **Fast** mode using the toggle button.

Step 5 Choose the port, you want to scan.

Step 6 Click **Start** to start scanning.

OTDR scan started message appears.

Step 7 Click **Ok**.

Step 8 Click **Stop**, when you want to stop scanning.

Step 9 Click **Yes** to confirm.

OTDR scan terminated message appears.

Step 10 Click **Ok**.

Note In the fast mode, an alarm (OTDR-FAST-SCAN-IN-PROGRESS-TX or OTDR-FAST-SCAN-IN-PROGRESS-RX) gets triggered informing that the scan is running in fast mode.

Automatic OTDR Scan

Automatic OTDR scan is started by checking the check box of the following parameters:

- **System Start-up, Fiber cut & Repair**-When there is a fiber cut or after fiber repair, automatic OTDR scan is started. You can set a time delay for the OTDR scan by choosing the **Start Delay (Min)** value.
- **Span Loss Increase**-When the span loss increases above the threshold value, automatic OTDR scan is started. You can choose the **Span Loss Increase Threshold (dB)** value.
- **Excessive ORL from Span**-When the ORL information is excessive, automatic OTDR scan is started.

OTDR Graph and Event Table

You can view the OTDR configurations in the graph. The Events in the graph are represented as following:

- O - OPEN CONNECTOR
- P - PASS THROUGH
- F - FACE PLATE

You can also print and download the graph in JPEG and PNG formats. You can view the Event table below the graph with the following parameters:

- Event ID
- Location (km)
- Magnitude (dB)
- Type

Expected Input Power

You to manage optical power on external devices while performing cross connection at the node level using expected input power. You can configure the expected input power on the OTS interface of the add port of the passive device.

You can set the expected input power on the following passive units:

- 15216-MD-48-ODD
- 15216-MD-48-EVEN
- 15216-MD-40-ODD
- 15216-MD-40-EVEN
- 15216-EF-40-ODD
- 15216-EF-40-EVEN
- NCS1K-MD-64-C
- NCS2K-MF-M16LC-CV
- NCS2K-MF-4X4-COFS
- NCS2K-MF-MPO-8LC
- NCS2K-MF-6AD-CFS
- NCS2K-MF-10AD-CFS

Manage Expected Input Power

Use this task to add, modify, view, or delete expected input power on the node.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **Expected Input Power** tabs.

Step 3 Perform these steps, as needed.

a) To add a new expected input power, perform these steps:

1. Click the **+** button.

   The **Configure Expected Input Power** dialog box appears.

2. From the **Type** drop-down list, choose **chassis** or **passive** unit.
3. Choose the **UID** and **Input Port** types from the drop-down lists.
4. Enter label to assign for the expected input power in the **Label** field.
5. Enter a value (dBm) in the **Expected Input Power** field.
6. Click **Apply**.

   The expected input power is added to the table that displays the following information:

   - **Input Port**—Specifies the port on which the expected input power is configured.
   - **Label**—Specifies the label information.
   - **Expected Input Power**—Specifies the expected input power that is configured in the port.

b) To delete the expected input power, perform these steps:

1. Check the check boxes corresponding to the expected input power you want to delete.
2. Click the **-** button to delete the selected input power.

   A confirmation message appears.

3. Click **Yes**.

   The expected input power is deleted from the table.

DCN Extension

Table 18: Feature History

Feature Name	Release Information	Feature Description
DCN Extension	Cisco NCS 2000 Release 12.3.1	External links are the logical links between two optical degrees that belong to two adjacent nodes. From this release, you can add one or more external links on a node using different optical degrees configured on that node. The creation of an external link allows the management of a remote node and these external links are used when it is not possible to create an optical-service-channel (OSC) communication.

SVO enables you to create and provision external logical links between a source local node and a destination remote node. These nodes use local and remote degrees and require IP addresses of the NCS 2000 devices.

You can also create external links using NETCONF. Ensure that you provide one interface and two endpoints. Each endpoint specifies one link index and IP address. For more information, See Cisco NCS 2000 Series SVO Data Models Configuration Guide.

Limitations for DCN Extension

- If any external link is already configured for a degree on a device, then you cannot use that degree for another external link on the same node or device. To achieve this, you should delete the existing external link and create a new external link on the same degree of the device.
- You cannot delete the degree if that degree is already used by an external link.

Manage DCN Extension

Use this task to add, view, or delete external links on the node.

Before you begin

Log into the SVO Web Interface, on page 67

Ensure that the degrees are existing in the node before configuring external links.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Configuration**.

Step 2 Click the **Optical Configuration** > **External Links** tabs.

Step 3 Perform these steps, as needed.

a) To add a new external link, perform these steps:

1. Click the **+** button.

   The **New External Link** dialog box appears.

2. In the **Local IP** field, the Local IP address of SVO instance that you are connected gets displays.

3. Enter username of the remote user who is allowed to perform configuration on the remote SVO instance in the **Remote Username** field.

4. Enter password of the remote user who is allowed to perform configuration on the remote SVO instance in the **Remote Password** field.

5. Enter the IP address of an SVO instance that you want to get connected in the **Remote IP** field.

6. Click the refresh (image) button at the end of the **Remote IP** field. The details from the remote node are fetched to allow the configuration.

7. From the **Local Degrees** drop-down list, select the available local degrees to create a starting point for the external link connection.

8. From the **Remote Degrees** drop-down list, select the available remote degrees to create an ending point for the external link connection.

   Note If no degree is displayed, check the remote SVO instance to configure the degrees.

9. Click **Add**.

   The external link is added to the table of the local and remote SVO **Node Configuration** pages. The table displays the following information under the **External Links** section of the **Node Configuration** page:

   - **Local Degrees**—Specifies the local degree on which the external link is created.
   - **Interfaces**—Specifies the interfaces on which the external link is created.
   - **Connected To**—Specifies the remote node instance to which it is connected. You can click the remote node instance link that is connected and it opens the remote node SVO instance. If nothing is displayed, then the local endpoint is not connected.
   - **Local IP**—Specifies the IP address of the NCS 2000 device on which the external link is created.
   - **Remote IP**—Specifies the NCS 2000 remote device IP address which is the end of the external link connection.

b) To delete the external link, perform these steps:

1. Check the check boxes corresponding to the external link that you want to delete.

2. Click the **-** button to delete the selected external link.

   A confirmation message appears. You must authenticate with the username and password for the remote SVO instance to which the external links are connected.

3. Click **Yes**.

The external link is deleted from both the local and remote SVO instances.

Remote Node Management Using GCC

Table 19: Feature History

Feature Name	Release Information	Description
Remote Node Management Using General Communication Channel (GCC)	Cisco NCS 2000 Release 12.3.1	You can manage remote nodes using fiber optics connection through GCC channels. You can only use the Cisco Light Web UI bring up the remote nodes.

The remote node management feature allows you to remotely manage NCS 2000 devices with transponder cards using the in-band General Communication Channel (GCC) channels with fiber optics from OTN clients. You can only use the Cisco Light Web UI on the NCS 2000 node to create and manage the GCC channel to the remote NCS 2000 node.

The transponder cards that are supported for remote node management using GCC on Cisco web UI are 200G-CK-LC, and 400G-XP and 10x10-LC cards.

Limitations

For remote node using a GCC0 channel, the SVO and NCS 2000 router should be in different subnets.

Manage Remote Node Using GCC

To manage a remote node, perform the following steps:

1. Bring up the remote node using the Light web UI. For more information, see Cisco Light Web User Interface.
2. Insert the transponder cards and pluggables in the NCS 2000 device at the remote site.
3. Provision a Node in GCC Using Light Web UI for Remote Node, on page 137.
4. Add NCS 2000 Node in SVO from SVO web UI, on page 139.

Provision a Node in GCC Using Light Web UI for Remote Node

Use this task to provision a node in GCC using the Cisco Light web UI.

Procedure

From the Cisco light web UI, click **Provisioning** > **GCC Configurations**.

a) In the **GCC Configuration** section, enter the following details:

- Shelf Number—Choose the shelf number.
- Slot Number—Choose the slot number.
- Port Number—Choose the port number. The options are:
  - **200G**—Port 2
  - **400G**—Port 11 or 12 pluggable
- Port Mode—Choose the transponder card port mode.
  - **200G**—The option is MXP 10x10G.
  - **400G**—The options are M100 or M200.
    - **M100**
      - First Slice—First slice should be configured when you are using M_200G as the port mode.
      - Second Slice—Choose the slice on which the card is configured. The options are OPM 100G or OPM 10 X 10G.
    - **M200**
      - First Slice—Choose the slice on which the card is configured. The options are OPM 100G or OPM 10 X 10G.
      - Second Slice—Choose the slice on which the card is configured. The options are OPM 100G or OPM 10 X 10G.
- GCC Rate—Choose the GCC rate for the channel.
  - **200G**—192K and 1200K
  - **400G**—1200K
- FEC—Choose the FEC rate.
  - **200G**—Standard, HG_FEC_7, or SD_FEC_20.
  - **400G**—SD_FEC_15_DE_OFF, SD_FEC_15_DE_ON, SD_FEC_25_DE_OFF, or SD_FEC_25_DE_ON.
- Wavelength—Choose the wavelength for the GCC channel.

View the GCC channel added under the GCC once the status of the GCC channel changes to Sync Completed. You can view the status of the GCC channel from both the SVO web UI and light web UI.

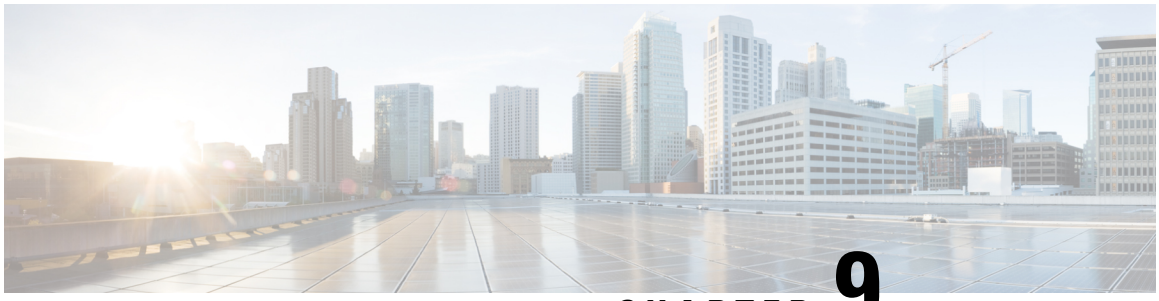
- For SVO web UI, see Add NCS 2000 Node in SVO from SVO web UI, on page 139.
- For the light web UI, you can check if the node is provisioned properly under the **Summary** table.

Now the GCC channel is created from remote to local node and the GCC channel is up.

Add NCS 2000 Node in SVO from SVO web UI

1. Log in to the SVO web UI. For more information, see Log into the SVO Web Interface.
2. Click **Networking** tab. In the **Networking** page, you can configure networking based on your requirement:
   a. Using Device Gateway—In the **Device Gateway** section, enter the IPv4 address of the Subnet and Gateway, and click **Add**. This option is used when the Gateway Network Element (GNE) (Firewall) is not configured on the gateway server.
   b. Using SOCKS Server—In the **SOCKS Server** section, enter the IPv4 address (with firewall) or IPv6 address of the SOCKS server and click **Add**.
3. Navigate to the **Device configuration** tab and add an NCS 2000 device in the SVO, and wait for the device to be **sync-completed**.

   Now the SVO is connected to the remote node.



CHAPTER 9

Provision Control Cards

This chapter describes the control cards used in Cisco NCS 2000 SVO and its related tasks.

The following table lists the package support for the control cards.

Card	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
SVO	✓	✓
TSCE	✓	✓
TNC	✓	✓
TNCE	✓	✓
TNCS	✓	✓
TNCS-O	✓	✓
TNCS-2	✓	✓
TNCS-2O	✓	✓

- Backup the System Database, on page 160

SVO Card

In this chapter, "SVO" refers to the NCS2K-SVO-K9 card.

The Shelf Virtualization Orchestrator (SVO) card is a two-slot card, which allows better management and control of multichassis solutions for the Cisco NCS 2000.

SVO extends the Network Services Orchestrator (NSO) application by network topology-aware virtualization, thereby improving the management of Cisco NCS 2000 through alarms, status and connection verifications, and so on.

SVO card enables High Availability functionality by connecting the two SFP+ 10GE optics back-to-back with another SVO card

The SVO card is provisioned as active and standby in the Cisco NCS 2006 or Cisco NCS 2015 chassis.

SVO card has a powerful 12 core 2GHz Intel Xeon processor with 64GB DDR4 RAM, 240GB SSD, 4x SFP+ ports, 5x 1GE copper for External Switch, 2x USB 3.0 along with Ethernet management and Console port.

On the Cisco NCS 2015 shelf, the cards can be installed in slots 2 to 15.

On the Cisco NCS 2006 shelf, the cards can be installed in slots 2 to 6.

The following pluggables on the four front panel ports.

SFP+ (10G)	SFP (1G)
ONS-SC+-10G-SR=	ONS-SI-GE-SX=
ONS-SC+-10G-LR=	ONS-SI-GE-LX=
SFP-10G-SR=	ONS-SE-ZE-EL=
SFP-10G-LR=	

The card has the features:

- Introduces a NETCONF interface with Cisco YANG models and a Nodal Craft web application.
- Hosts up to 15 OLA, DGE, or TXP container along with one ROADM in Release 12.3 and earlier.
- Hosts up to 20 OLA, DGE, or TXP container along with one ROADM in Release 12.3.1.
- Runs in complete redundancy mode with another standby SVO card.
- Provides selfmonitored hardware status with on board logging.
- Provides virtualization of nodes in a network.

TNC and TNCE Card

Cisco NCS 2002 and Cisco NCS 2006

On the NCS 2006 shelf, install redundant TNC or TNCE cards in slots 1 and 8. If the active TNC or TNCE card fails, the system traffic switches to the redundant TNC or TNCE card.

The NCS 2006 shelf has dual power supply. The TNC or the TNCE card monitors both supply voltage inputs on the NCS 2006 shelf. The TNC or TNCE card raises an alarm if one of the supply voltage inputs has a voltage out of the specified range.

You can insert and remove the TNC or TNCE card without impacting the system traffic, even when the system is online.

Note The TNC and TNCE cards are not supported on NCS 2015. When these cards are inserted into the active or standby slots of the NCS 2015 chassis, the cards do not start and become active.

TSCE Card

Cisco NCS 2002 and Cisco NCS 2006

The TSCE card is provisioned as active and standby in the NCS 2006 shelf. The TSCE card serves as the processor card for the shelf.

The NCS 2006 shelf has dual power supply. The TSCE card monitors both supply voltage inputs on the NCS 2006 shelf. The TSCE card raises an alarm if one of the supply voltage inputs has a voltage out of the specified range.

You can insert and remove the TSCE card without impacting the system traffic, even when the system is online.

The TSCE card does not support optical service channel (OSC) and SFP ports.

Note The TNC, TNCE, and TSCE cards cannot be inserted in the same shelf.

The TSCE card is not supported on NCS 2015. When the card is inserted into the active or standby slots of the NCS 2015 chassis, the card does not start and become active.

TNCS Card

In this chapter, "TNCS" refers to the NCS2K-TNCS-K9 card.

The TNCS cards are provisioned as active and standby in the Cisco NCS 2006 or NCS 2015 shelves. On the NCS 2015 shelf, the TNCS cards can be installed in slots 1 and 17. On the NCS 2006 shelf, the cards can be installed in slots 1 and 8. If the active TNCS card fails, the system switches to the redundant TNCS card.

The NCS 2015 shelf is powered by DC power modules with 3+1, 2+2, 2+1, or 1+1 redundancy. A minimum of one power module is required to turn up the chassis. The number of power modules to be connected is dependent on the chassis load. The TNCS cards raise an alarm if one of the supply voltage inputs has a voltage out of the specified range.

You can insert and remove the TNCS cards without impacting the system traffic, even when the system is online.

TNCS-O Card

In this chapter, "TNCS-O" refers to the NCS2K-TNCS-O-K9 card.

The TNCS-O card is provisioned as active and standby in the Cisco NCS 2006 or NCS 2015 shelves. On the NCS 2015 shelf, the TNCS-O card can be installed in slots 1 and 17. On the NCS 2006 shelf, the card can be installed in slots 1 and 8. If the active TNCS-O card fails, the system switches to the redundant TNCS-O card.

The TNCS-O cards support only Fast Ethernet (FE) and wavelength of 1518 nm in OSC transmissions.

Note OC-3 and ONE-GE payloads are not supported by the TNCS-O card.

The OSC transmission ranges are:

- Standard range: 12 - 43 dB
- Reduced range: 5 - 30 dB

Note The OTDR feature of TNCS-O and TNCS-2O cards is not supported over DWDM network configuration having PSM card at the line side of booster amplifier. In this configuration, the PSM Working (W) and Protect (P) ports are connected to the fiber. The OTDR signal is split into both W and P fibers and back reflected light from both the fibers leads to inconsistent OTDR results.

TNCS-2 and TNCS-2O Cards

In this chapter, "TNCS-2" refers to the NCS2K-TNCS-2-K9 card. "TNCS-2O" refers to the NCS2K-TNCS-2O-K9 card.

(NCS 2002, NCS 2006, NCS 2015)

The TNCS-2 and TNCS-2O cards are provisioned as active standby in the NCS 2006 or NCS 2015 chassis.

On the NCS 2015 shelf, the TNCS-2 and TNCS-2O cards can be installed in slots 1 and 17.

On the NCS 2006 shelf, the cards can be installed in slots 1 and 8.

On the NCS 2002 shelf, the cards can be installed in slot 1.

You can insert and remove the TNCS-2 and TNCS-2O cards without affecting the system traffic, even when the system is online.

The card has the following features:

- The TNCS-2 and the TNCS-2O cards work in redundant mode with another TNCS-2, TNCS-2O, TNCS, TNCSO, or TNCE cards.
- Synchronous Ethernet is supported on all GE and FE ports of the TNCS-2 and the TNCS-2O cards.
- The TNCS-2 and TNCS-2O cards address CPU EOL and SDRAM supply issues on the existing controller cards.

- The TNCS-2 and the TNCS-2O cards supports a secure boot.
- The TNCS-2 and TNCS-2O cards exhibit chassis control functions including the control of power supplies, fans, ECU, optical modules, clock synchronization, and line card configuration. It can also configure the field programmable devices present in the TNCS-2 or TNCS-2O card.
- The TNCS-2 and TNCS-2O cards support environment monitoring and alarm reporting features.

Note The TNCS-2 and TNCS-2O cards cannot be installed in the chassis that runs software earlier than R11.0.

- All packages are supported on the TNCS-2 and TNCS-2O cards.

The **Lamp Test** button is not available on the TNCS-2 and TNCS-2O cards.

Note When the EMS port is configured with 10 Mbps speed for TNCS-2 and TNCS-2O cards, it causes unicast storm control over the EMS peer port connected to the switch. However, when the storm controller is enabled on the EMS port for unicast packets on the switch, the EMS link goes down.

Table 20: The TNCS-2 and TNCS-2O cards support the following shelf control options:

Standby Slot	Active Slot	Support
TSC	TNCS-2O	Not Supported
TSC-E	TNCS-2O	Not Supported
TNC	TNCS-2O	Not Supported
TNC-E	TNCS-2O	Yes
TNCS	TNCS-2O	Yes
TNCS-O	TNCS-2O	Yes
TNCS-2	TNCS-2O	Yes
TSC	TNCS-2	Not Supported
TSC-E	TNCS-2	Not Supported
TNC	TNCS-2	Not Supported
TNC-E	TNCS-2	Yes
TNCS	TNCS-2	Yes
TNCS-O	TNCS-2	Yes
TNCS-2O	TNCS-2	Yes

Power Settings of TNCS-O and TNCS-2O OTDR Ports

OTDR ports of TNCS-O and TNCS-2O operate in two modes:

- High Power
- Low Power

These power changes occur based on the settings of the **Max Expected Span Loss** parameter. If the **Max Expected Span Loss** parameter is set to 28 dB or less, OTDR ports operate in low power and if the **Max Expected Span Loss** parameter is set to more then 28 dB, OTDR ports operate in high power.

After changing the value of **Max Expected Span Loss** parameter, you must perform **Launch ANS** from CTC as it is an ANS parameter.

Installing the TNC, TNCE, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card

This task installs active and standby cards on the Cisco NCS 2006 or Cisco NCS 2015 shelf.

Caution Do not remove the control cards during the software installation process, which is indicated by the alternate flashing of the FAIL and ACT/STBY LEDs. Removing the control cards during the software installation process corrupts the system memory.

Note Allow each control card to boot completely before installing the redundant control card.

Note TNCS and TNCS-O cards are having new bootcode version from R12.2. Due to this, TNCS and TNCS-O cards go for an additional reboot during software upgrade to R12.2.

Note You cannot insert the control cards in other slots due to mechanical constraints. To identify the card slot, match the symbol placed on the lower side of the card front panel with the symbol on the shelf.

Procedure

Step 1 Open the latches or ejectors of the first control card that you will install.

Step 2 Use the latches or ejectors to firmly slide the card horizontally along the guide rails until the card plugs into the receptacle at the back of the slot (slot 1 or 8 in the NCS 2006 shelf, slot 1 or 17 in the NCS 2015 shelf).

Note The cards slide vertically in the NCS 2015 shelf.

Step 3 Verify that the card is inserted correctly, and close the latches or ejectors on the card.

If you insert a card into a slot assigned for a different card, all LEDs turn off.

Step 4 If needed, verify the LED activity on the control card.

- The red FAIL LED, PWR LED turn on briefly.
- The red FAIL LED turns on for about 10 seconds.
- The red FAIL LED and the amber ACT/STBY LED turn on for about 30 seconds.
- The red FAIL LED blinks for about 10 seconds.
- The red FAIL LED turns on for about 15 seconds.
- All the LEDs including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs blink once and turn off for about 10 seconds.
- ACT/STBY LED blinks for about 1 second.
- All the LEDs including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs turn off for about 10 seconds.
- The ACT/STBY, ACO, and PWR LEDs turn on.
- The boot process is complete when the PWR LEDs turn green and the amber ACT/STBY LED remains on. The ACT/STBY LED turns green if this is the first control card installed, but turns amber if this is the second control card installed.

  Note It might take up to four minutes for the power alarms to clear.

  Note During the control card initialization, the SFTWDOWN alarm appears twice. The alarm clears after the control card boots completely.

  Note If the FAIL LED is on continuously, see the note in Step 8 about the control card automatic upload.

Figure 11: Installing TNC and TNCE Cards on the NCS 2006 Shelf

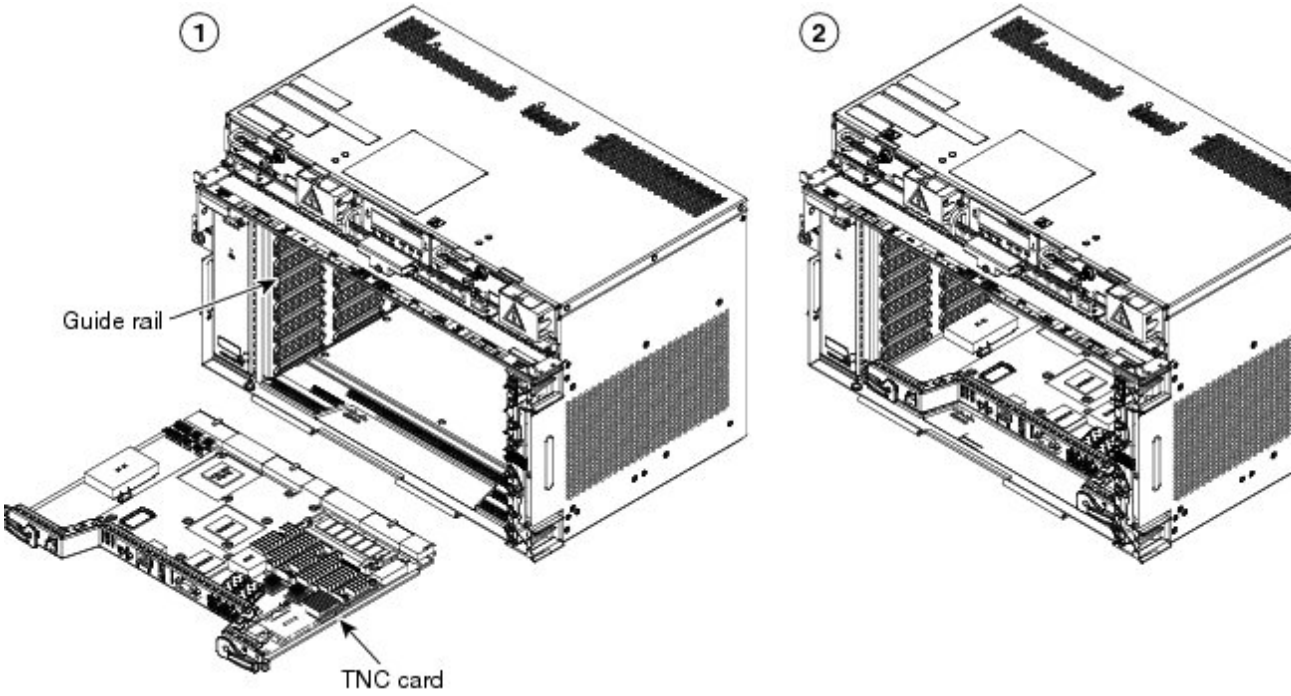
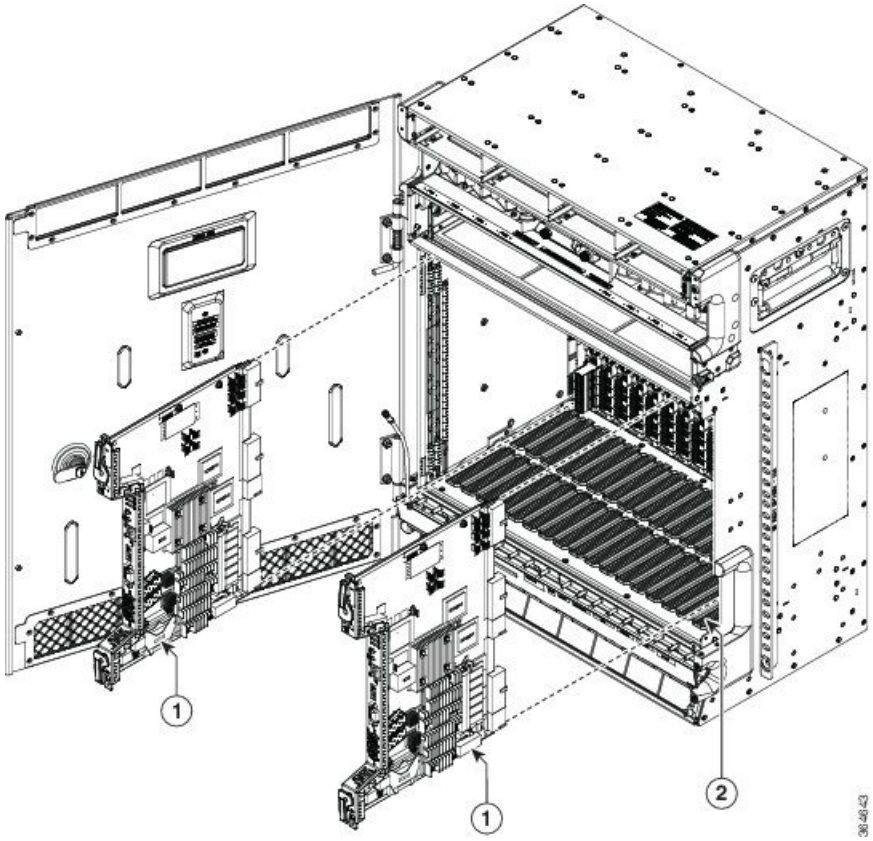


Figure 12: Installing TNCS/TNCS-O Cards on the NCS 2015 Shelf



1	TNCS/TNCS-O Card	2	Guide Rail

Step 5 Verify that the ACT/STBY LED is green if this is the first powered-up control card installed or amber if this is the second powered-up control card. The IP address, temperature of the node, and time of day appear on the LCD. The default time and date is 12:00 AM, January 1, 1970.

Step 6 The LCD cycles through the IP address (the default is 192.1.0.2), node name, and software version. Verify that the correct software version is shown on the LCD. The software text string indicates the node type (SDH or SONET) and software release. (For example: SDH 09.20-05L-20.10 indicates it is an SDH software load, Release 9.2. The numbers following the release number do not have any significance.)

Step 7 If the LCD shows the correct software version, continue with Step 8. If the LCD does not show the correct software version, refer to your next level of technical support, upgrade the software, or remove the control card and install a replacement card. Refer to the release-specific software upgrade document to replace the software.

Step 8 (NCS 2006 or NCS 2015 shelf only) Repeat Steps 1 through 7 for the redundant control card.

Note If you install a standby control card that has a different software version than the active control card, the standby control card copies the software version from the one in the active control card. When the standby card is first inserted, the LEDs follow the normal boot-up sequence. However, after the red FAIL LED turns on for about 5 seconds, the FAIL LED and the ACT/STBY LED begin to flash alternately for up to 30 minutes. After loading the new software, the upgraded control cards LEDs repeat the appropriate bootup sequence, and the amber ACT/STBY LED turns on.

Step 9 Return to your originating procedure.

Installing the SVO Card

This task installs the SVO card on the Cisco NCS 2006 or the Cisco NCS 2015 shelf.

Note Install and configure the SVO card before installing any other line cards into the shelf assemblies.

When you install the SVO card on the NCS 2000 chassis, the PWR-CON-LMT alarm is raised when the power consumption limit is exceeded. We recommend that you remove the SVO card and place it in another chassis that supports the required power.

Procedure

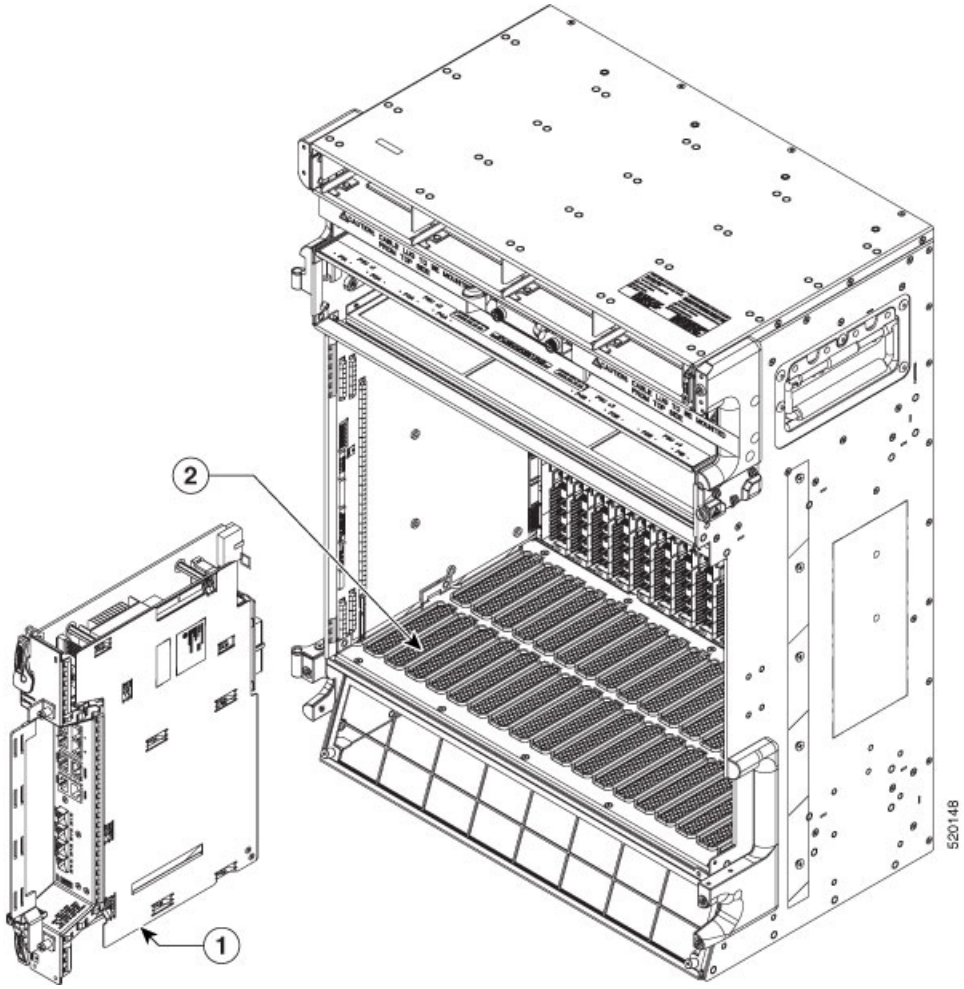
Step 1 Align the SVO card so the markings on the card and the chassis are on the same side.

Step 2 Open the latches or ejectors of the first SVO card that you will install.

Step 3 Use the latches or ejectors to firmly slide the card horizontally along the guide rails until the card plugs into the receptacle at the back of the slot (any slot from slot 2 to 6 in the NCS 2006 shelf or slot 2 to 15 in the NCS 2015 shelf).

Step 4 Verify that the card is inserted correctly, and close the latches or ejectors on the card.

Figure 13: Installing SVO Card on the NCS 2015 Shelf



1	SVO Card	2	Guide Rail

Figure 14: Installed SVO Card on the NCS 2015 Shelf

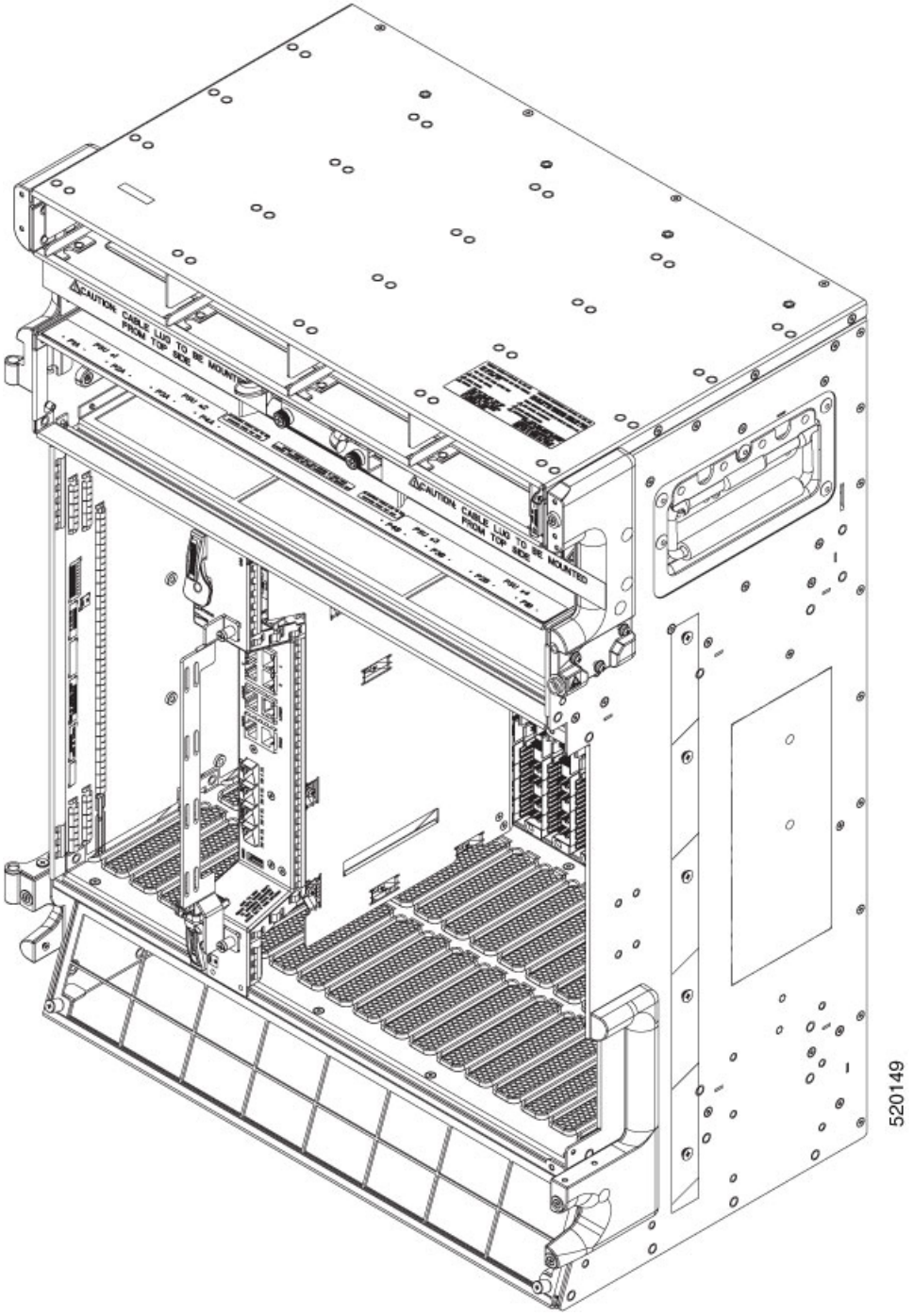
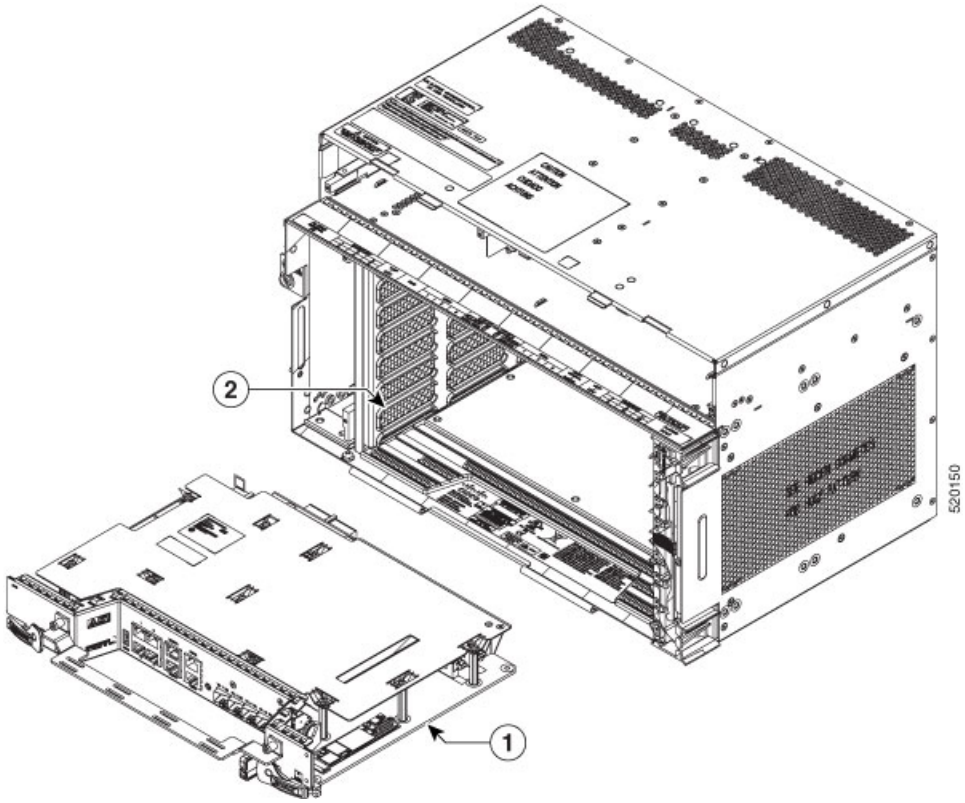
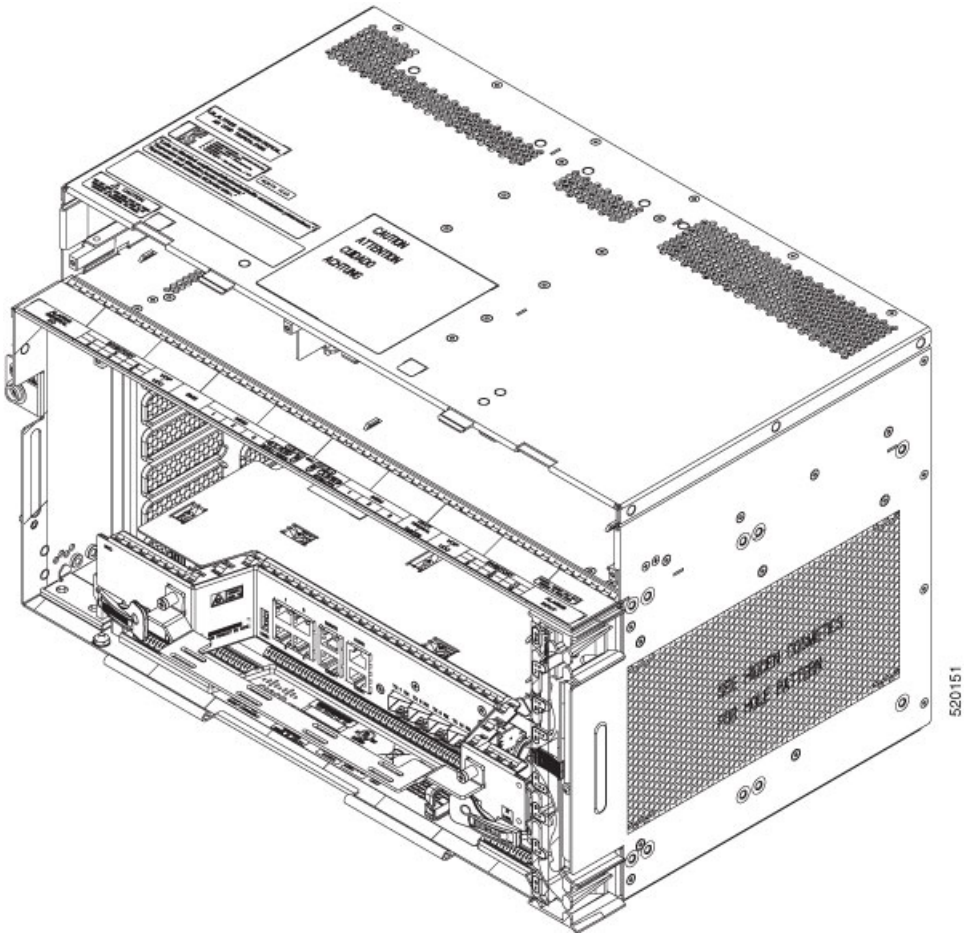


Figure 15: Installing SVO Card on the NCS 2006 Shelf



1	SVO Card	2	Guide Rail

Figure 16: Installed SVO Card on the NCS 2006 Shelf



Cable Routing for SVO Card

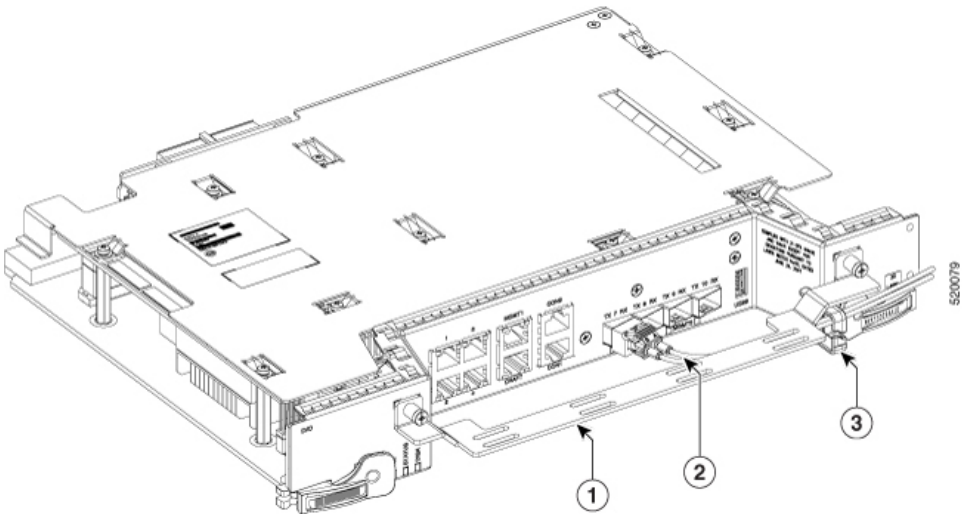
This task routes the cables on the SVO card that you are installing on the Cisco NCS 2006 or Cisco NCS 2015 shelf.

Before you begin

- Log into the SVO Web Interface, on page 67
- Installing the SVO Card

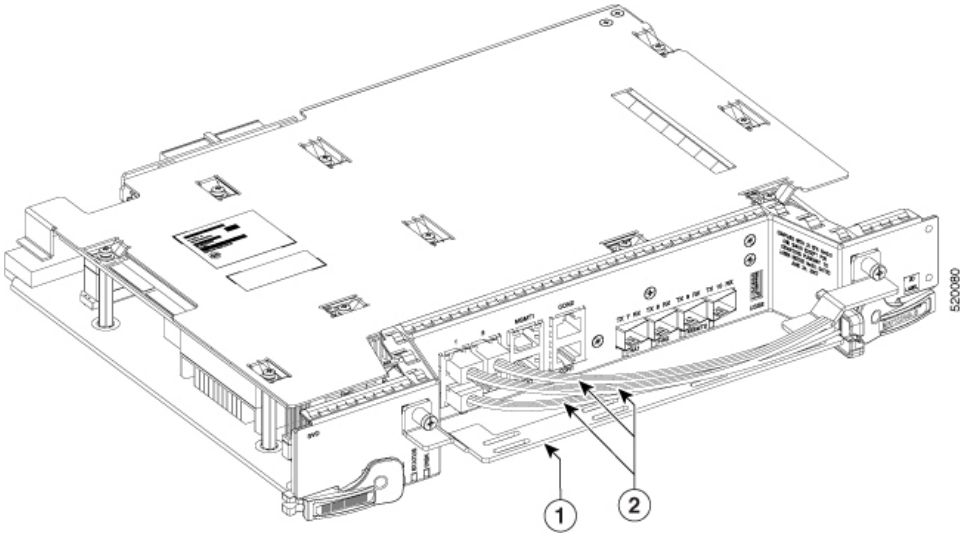
Procedure

Step 1 Route the optical fiber cables under the cable management bracket through the optical fiber clip as shown below.



1	Cable Management Bracket	2	Optical Fiber Cables
3	Clip for Optical Fibers		

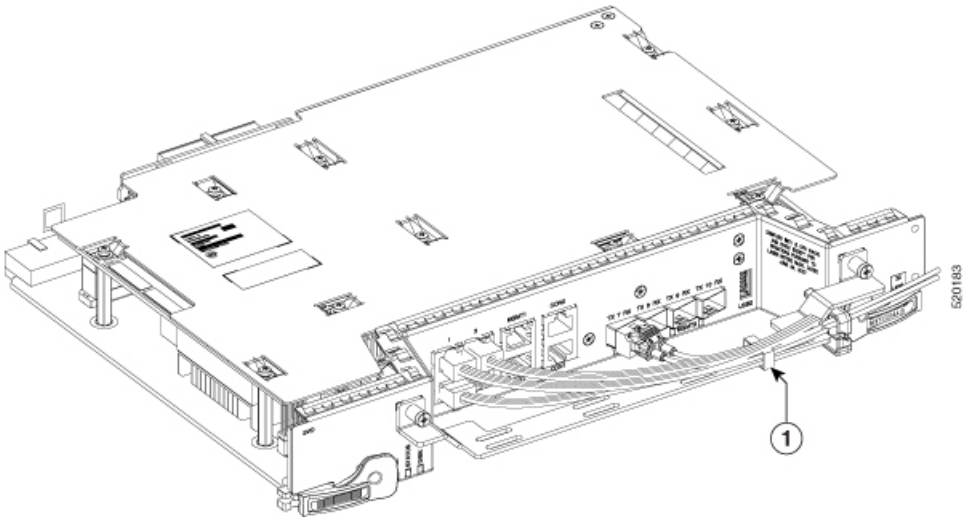
Step 2 Route the Amphenol, CAT6 FTP flat cable or an equivalent on top of the cable management bracket.



1	Cable Management Bracket	2	CAT6, FTP flat cable. For 1G copper ports use Amphenol CAT6, FTP flat cables (CMP compatible) or Equivalent.

Note The CMP compliant flat cable manufacturer is Amphenol and the MPN's for the same are 1 meter, 3 meters, and 10 meters.

Step 3 Wrap the velcro tape over the cable management bracket to retain the cables in position.



1	Velcro tape over the cable management bracket to retain the cables in position.	

Provision PPM

Use this task to provision the Pluggable Port Module (PPM) on the control card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Pluggable Port Modules** tabs.

Step 2 Click the + button.

The **Add PPM** dialog box appears.

Step 3 Choose the PPM port from the PPM drop-down list and click **Apply**.

The newly created PPM appears in the Pluggable Port Modules tab.

Provision Operating Mode

Use this task to provision the operating mode on the control card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Card Mode** tabs.

Step 2 In the Card Mode area, choose **TNC-MODE** or **TNCO-MODE** and click **Apply**.

The control cards can be configured either in TNC or TNCO operating mode. The TNC mode is the default operating mode for the cards. A card is configured in TNCO mode if the actual card that must be inserted into a shelf is a TNCS-O card.

Provision UDC

Use this task to provision the UDC on the control card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **UDC** tabs.

The UDC tab displays the port and its service type. Only the service type port can be manually changed.

Step 2 Click on the **Service Type** cell for the port you wish to change the service type.

A drop-down list appears with options **NONE** and **UDC**.

Step 3 Choose the **Service Type** mode from the drop-down list.

Step 4 Click **Apply**.

Provision RMON Thresholds

Use this task to provision the RMON thresholds on the control card.

Before you begin

- Log into the SVO Web Interface, on page 67

- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **RMON Thresholds** tabs.

Step 2 Click the + button.

The Create RMON Threshold dialog box appears.

Step 3 From the **Port ID** drop-down list, choose the port number.

Step 4 From the **Variable** drop-down list, choose a variable.

Step 5 From the **Alarm Type** drop-down list, indicate whether the event is triggered by the rising threshold, falling threshold, or both thresholds.

The available options are **Rising Threshold**, **Falling Threshold**, and **Rising and Falling Threshold**.

Step 6 From the **Sampling Type** drop-down list, choose either **Relative** or **Absolute**.

Relative restricts the threshold to use the number of occurrences within the user-set sample period.

Absolute sets the threshold to use the total number of occurrences, regardless of the time period.

Step 7 Enter the appropriate number of seconds in the **Sampling Period** field.

Step 8 Enter the appropriate number of occurrences in the **Rising Threshold** field.

For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1000 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

Step 9 Enter the appropriate number of occurrences in the **Falling Threshold** field.

In most cases, a falling threshold is set lower than the rising threshold.

Step 10 Click **Apply**.

Change Admin State for SVO Card Ports

Use this task to change the admin state of the ports on the SVO card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** tab.

The different ports along with their rates, reach distances, and admin states are displayed in the Ports pane.

Only the admin state of each port may be changed. For ANSI node, the admin state options are IS, OOS, and AINS. For ETSI nodes, the admin state options are unlocked, locked, or maintenance.

Step 2 Change the admin state as appropriate and click **Apply**.

Step 3 (Optional) Choose a port from the drop-down list and click **Reset to Defaults** to reset the port to default values.

Provision Optical Threshold Settings for the SVO Card

Use this task to provision the optical thresholds on the SVO card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70
- Provision PPM

Procedure

Step 1 Click the **Provisioning** > **Optics Thresholds** tabs.

Step 2 Choose the type of threshold that you want to change, 15 Min TCA, 1 Day TCA, or Alarm.

Step 3 Click **Refresh** to view the latest values.

Step 4 Modify any of the following threshold settings as needed by double-clicking the threshold value, deleting it, and entering a new value.

- **Port**—(Display only) Displays the port number and port type.
- **Laser Bias High**—Sets the maximum laser bias in percentage.
- **RX Power High**—Sets the maximum optical power received in dBm.
- **RX Power Low**—Sets the minimum optical power received in dBm.
- **TX Power High**—Sets the maximum optical power transmitted in dBm.
- **TX Power Low**—Sets the minimum optical power transmitted in dBm.

Step 5 Click **Apply**.

Step 6 Click **Yes** to complete the changes.

Backup the System Database

From R12.01 onwards, you can back up the database of SVO instance and NCS 2000 on the SVO card. You can backup the database on an individual node on which the SVO node-level software is running. The SVO instances of SVO node-level database include ROADM nodes, and NCS 2000 nodes connected to ROADMs.

You can request the backup using the NETCONF command (RPC call). For example, you can use the following XML for backup.

```
backup='''
<action xmlns="http://tail-f.com/ns/netconf/actions/1.0">
<data>
<svo-backup xmlns="http://cisco.com/yang/svo/diag">
<commands>
<backup>
</backup>
</commands>
</svo-backup>
</data>
</action>
```

The backup is performed and the database is stored on the SVO. You can view the backups taken from the SVO web UI. You can take any number of backups as required but the last backup taken is only available to download.

View the System Database Backup

Use this task to view the backup taken for the system database.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and Select **Database**.

In the **Database** page, you can view the following information:

- Latest Backup File Name
- Latest Backup Timestamp
- Current Status
- Log Message
- Current Log Status Timestamp

Step 2 Click **Download** to download the current backup.

The current backup is downloaded to your system.

Step 3 In the **Database** page, you can view a list of backups taken with the following information for the ROADM and NCS 2000 nodes:

- Component—Displays the list of ROADM and NCS 2000 node names.
- Log message—Displays whether the backup for the component is performed or not.

- Timestamp—Displays the date and time at which the backup is taken.

Restore the System Database from a Backup

You can back up the database of SVO instance and NCS 2000 on the SVO card. You can back up the database on an individual node on which the SVO node-level software is running. The SVO instances of SVO node-level database include NCS 2000 nodes.

The following steps describe how to perform the database restore operation.

1. Click the hamburger icon at the top-left of the page, and Select **Database**.

   In the **Database** page, you can view a list of backups that are taken for the ROADM and NCS 2000 nodes.

2. (Optional) Click **Upload** to upload a backup file.

   The backup file that you upload is the latest backup file.

3. Click **Restore** to restore the SVO node to the latest backup file.

   The restore process takes some time to complete. After the restore process, you have to log in to the SVO container again.

Note When you create a new container and restore the database:

- If the SVO instance name and Device name are the same as in the backup file, but the SVO instance IP address is different, database restore operation takes place.
- If the SVO instance name is different from the one in the backup file, database restore operation fails with the following error message.

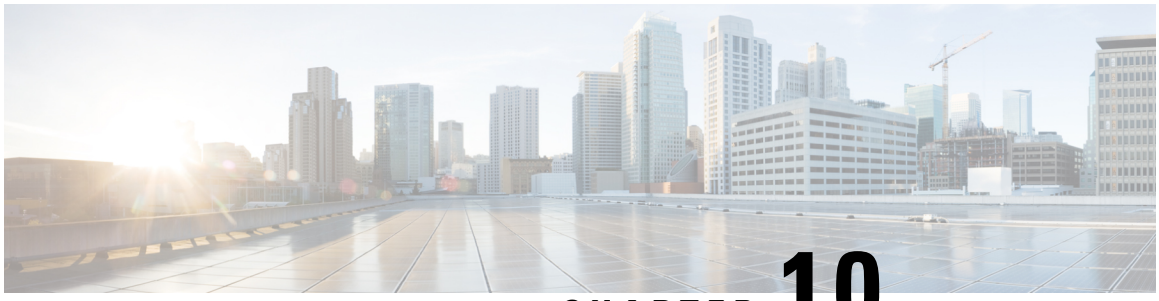
```
Request cannot be executed: Backup file was generated in SVO 'old-name' but current SVO
 is 'new-name'
```

- If the Device name is different from the one in the backup file, database restore operation fails with the following error message.

```
DB Restore of all devices completed with some error.
SVO_NAME (SVO) restore-procedure of component is busy saving recent modifications.
Please retry this operation later.
DEVICE_NAME (NCS2K) restore-procedure of component is failed.
```

- If the backed-up database contains both SVO and NCS2K components, add the NCS2K component to the SVO container before restoring. Otherwise, database restore operation fails with the following error message.

```
Request cannot be executed: Backup file was generated with '1' device(s) but currently
 '0' present(s)
```



CHAPTER 10

Manage the Shelf

This chapter describes the tasks related to shelf management in Cisco NCS 2000 SVO.

Configure Alarms and Controls

Use this task to configure external (environmental) alarms and external controls.

Note You can configure up to 14 alarms in the external alarms mode. You can configure up to 10 entities under external alarms and 4 entities under external controls in the external controls mode.

Note External alarms or external controls are not supported on the NCS 2002 chassis.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Alarm Extender** > **Alarm Dry Contacts Mode** tabs.

Step 5 Choose whether to configure the alarms as external alarms or external controls.

a. To configure external alarms, click the **External Alarm** option and click **Apply**.

b. To configure external controls, click the **External Control** option and click **Apply**.

Step 6 To configure external alarms, click the **External Alarms** tab, complete the following fields, and click **Apply**.

- **Enabled**—Check the check box to activate the fields for the alarm input number.
- **Severity**—Choose a severity from the drop-down list.

  The severity determines the alarm's severity in the Alarms and History tabs.

- **Alarm Type**—Choose an alarm type from the drop-down list.
- **Virtual Wire**—Choose the virtual wire number from the drop-down list to assign the external device to a virtual wire. Otherwise, do not change the None value.
- **Raised When**—From the drop-down list, choose the contact condition (open or closed) that triggers the alarm.
- **Description**—Enter a description.

Step 7 To configure external controls, click the **External Controls** tab, complete the following fields, and click **Apply**.

- **Enabled**—Check this check box to activate the fields for the alarm input number.
- **Control Type**—Choose the control type from the drop-down list: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- **Trigger Type**—Choose a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.
- **Description**—Enter a description.

Note External alarms and external controls must be recorded locally for the network element (NE). Both the alarm name and resolution are node-specific.

Step 8 To add new alarm types, complete the following:

a) Click the **User Defined Alarms** tab.

The user-defined alarms are displayed under the External Alarms tab if provisioned. If the user-defined alarm is configured as an external alarm, the alarm cannot be deleted. You can create up to 50 user-defined alarms.

b) Click **Add**.
c) Enter the new alarm type and click **OK**.

Suppress ECU Multishelf Ports Alarm

Alarms are raised when an ECU Multishelf (Management Ethernet) port is open. You can suppress the alarms on the unused ECU MSM ports and verify the ECU Multishelf ports alarm suppression settings.

Note ECU multishelf is not supported on the NCS 2002 chassis.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page and select **SVO Topology**.

The **SVO Topology** page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **ECU Multishelf** tabs.

Step 5 To suppress alarms for ECU multishelf ports:

a) Check the **Suppress Alarms** check box corresponding to the port for which you want to suppress the alarm.
b) Click **Apply**.
c) Click **Yes**.

Step 6 Click the **Alarms** tab and verify whether the suppressed alarms are removed from the Alarms Summary table.

Step 7 Click the **Conditions** tab and verify whether the suppressed conditions are removed from the table.

Step 8 (Optional) To discontinue alarm suppression for the ECU ports:

a) Check the **Suppress Alarms** check box corresponding to the port for which you want to suppress the alarm.
b) Click **Apply**.
c) Click **Yes**.

Display Power Monitoring Parameters

Use this task to display the power monitoring parameters of a chassis.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Power Monitor** tabs.

The Power Monitor tab displays the environment type, power summary, voltage thresholds for NCS 2006, and PSU configuration for NCS 2015.

Set Voltage Thresholds

Use this task to set voltage thresholds within a –48 (ECU48) VDC environment and –60 (ECU60) VDC environment for NCS 2006.

Note This task is applicable only for NCS2006-SA; voltage thresholds are not applicable for NCS2015-SA.

Caution The default battery voltage thresholds are not changed. Threshold changes must only be performed at the direction of your site administrator.

The voltage threshold range for each battery is –40.5 to –57.2 for ECU 48 and 40.5 to 72.0 for ECU 60.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Power Monitor** tabs.

Step 5 To change the extreme low battery voltage threshold in 0.5 VDC increments, choose a voltage from the ELWBATVGVdc drop-down list. The default value is -40.5.

Step 6 To change the low battery voltage threshold in 0.5 VDC increments, choose a voltage from the LWBATVGVdc drop-down list. The default value is -44.

Step 7 To change the high battery voltage threshold in 0.5 VDC increments, choose a voltage from the HIBATVGVdc drop-down list. The default value is -54 or -68.5 (for ECU 60).

Step 8 To change the extreme high battery voltage threshold in 0.5 VDC increments, choose a voltage from the EHIBATVGVdc drop-down list. The default value is -57.5 or -72.0 (for ECU 60).

Step 9 Click **Apply**.

Set PSU Configuration

Use this task to set PSU configuration for NCS 2015.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Power Monitor** tabs.

Step 5 Choose the appropriate PSU configuration for each PSU. The applicable values are none, work, protect, and both.

Step 6 Click **Apply**.

Display Voltage and Temperature Information

Use this task to display the voltage and temperature information of a chassis.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Voltage/Temperature** tabs.

The **Voltage/Temperature** tab displays the voltage and temperature information of the chassis.

Cooling Profile

The cooling profile feature allows you to control the speed of the fans in the Cisco NCS 2006 depending on the line cards used.

You can enable automatic cooling profile or manual cooling profile at the node level. The automatic cooling profile is selected by default. In this case, the cooling profile of the shelf is set, based on the line cards used in the shelf. The supported cooling profile values are Low, Medium, and High. The default cooling profile value is High.

You can change the cooling profile of the node from automatic to manual. In this case, you must change the cooling profile of the shelf depending on the line cards used in the shelf. If there are multiple cards in the shelf, you must choose the cooling profile of the card that requires the highest cooling profile. For example, if the shelf has two cards with low cooling profile, three cards with medium cooling profile, and one card with high cooling profile, you must choose a high cooling profile for the shelf.

Set Cooling Profile

Use this task to set the cooling profile on Cisco NCS 2006.

Before you begin

- Log into the SVO Web Interface, on page 67
- Change the Cooling Profile Control, on page 106

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the NCS 2006 chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Voltage/Temperature** tabs.

Step 5 From the **Cooling Profile** drop-down list, choose the cooling profile.

Step 6 Click **Apply**.

Set IP Address, Subnet Mask, Default Router Using LCD

Use this task to change the IP address, default router, and network mask using the LCD of NCS 2006 and NCS 2015. On NCS 2006, the LCD is a separate unit at the top of the shelf with a display. On NCS 2015, the LCD is on the fan tray.

Note You cannot perform this task if the LCD IP display screen is set to *Display Only* or *Suppress Display*.

Note The LCD reverts to normal display mode after five seconds of button inactivity.

Procedure

Step 1 On the NCS 2000 front panel, repeatedly press the **Slot** button until SHELF appears on the first line of the LCD. You are in the Shelf menu.

Step 2 Repeatedly press the **Port** button until the following information appears:

- To change the node IP address, Node Status=IpAddress
- To change the node network mask, Node Status=Net Mask
- To change the default router IP address, Node Status=Default Rtr

Step 3 Press the **Status** button to display the node IP address, the node subnet mask length, or the default router IP address.

The following IP addresses are displayed in the LCD one after the other:

- Regular IP—Node IP address that is used to access the node when the controller card is in nonsecure mode.
- Secure IP (15454 secure mode IP)—IP address that is assigned to the backplane LAN port. This port connects the node to an operations support system (OSS) through a central office LAN or private enterprise network. This IP address becomes a private address in the secure mode and prevents the front-access craft port user from accessing the LAN through the backplane port.
- Primary SVO—IP address of the SVO card that is currently managing the NCS 2000 device. The value is assigned only when the SVO card is connected to the NCS 2000 device and managing it. Otherwise, when SVO is not connected, the value of the IP address is 0.0.0.0. It is a read-only IP address that is displayed for troubleshooting.

Restriction If the Primary SVO node has an IPv6 address, the LCD is unable to display the full IP address because of the character limit of the display.

Step 4 Push the **Slot** button to move to the digit of the IP address, subnet mask, or default router that you want to change. The selected digit flashes.

The Slot, Status, and Port button positions correspond to the positions of the commands shown on the LCD. For example, you press the Slot button to invoke the Next command and the Status button to invoke the Done command.

Step 5 Press the **Port** button to cycle the IP address, subnet mask, or default router to the correct digit.

Step 6 When the change is complete, press the **Status** button to return to the relevant Node Status menu.

Step 7 Repeatedly press the **Port** button until the Shelf Save Configuration option appears.

Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears.

Step 9 Press the **Slot** button to apply the new IP address, subnet mask, or default router configuration or press **Port** to cancel the configuration.

Note The IP address and default router must be on the same subnet. If it is not, you cannot apply the configuration.

Step 10 Saving the new configuration causes the control cards to reboot. During the reboot, a message appears on the LCD. The LCD returns to the normal alternating display after both the control cards finish rebooting.

Configure Timing

Use this task to configure the node identification information such as NTP servers, date, time, and time zone.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Configuration**.

Step 2 Click the **SVO Configuration** > **Time Settings** tabs to view the timezone information.

- **Enable Date and Time**—Check this check box to enable the synchronization of SVO card with network time.
- **Server Address**—Type the IP address of the primary NTP server.
- **Backup Server Address**—Type the IP address of the secondary NTP server.

  When the primary NTP server fails or is not reachable, the node uses the secondary NTP server to synchronize its date and time. If both the primary and secondary NTP servers fail or are not reachable, the SNTP-FAIL alarm is raised. The node checks for the availability of the primary or secondary NTP server at regular intervals until it can get the time from any one of the NTP servers. When the node receives the time from any one server, it synchronizes its date and time with the server's date and time and the SNTP-FAIL alarm is cleared. For each retry and resynchronization, the node checks the availability of the primary NTP server first, followed by the secondary NTP server. The node synchronizes its date and time every hour.
- **Date and Time**—Choose the date and time.
- **Time Zone**—Choose a city within your time zone from the drop-down list.

Step 3 Click **Apply**.

A confirmation message appears.

Step 4 Click **Yes**.

Retrieve and Download SVO Diagnostics and System Diagnostics

Table 21: Feature History

Feature Name	Release Information	Feature Description
NCS Callback Log	Cisco NCS 2000 Release 12.2	This feature allows you to retrieve NCS callback diagnostic logs. This log collects information about the implementation status and return values of entire NSO data tree.

Use this task to retrieve and download SVO diagnostics and system diagnostics information.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Configuration**.

Step 2 Click the **Diagnostics** tab.

Step 3 To retrieve SVO diagnostic logs, perform these steps:

a) Click the **SVO Logs** tab.

b) Check the **Alarms**, **Audit Logs**, **Conditions**, **DB Logs**, **Engineer Logs**, **History Logs**, **NCS Callback Log**, and **Inventory Logs** check boxes as appropriate.

Note **NCS Callback Log** check box is not selected by default because retrieving NCS callback log could take long time to complete.

Table 22: Fields Description

Fields	Description
Alarms	Collects the active alarms
Audit Logs	Collects NSO audit logs
Conditions	Collects the active conditions
DB Logs	Collects the database logs
Engineer Logs	Collects all the system software logs
History Logs	Collects the alarms history logs
Inventory Logs	Collects the hardware inventory logs

Fields	Description
NCS Callback Log	Collects information about the implementation status and return values of entire NSO data tree

c) Click **Retrieve** to retrieve the diagnostics report.

A confirmation message appears.

d) Click **Yes**.
e) Click **Download** to download the diagnostics report.

A zip file containing the logs is downloaded.

Step 4 To retrieve system diagnostic logs, perform these steps:

Note The System logs can be retrieved only by the superuser on a ROADM node.

a) Click the **System Logs** tab.
b) Check the **Admin Plane Logs**, **HA Logs**, and **System Logs** check boxes as appropriate.
c) Click **Retrieve** to retrieve the diagnostics report.

A confirmation message appears.

d) Click **Yes**.
e) Click **Download** to download the diagnostics report.

A zip file containing the logs is downloaded.

The following details are displayed for both SVO logs and system logs:

- **Diagnostic Type**—Displays the request of the user
- **Progress Status**—Displays the progress of retrieval of logs
- **Result Info**—Displays the completed progress of retrieval of logs
- **Latest Log Time Stamp**—Displays the latest date and time of retrieval of logs

Fault Monitoring

The Fault Monitoring pane provides an alarm summary for all alarms and conditions that are encountered. It displays the number of Critical (CR), Major (MJ), Minor (MN), Warnings (W), and Non-applicable (NA) alarms. It displays the alarms, transient conditions, and historical alarms that are related to chassis, passive devices, pluggables, line cards, amplifier cards, and control cards. You can also create custom alarm profiles and apply them on the node using this pane.

Display Alarms

Use this task to display the alarms raised on a rack, chassis, or card.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Perform this step, as needed.

a) To view the alarms raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

   From R12.0.1 onwards, the alarm severities are displayed with alarm icons that are based on the alarm severity colors along with alarms. The expanded rack view on the left panel displays the highest alarm severity for each chassis.

3. Click the **Alarms** tab.

   In the rack view, the alarms that are related to the rack are displayed. The alarms with several severities such as Critical, Major, Minor, and Not Alarmed are displayed. The alarm severities are indicated by different colors.

b) To view the alarms raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Click the **Alarms** tab.

   In the chassis view, the alarms that are related to chassis and ancillaries of NCS 2006 and NCS 2015, control cards, line cards, amplifier cards, and pluggables are displayed. The alarms with several severities such as Critical, Major, Minor, and Not Alarmed are displayed. The alarm severities are indicated by different colors.

   In the chassis view, you can view borders with maximum alarm severity. For example, if critical alarms are raised for ports, then the borders of the ports section along with the chassis display with the designated alarm severity color.

c) To view the alarms raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **Alarms** tab.

   In the card view, the alarms that are related to the card are displayed. The alarms with several severities such as Critical, Major, Minor, and Not Alarmed are displayed. The alarm severities are indicated by different colors. The color of the card is the same as that of the highest severity alarm.

Step 2 Click the **Auto delete cleared alarms** check box to automatically delete the cleared alarms.

Step 3 Click **Export to Excel** to export the alarms to the excel sheet.

Step 4 From the **Severity** drop-down list, choose a severity to filter the alarms based on severity.

Display Transient Conditions

Use this task to display the transient conditions raised on a rack, chassis, or card.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Perform this step, as needed.

a) To view the transient conditions raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Click the **Conditions** tab.

b) To view the transient conditions raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

The chassis view appears.

4. Click the **Conditions** tab.

c) To view the transient conditions raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **Conditions** tab.

Step 2 Click **Fetch Conditions** to display the transient conditions.

Step 3 Click **Export to Excel** to export the transient conditions to the excel sheet.

Display Historical Alarms

Use this task to display the historical alarms raised on a rack, chassis, or card.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Perform this step, as needed.

a) To view the historical alarms raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Click the **History** tab.

b) To view the historical alarms raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Click the **History** tab.

c) To view the historical alarms raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **History** tab.

Step 2 Click **Export to Excel** to export the historical alarms to the excel sheet.

Step 3 From the **Severity** drop-down list, choose a severity to filter the alarms based on severity.

Alarm Profiles

The alarm profiles feature allows the user to change default alarm severities by creating unique alarm profiles for individual ports, cards, chassis, passive units, optical cross-connects, and optical interfaces.

By defalut, you can view two alarm profiles:

- Defalut—The Default alarm profile containing all the alarms is preprovisioned on the node. The Default profile sets alarm severities to standard Telcordia GR-474-CORE settings. The alarm severities in the Default profile cannot be changed. After loading the Default profile on the node, you can create custom alarm profiles. In the Inherited alarm profile, alarms inherit or copy severity from the next highest level. For example, a card with an Inherited alarm profile copies the severities that are used by the node hosting the card.
- all-suppressed alarms—Includes all the suppressed alrams.

You do not have to apply a single alarm profile to the node, card, and port-level alarms. Different profiles can be applied at different levels. You could use the default profile on a node and on all the cards and ports, but apply a custom profile that downgrades an alarm on a specific card.

When you modify severities in an alarm profile, all the Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) settings and the other way

round as defined in Telcordia GR-474. Default severities are used for all alarms and conditions until you create a new profile and apply it.

Create and Load Alarm Profiles

Use this task to create and load alarm profiles on the node.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Fault Monitoring**.

Step 2 Click the **Profiles** > **Alarm Profile** tabs.

The Default profile and all-suppressed alarms profile, along with the complete list of alarms appear in this tab.

Step 3 Click the + button to create a alarm profile.

The **Alarm Profile** dialog box appears.

Step 4 Enter the name of the custom alarm profile in the **Name** field.

Step 5 (Optional) Choose the resources such as card, ecu, and fan-tray from the **Resources** drop-down list.

A specific set of alarms is available for each resource.

Step 6 Click **Apply**.

The created alarm profile appears along with the Default alarm profile in the **Alarm Profile** tab.

Step 7 In the **Alarm Profile** tab, choose the new alarm profile and click **Load Profile** to load the new alarm profile on the node.

The alarms that belong to this alarm profile appear in the **Alarms for Profile** area.

Step 8 Perform these steps, as needed.

a) From the **SA Severity**, **NSA Severity**, and **Alarm Reported** drop-down lists for each alarm, choose the desired values and click **Apply**.

If Alarm Reported for an alarm is set as false, the alarm is not reported and is not available in the list of outstanding alarms.

b) To add a new alarm to the alarm profile, perform these steps:

1. Click the + button in the **Alarms for Profile** area.

   The **Add Alarm To Profile** dialog box appears.

2. From the **Alarm Name** drop-down list, choose the alarm and click **Apply**.

c) To remove an existing alarm from the alarm profile, perform these steps:

1. Choose the alarms to be removed in the **Alarms for Profile** area.

2. Click the - button.

   A confirmation message appears.

3. Click **Yes**.

Associate Alarm Profiles

Use this task to associate alarm profiles with the resources such as ports, cards, chassis, passive units, optical cross-connects, and optical interfaces.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Fault Monitoring**.

Step 2 Click the **Profiles** > **Profile Association** tabs.

Step 3 Click the + button.

The **Profile Association** dialog box appears.

Step 4 Enter the name of the association in the **Association** field.

Step 5 Choose the alarm profile from the **Profile** drop-down list.

Step 6 Click **Apply**.

Step 7 Choose the association and click **Load Association**.

Step 8 In the **Resource for Association** area, click the + button to associate a resource to the association.

The **Resource** dialog box appears.

Step 9 From the **Resoure Type** drop-down list, choose the resource such as device, chassis, passive unit, module, port, and so on.

The **Resource Type** drop-down list contains all the resources to which the alarm profile can be associated. Multiple resources can be associated with the same alarm profile. The other drop-down list options in the **Resource** dialog box vary based on the selected resource type.

Step 10 Choose the desired values from the other drop-down lists in the **Resource** dialog box.

Step 11 From the **Inherited** drop-down list, choose **Yes** or **No** to indicate whether the association must be applied to all the children of this resource or not.

Step 12 Click **Apply**.

When the alarm profile is associated with the resources, all the outstanding and new alarms matching these resources are immediately set with the new alarm severities.

High Availability Support on SVO

High Availability (HA) runs as a service package in each of the SVO instances. It is responsible for:

- Manual switchover for ROADM and OLA nodes
- Public IP address management after switchovers

A manual switchover is performed by the user for load balancing or during an upgrade, where an active instance is made standby and the standby instance becomes active. When the switchover is completed, the public IP address of the active instance is moved to the standby instance (which is currently the active instance). When the switchover between the primary and secondary instance is completed, the user must relogin.

Perform Manual Switchover for High Availability

Use this task to perform the manual switchover for high availability.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **HA Manager**.

The HA Status pane is displayed with the following details:

- **SVO Instance Name**—Displays the name of the SVO instance.
- **SVO Instance IP**—Displays the public IP address of the SVO instance that is used to access the Web UI of the SVO instance.
- **SVO Role on Primary**—Displays the role of the SVO instance on the primary card. The role can be primary or secondary.
- **SVO Role on Secondary**—Displays the role of the SVO instance on the secondary card. The role can be primary or secondary.

Step 2 From the SVO Instance drop-down list, select the SVO instance for which the switch over is required.

Step 3 Click **Switch**.

The HA Status table is automatically updated with the switchover details for the selected SVO instance.

Step 4 Click the IP address in the IP address column to get the details of the nodes.

Note While configuring a standalone HA link, if the user puts the high availability port on the standby SVO to OOS through the nodal craft, the standby SVO becomes unmanageable on nodal craft permanently.

To avoid this situation, click **Admin Plane** > **Details of Instance icon** > **Make the instance active** on the SVO where HA port is put to the OOS.

View Granular Details of the Card

Table 23: Feature History

Feature Name	Release Information	Feature Description
View Granular Details of the Card	Cisco NCS 2000 Release 12.3	You can view the granular details of the card, such as port name, admin state, and service state, by hovering the mouse over the ports in the card view.

Use this task to view the granular details of cards up to the port details.

Before you begin

Log into the SVO Web Interface, on page 67.

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Hover the mouse over the card ports to view the following details that are available under the **Provisioning** > **Optical Channel** or **Provisioning** > **Interface** tabs in the card view:

- Port name
- Service state
- Admin state

You can view these details in the rack view, chassis view and card view as well.

The following cards are supported:

- 15454-M-10X10G-LC
- 15454-M-100G-LC-C
- 15454-M-CFP-LC
- NCS2K-100G-CK-C
- NCS2K-100GS-CK-C
- NCS2K-200G-CK-C
- NCS2K-MR-MXP

- NCS2K-400G-XP
- NCS2K-1.2T-MXP
- 15454-40E-MXP-C
- 15454-OPT-AMP-C
- 15454-OPT-EDFA-17
- 15454-OPT-EDFA-24
- NCS2K-OPT-EDFA-35
- 15454-M-RAMAN-CTP
- 15454-M-RAMAN-COP
- NCS2K-EDRA1-26C
- NCS2K-EDRA1-26C
- NCS2K-EDRA2-26C
- NCS2K-EDRA2-35C
- NCS2K-EDRA1-35C
- NCS2K-9-SMR17FS
- NCS2K-9-SMR24FS
- NCS2K-9-SMR34FS
- NCS2K-20-SMRFS-CV
- NCS2K-20-SMRFS
- NCS2K-12-AD-CCOFS
- NCS2K-16-AD-CCOFS
- NCS2K-6-AD-DD-CFS
- 15454-PSM
- 15454-OTU2-XP
- 15454-80-WXC-C
- 15454-40-SMR1-C
- 15454-40-SMR2-C
- 15454-OPT-PRE
- 15454-OPT-BST
- 15454-OPT-BST-E
- 15454-OPT-AMP-17C
- 15454-OSC-CSM

- TNC
- TNCS-2
- TNCS-20
- TSC

Enable Autonegotiation on Ethernet Ports

Table 24: Feature History

Feature Name	Release Information	Feature Description
Auto negotiation Support on Ethernet Ports	Cisco NCS 2000 Release 12.3	Autonegotiation is supported for CRAFT, EMS, and UDC ethernet ports. You must choose AUTO for **Speed** or **Duplex** parameter to enable auto negotiation between the current node and peer node.

From Release 12.3, Autonegotiation can be enabled for CRAFT, EMS, and UDC ethernet ports.

Use this task to provision the parameters for the Ethernet interfaces of a chassis.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Ethernet** tabs.

Step 5 Modify any of the Ethernet settings as described in the following table.

Table 25: Ethernet Settings

Parameter	Description	Options
Name	(Display only) Name of the port	• CRAFT • EMS • UDC-VOIP-1 • UDC-VOIP-2
Speed	Sets the expected port speed.	• 10 • 100 • 1000 • AUTO. Selecting AUTO enables aut negotiation between the current node node. **Note** If AUTO is selected for **Spee** the value of **Duplex** parameter to AUTO. Collapse and expa Ethernet tab to reflect the cha
Duplex	Sets the expected duplex capability of ports.	• Full • Half • AUTO. Selecting AUTO enables aut negotiation between the current node node. **Note** If AUTO is selected for **Dupl** the value of **Speed** parameter to AUTO.
Current Value	Displays current value of speed and duplex.	—
Primary State	Displays the primary state of port.	—
Secondary State	Displays the secondary state of port.	—

Step 6 Click **Apply**.

View Blinking Alarm of a Card

Table 26: Feature History

Feature Name	Release Information	Feature Description
Blinking Alarm of a Card	Cisco NCS 2000 Release 12.3	You can view alarms blinking on a card in the rack, chassis, and card view. By default, the blinking alarms are enabled.

In Release 12.3, the SVO application displays blinking alarms for a card. The color of the blinking alarm changes based on the severity level of the alarm. The SVO application displays the highest severity alarm and hides the low severity alarms. To view the low severity alarms, you must disable the high severity alarms.

Use this task to view the blinking alarm of racks, chassis, and cards.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 To view the blinking alarm in the specific rack, perform these steps:

a) Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

b) Click the specific rack in the left panel.

The rack view appears.

Step 2 To view the blinking alarm in the specific chassis, perform these steps:

a) Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

b) Click the specific rack in the left panel.

The rack view appears.

c) Left-click the chassis, and select **Open**.

The chassis view appears.

Step 3 To view the blinking alarm in the specific card, perform these steps:

a) Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

b) Click the specific rack in the left panel.

The rack view appears.

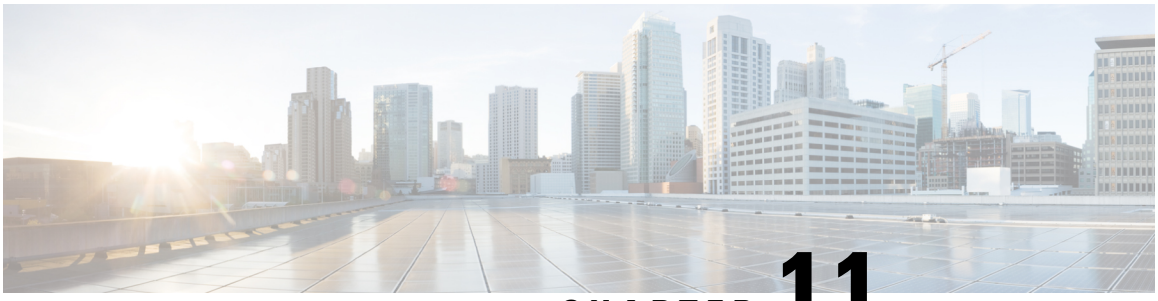
c) Left-click the specific chassis, and select **Open**.

The chassis view appears.

d) Click the slot that contains the card, and click **Open Card**.

The card view appears.

Note To disable the blinking alarms, click the respective alarm status icon in Alarm Summary under the **Alarms** tab.



CHAPTER 11

Provision Transponder and Muxponder Cards

This chapter describes the transponder and muxponder cards used in Cisco NCS 2000 SVO and its related tasks.

The following table lists the package support for the transponder and muxponder cards.

Card	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
10x10G-LC	✓	✓
CFP-LC	✓	✓
MR-MXP	✓	✓
100G-LC-C	✓	✓
100G-CK-C	✓	✓
100GS-CK-C	✓	✓
200G-CK-C	✓	✓
400G-XP	✓	✓
40E-MXP-C	✓	✓
OTU2-XP		✓
1.2T-MXP	✓	

10x10G-LC Card

In this chapter, "10x10G-LC" refers to the 15454-M-10x10G-LC card.

The 10x10G-LC card is a DWDM client card, which simplifies the integration and transport of 10 Gigabit Ethernet interfaces and services to enterprises or service provider optical networks. The 10x10G-LC card is supported on Cisco NCS 2000 Series platforms.

The 10x10G-LC card is a single-slot card and can be installed in any service slot of the chassis. The 10x10G-LC card consists of a 10-port SFP+ based (with gray-colored, coarse wavelength division multiplexing ([CWDM] and DWDM optics available) and one 100 G CXP-based port.

The 10x10G-LC card interoperates with 100G-LC -C, 100G-CK-C, 100GS-CK-C, and 200G-CK-C cards through a chassis backplane.

The 10x10G-LC card supports the following signal types:

- 10 Gigabit Ethernet LAN PHY (10.3125 Gbps)
- OTU-2

- G.709 overclocked to transport 10 Gigabit Ethernet as defined by ITU-T G. Sup43 Clause 7.1 (11.0957 Gbps)
- IB_5G (supported only in TXP-10G operating mode)

Note You may observe traffic glitches on the receiving direction of client ports 7, 8, 9, and 10 on the 400G-XP-LC card that you connect to CXP port of a 10x10G-LC card in fanout mode. To bringup traffic in such cases, change the admin state of the CXP port from **OOS-DSBLD** state to **IS-NR** state. Repeat the same action if you continue to observe glitches.

The key features of 10x10G-LC card are listed in Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards, on page 198.

Operating Modes for 10x10G-LC Card

The 10x10G-LC card supports the following operating modes:

- MXP-10x10G (10x10G Muxponder)
- RGN-10G (5x10G Regenerator)/TXP-10G (5x10G Transponder)
- Low Latency
- Fanout-10X10G
- TXPP-10G

Each operating mode can be configured using specific set of cards and client payloads. Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards, on page 198 lists the valid port pair for a specific operating mode and the supported payloads, and describes how each mode can be configured.

MXP-10x10G (10x10G Muxponder)

The 10x10G-LC card can be configured as a 10x10G muxponder. It can be connected with a 100G-LC-C, 100G-CK-C, or 100GS-CK-C card to support 10-port 10 G muxponder capabilities. The 100G-LC-C, 100G-CK-C, 100GS-CK-C, or 200G-CK-C card can be connected through the chassis backplane (no client CXP/CPAK is required) with the 10x10G-LC card to provide OTN multiplexing of the 10 G data streams into a single 100 G DWDM OTU4 wavelength. When the 10x10G-LC card is configured with the 100GS-CK-C card, and 10 Gigabit Ethernet LAN PHY payloads are supported. The allowed slot pairs are 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, or 14-15.

The 10x10G muxponder mode supports client signals that are a combination of any 10 Gigabit Ethernet LAN-PHY or OTU2 data rates.

RGN-10G (5x10G Regenerator)/TXP-10G (5x10G Transponder)

The 10x10G-LC card works as a standalone card, supporting the multitransponder functionality. The 10 Gbps SFP+ ports should be paired to provide the 10 G transponder functionality for each port of the port pair. By using the grey optics SFP+ to provide the client equipment connectivity and DWDM SFP+ on the WDM side, up to five 10 G transponders are supported by a single 10x10G-LC card. Up to six 10x10G-LC cards are supported on the Cisco NCS 2006 chassis allowing for 30 10 Gbps transponders in a single shelf.

All ports can be equipped with or without the G.709 Digital Wrapper function that provides wide flexibility in terms of the supported services.

As the client and trunk ports are completely independent, it is also possible to equip both SFP+ of the same pair of ports with the DWDM SFP+, thereby allowing them to function as a WDM regenerator. The CXP pluggable is unused in this configuration.

Each of the SFP+ ports can be provisioned as a client or trunk. When one port is selected as a trunk, the other port of the pair is automatically selected as the client port. The allowed port pairs are 1-2, 3-4, 5-6, 7-8, or 9-10.

For RGN-10G mode, both ports are trunk ports.

It is not a constraint to provision five pairs of TXP-10G mode or five pairs of RGN-10G mode. A mix of TXP-10G and RGN-10G modes can be configured. For example, pairs 1-2 and 5-6 can be configured as TXP-10G mode and the remaining pairs as RGN-10G mode.

Table 27: Supported Payload Mapping Between Two SFP+ Ports

SFP+ Payload (Peer-1)	SFP+ Payload (Peer -2)
10GE-LAN (CBR Mapped)	OTU2e or 10GE-LAN (CBR Mapped)
OTU2	OC192 or OTU2

Low Latency

The 10x10G-LC card can be configured in low latency mode. This configuration minimizes the time spent by the signal to cross the card during the regeneration process. Athough each SFP port functions as a unidirectional regenerator, adjacent SFP ports must be selected while provisioning this mode. Both ports are trunk ports. The allowed ports are 1-2, 3-4, 5-6, 7-8, or 9-10. A mix of TXP-10G, RGN-10G, and low latency modes can be configured.

The low latency mode supports 10GE data rates. The same payload must be provisioned on both SFP ports involved in this operating mode. GCC cannot be provisioned on the ports used in low latency mode. The low latency mode does not support terminal and facility loopback.

Fanout-10X10G

The 10x10G-LC card can be configured in the fanout-10x10G mode. The fanout configuration configures the CXP side as the client and SFP side as the trunk. This configuration functions as ten independent transponders. The CXP lanes are managed independently and the payload for each CXP-lane-SPF+ pair is independent of the other pairs.

The fanout configuration provides the following mapping for the port pairs:

- CXP lane 2-SFP1
- CXP lane 3-SFP2
- CXP lane 4-SFP3
- CXP lane 5-SFP4
- CXP lane 6-SFP5
- CXP lane 7-SFP6
- CXP lane 8-SFP7

- CXP lane 9-SFP8
- CXP lane 10-SFP9
- CXP lane 11-SFP10

Note CXP lane 1 and CXP lane 12 are not supported in this configuration.

The fanout configuration supports the following payload types and mapping modes:

- 10GE (CXP line), transparent (no mapping), 10GE (SFP)
- 10GE (CXP line), GFP mapping, OTU2 (SFP)
- 10GE (CXP line), CBR mapping, OTU2e (SFP)

TXPP-10G

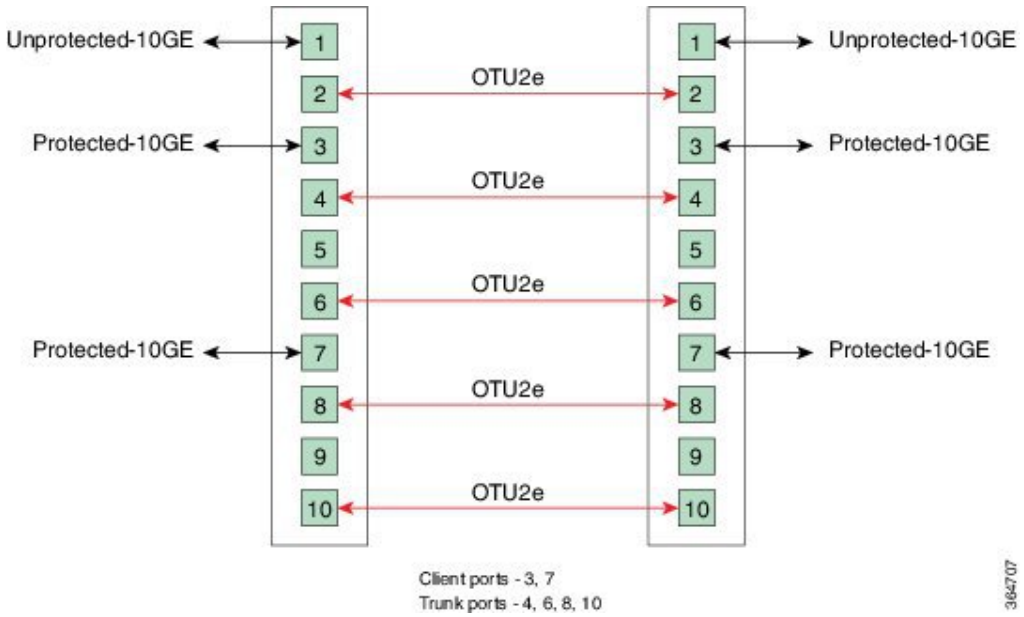
Splitter protection can be implemented on the 10x10G-LC card in TXPP-10G mode. The 10x10G-LC card supports up to two splitter protection groups with one client and two trunk ports. The client and trunk ports on the two groups are:

- Port 3 (client), port 4, and port 6 (trunks) on the first protection group
- Port 7 (client), port 8, and port 10 (trunks) on the second protection group

Port 1 and port 2 are available for unprotected transponders and can be configured in the standard TXP-10G mode, with the first port selected as the trunk and the other port selected as the client. Two ports, port 5 and port 9, are left unused. A Y-Cable protection group cannot be defined on the same 10x10G-LC card when it is provisioned in the TXPP-10G mode. The splitter protection is supported only for 10GE traffic, with trunk ports set to disabled FEC, standard FEC, or enhanced FEC (E-FEC) mode.

The following figure shows the 10x10G-LC card configured for splitter protection.

Figure 17: Splitter Protection on the 10x10G-LC card



For more information about the 10x10G-LC card, see http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/data_sheet_c78-713296.html.

CFP-LC Card

In this chapter, "CFP-LC" refers to the _15454-M-CFP-LC card.

The CFP-LC card is a client card, which simplifies the integration and transport of 40 GE and 100 GE interfaces and services to enterprises or service provider optical networks. The CFP-LC card is supported on the Cisco NCS 2006 and NCS 2015 platform. The CFP-LC card provides 100 Gbps services to support 100 G DWDM wavelengths generated by the 100G-LC-C card. The traffic coming from CFP interfaces is switched to the trunk port through a cross-switch.

The CFP-LC card supports the following signal types:

- 100 Gigabit Ethernet
- 40 Gigabit Ethernet
- OTU-3
- OTU-4

Client ports can be equipped with a large variety of CFP pluggables.

Key Features

The key features of CFP-LC card are listed in Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards, on page 198.

The CFP-LC card is a double-slot card and can be installed in Slot 3 or Slot 5 in the Cisco NCS 2006 chassis, and the 100G-LC-C peers cards must be placed in the adjacent slots (2 and 5 or 4 and 7). If the card is plugged in one of the unsupported slots or in a Cisco NCS 2002 chassis, the system raises an EQPT::MEA (Mismatch of Equipment Alarm) notification. Up to two CFP-LC cards per Cisco NCS 2006 shelf assembly can be installed, supporting up to 28x 40-Gbps or 14x 100 Gbps interfaces per 42-rack units (RU) bay frame.

The CFP-LC card is equipped with two 100 G CFP pluggable modules and a cross-bar embedded switch module. The CFP-LC card provides two backplane interfaces (working both at 100 Gb or 40 Gb) that are suitable for the cross-switch application on the incoming CFP signals. The CFP-LC card can be configured to send all client CFP services towards the backplane to be connected with up to two 100G-LC-C cards placed in the two adjacent slots (upper and lower) of the Cisco NCS 2006 chassis in order to provide two 100 G transponders configurations.

Operating Modes for CFP-LC Card

The CFP-LC card supports the following operating modes:

- 2x40G Muxponder
- CFP-TXP (100G Transponder)

Each operating mode can be configured using the specific set of cards and client payloads. Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards, on page 198 lists the valid port pair for a specific operating mode and the supported payloads, and describes how each mode can be configured.

2x40G Muxponder

The CFP-LC card can be configured as a 2-port 40 G muxponder. It can be connected with the 100G-LC-C or 100G-CK-C card to support 2-port 40 G muxponder capabilities. The 100G-LC-C or 100G-CK-C card can be connected through the Cisco NCS 2006 backplane (no client CXP/CPAK required) with the CFP-LC card to provide OTN multiplexing of the 40 G data streams into a single 100 G WDM OTU4 wavelength. The 2x40G muxponder mode supports client signals that are a mix and combination of any 40 Gigabit Ethernet LAN-PHY or OTU3 data rates.

CFP-TXP (100G Transponder)

The CFP-LC card can be configured as a 100G transponder. It can be connected with the 100G-LC-C or 100G-CK-C card to support the client interface for the 100-Gbps transponder capabilities. The 100G CXP pluggable available on the 100G-LC card supports only the 100GE-BASE-SR10 client interface, while the 100GE-BASE-LR4 is supported using only a CFP form factor. The 100G CPAK pluggable available on the 100G-CK-C card supports the CPAK-100G-SR10 and CPAK-100G-LR4 client interfaces.

The CFP-LC card can be connected through the Cisco NCS 2006 backplane with up to two 100G-LC cards placed in the upper or lower slot of the same shelf to provide the equivalent functionalities of two 100 G LR4 transponders, leveraging on CFP pluggables as the client interface.

For more information about the CFP-LC card, see
http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/data_sheet_c78-713295.html

MR-MXP Card

In this chapter, "MR-MXP" refers to the NCS2K-MR-MXP card.

The MR-MXP card is a mixed rate 10G and 40G client muxponder that is supported on Cisco NCS 2000 Series platforms. The card is equipped with one CPAK port, two SFP ports, and two QSFP+ ports. The card can interoperate with 100GS-CK-C, 200G-CK-C, and 10x10G-LC cards through a chassis backplane.

Key Features

The card key features are listed in the Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards, on page 198.

The MR-MXP card provides the following features:

- Termination point for a 100G client payload on the CPAK port. The aggregated payloads are forwarded to a 200G companion trunk card.

For a detailed list of the supported pluggables, see, http://www.cisco.com/c/en/us/td/docs/optical/spares/gbic/guides/b_ncs_pluggables.html

Operating Modes for MR-MXP Card

The MR-MXP card supports the following 200G operating modes:

- MXP-200G
- MXP-10x10G-100G
- MXP-CK-100G

Each operating mode can be configured using specific set of cards and client payloads. The operating mode is configured on the companion trunk card (100GS-CK-C or 200G-CK-C). For more information about these operating modes, see Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards, on page 198.

The MR-MXP card supports the following 100G operating modes:

- MXP-100G
- TXP-100G
- 100G-B2B

Note All 100G and 200G operating modes support the encryption feature except for the MXP-CK-100G mode.

MXP-100G

The MXP-100G operating mode is provisioned with MR-MXP card on the client side and the adjacent 200G-CK-C card or 100GS-CK-C card on the trunk side. The operating mode can be provisioned only from the client side but can be deleted from both client and trunk sides. This mode supports 10GE as the payload. This mode uses the SFP+ and QSFP+ ports on MR-MXP client card and the DWDM port on the 200G-CK-C card or 100GS-CK-C card. The aggregate signal from the client is sent to trunk through the backplane.

The MXP-100G operating mode is also provisioned with MR-MXP card on the client side and the adjacent 200G-CK-C card on the trunk side. The operating mode can be provisioned only from the client side but can be deleted from both client and trunk sides. This mode supports 2X10GE+2X40GE as the payload. This mode

uses the SFP+ and QSFP+ ports on MR-MXP client card and the DWDM port on the 200G-CK-C card. The aggregate signal from the client is sent to trunk through the backplane.

The operating mode can be provisioned on the following slots:

- NCS 2006: Slots 2 and 3, 4 and 5, 6 and 7
- NCS 2015: Slots 2 and 3, 4 and 5, 6 and 7, 8 and 9, 10 and 11, 12 and 13, 14 and 15

TXP-100G

TXP-100G operating mode is provisioned with MR-MXP card on the client side and the adjacent 200G-CK-C card or 100GS-CK-C card on the trunk side. The operating mode can be provisioned only from the client side but can be deleted from both client and trunk sides. This mode supports 100GE as the payload. This mode uses the CPAK port on MR-MXP client card and the DWDM port on the 200G-CK-C card or 100GS-CK-C card. The aggregate signal from client is sent to trunk through the backplane.

The operating mode can be provisioned on the following slots:

- NCS 2006: Slots 2 and 3, 4 and 5, 6 and 7
- NCS 2015: Slots 2 and 3, 4 and 5, 6 and 7, 8 and 9, 10 and 11, 12 and 13, 14 and 15

100G-B2B

The 100G-B2B operating mode can be provisioned with MR-MXP card on the client side and the adjacent MR-MXP card card on the trunk side. The operating mode performs encryption of an 100GE client signal taken from the CPAK interface or 10x10GE client signal taken from the two QSFP and SFP interfaces of the client MR-MXP card and maps it to an OTU4 signal with encryption. The OTU4 signal is passed to the trunk MR-MXP card in the peer slot through the back plane. The trunk MR-MXP card converts the OTU4 signal to grey wavelength with either an SR-10 or an LR-4 through the CPAK interface of the trunk card. The 100GE client payload can be divided into either four or 10 sub-lanes.

The CPAK port or two QSFP and 2 SFP+ ports can be selected on the client card during the provisioning. The operating mode can be provisioned from any MR-MXP card in the peer slot pair. When the operating mode is created, the card that the user selects to create operating mode acts as the client card and the peer card for that card acts as the trunk card.

The operating mode can be provisioned on the following slots:

- NCS 2006: Slots 2 and 3, 4 and 5, 6 and 7
- NCS 2015: Slots 2 and 3, 4 and 5, 6 and 7, 8 and 9, 10 and 11, 12 and 13, 14 and 15

The provisioning operations like payload/operating mode creation and FEC settings in 100G-B2B operating mode of MR-MXP card takes longer when compared to other operating modes.

Sub Operating Modes

The sub OpMode in MR-MXP cards determines the operating mode on the card client ports. For example, the QSFP+ port can be provisioned either as a 40GE port or can be divided into four 10G ports. This provisioning is controlled by the sub OpMode. The sub OpMode is created by default when the operating mode is configured on the card.

- OPM_10x10G—This is the default sub OpMode for the MXP-100G, MXP-200G, and MXP-10x10G-100G operating modes. In this sub OpMode, the SFP and QSFP+ ports are divided in such a way that 10 10GE payloads can be provisioned. When a PPM is provisioned on a QSFP+ port, four internal ports are created. A 10 GE payload can be provisioned on each of these ports. The OPM-10x10G operating mode is

provisioned with MR-MXP card on the client side and the adjacent MR-MXP card on the trunk side. The operating mode can be provisioned only from the client side but can be deleted from both client and trunk sides. The aggregate signal from client is sent to trunk through the backplane.

- OPM_100G—This is the default sub OpMode for the MXP-CK-100G operating mode where the CPAK port can be provisioned with a 100GE or OTU4 payload. The 100GE payload can be divided into either four or ten sub-lanes. For 100GE payload, the OPM-100G operating mode is provisioned with MR-MXP card on the client side and the adjacent MR-MXP card on the trunk side. For OTU4 payload, the OPM-100G operating mode is provisioned with MR-MXP card on the client side and the adjacent 200G-CK-C card on the trunk side.The operating mode can be provisioned only from the client side but can be deleted from both client and trunk sides. The aggregate signal from client is sent to trunk through the backplane.
- OPM_2x40G_2x10G—This sub OpMode is provisioned for the MXP-100G operating mode to support the 2X10GE+2X40GE payload. This operating mode is provisioned with MR-MXP card on the client side and the adjacent 200G-CK-C card on the trunk side. The operating mode can be provisioned only from the client side but can be deleted from both client and trunk sides. The aggregate signal from client is sent to trunk through the backplane.

  This sub OpMode is also provisioned for the MXP-200G operating mode to support the following sub OpMode combinations on both peer and skip MR-MXP cards.

  - OPM_10x10G and OPM_10x10G
  - OPM_2x40G_2x10G and OPM_2x40G_2x10G
  - OPM_2x40G_2x10G and OPM_10x10G
  - OPM_10x10G and OPM_2x40G_2x10G

Limitations for MR-MXP Card

- Line timing is not supported.
- GCC0 communication channel is not supported.
- Overclocking of OTU2 payload is not supported.
- Y cable protection is not supported.
- Only G-FEC is supported on OTN payloads.
- The lanes in a QSFP+ port support only homogeneous payloads.
- Terminal loopback on the client port is not supported for the CPAK-FRS pluggable.
- In MXP-CK-100G-CPAK operating mode, when the MR-MXP card with a CPAK-FRS client pluggable is rebooted or chassis power cycled, the traffic in the transmit direction does not recover. To recover the traffic, you must delete and recreate the operating mode.

100G-LC-C, 100G-CK-C, 100GS-CK-C, and 200G-CK-C Cards

100G-LC-C and 100G-CK-C Cards

In this chapter, "100G-LC-C" refers to the _15454-M-100G-LC-C card. "100G-CK-C" refers to the NCS2K-100G-CK-C card.

The 100G-LC-C and 100G-CK-C cards are tunable DWDM trunk cards. These cards simplify the integration and transport of 100-Gigabit Ethernet interfaces and services to enterprises or service provider optical networks. The 100GS-CK-C and 200G-CK-C cards simplify the integration and transport of 100 and 200-Gigabit Ethernet interfaces and services to enterprises or service provider optical networks. These cards are supported on Cisco NCS 2006 and Cisco NCS 2015 platforms.

The cards interoperate with 10x10G-LC and CFP-LC cards through a chassis backplane.

Note The 100GS-CK-C and 200G-CK-LC cards do not operate with the CFP-LC card.

The cards provide the following benefits:

- Provide 100-Gbps wavelengths transport over fully uncompensated networks, with more than 2,500 km of unregenerated optical links
- Enable 100-Gbps transport over very high Polarization Mode Dispersion (PMD)
- Improve overall system density of up to 100-Gbps per slot, which is five times greater than what can be achieved with 40-Gbps units

You can install up to six cards per Cisco NCS 2006 shelf, supporting up to 42 100-Gbps interfaces per 42-rack units (RU) bay frame. It is possible to place up to two 100G TXPs, one 100 G Regen, or one 100 G MXP on a Cisco NCS 2006 shelf.

Note You must instal the fan-tray assembly NCS2006-FTA= (for the NCS 2006 chassis) on the shelf, where the cards are installed. When you use an ONS-SC+-10G-C pluggable along with the 10x10G-LC card, the maximum operating temperature of the shelf must not exceed 50 degrees Celsius.

The 100G-CK-C card works in a similar way as the 100G-LC-C card. The 100G-CK-C card has the new CPAK client interface replacing the CXP client interface of the 100G-LC-C card. The CPAK client interface enables different payload combinations, and so this card can be used instead of the 100G-LC-C and CFP-LC cards.

The 100G-CK-C card supports the following pluggables:

- CPAK-100G-SR10 pluggable with 100GE/OTU4 and 40GE payloads
- CPAK-100G-LR4 pluggable with 100GE/OTU4 payloads
- CPAK-100G-SR4 pluggable with 100GE payloads

The 100G-LC-C card supports the following client signal types:

- 100GE/OTU4
- OTU4 from BP OTL4.10 (interconnect with the CFP client)
- 100GE from BP CAUI (interconnect with CFP client)
- 3 x OTU3e(255/227) from BP OTL3.4 (interconnect with 10 x10G client)
- 2 x OTU3 from BP OTL3.4 (interconnect with the CFP client)
- 2 x 40 GE from BP XLAUI (interconnect with the CFP client)

In addition to the above, the 100G-CK-C card supports the following client signal types:

- 100GE/OTU4 for the CPAK-100G-SR10/CPAK-100G-LR4 client interface
- 40GE for the CPAK-100G-SR10 client interface

The 100G-LC-C card and 100G-CK-C cards provide a 100G DWDM trunk interface that supports up to 70000 ps/nm of CD robustness. These cards enable configuration of the CD dispersion tolerance to 50000 ps/nm and 30000 ps/nm to reduce power consumption.

100GS-CK-C and 200G-CK-C Cards

In this chapter, "100GS-CK-C" refers to the NCS2K-100GS-CK-C card. "200G-CK-C" refers to the NCS2K-200G-CK-C card.

The 100GS-CK-C and 200G-CK-C cards are tunable DWDM trunk cards, which simplify the integration and transport of 100 and 200- Gigabit Ethernet interfaces and services to enterprises or service provider optical networks. The 200G-CK-C card is an enhancement of the 100GS-CK-C card.

The 100GS-CK-C and 200G-CK-C cards provide the following benefits:

- Allow choosing 16 QAM and QPSK as the modulation formats at the line side
- Provide Standard G-FEC (Reed-Solomon), Soft Decision FEC (SD-FEC) encoding with 20% overhead, and Hard Decision FEC (HD-FEC) encoding with 7% overhead
- Provide Nyquist filtering for best performance and optimal band usage
- Support gridless tunability
- Allow client access either through the local 100G CPAK interface or through backplane lines
- In MXP-10X10G operating mode, allow 10GE clients (multiplexed on 100G trunk)

Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards

The 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP cards support the following key feature:

- Operating Modes—You can configure the cards into multiple operating modes. The cards can be equipped with pluggables for client and trunk options, and offer large variety of configurations. When you configure the card into multiple operational modes, make sure that you complete the following tasks:

- The card must be preprovisioned and the modes must be configured. None of the modes are provisioned on the card by default. All operating modes are created on the card level. These are card-specific provisioning, which decides the behavior of a particular card.
- Depending on the card mode selected, the supported payload for that particular card mode must be provisioned on the PPMs. The payloads can be provisioned after configuring the operational mode on the card.

For a detailed list of the supported pluggables, see, http://www.cisco.com/c/en/us/td/docs/optical/spares/gbic/guides/b_ncs_pluggables.html.

For operating modes of the respective cards, see the Operating Modes for 10x10G-LC Card, Operating Modes for CFP-LC Card, Operating Modes for MR-MXP Card, on page 194, and Operating Modes for 100G-LC-C, 100G-CK-C, 100GS-CK-C, and 200G-CK-C Cards, on page 202.

- Protocol Transparency—The 100G-LC-C, 100G-CK-C, 100GS-CK-C, and 200G-CK-C cards deliver any 100-Gbps services for cost-effective, point-to-point networking. The 10x10G-LC card delivers any 10-Gbps services for cost-effective, point-to-point networking. In case of 100 G muxponder clients that are mapped into OTU4 DWDM wavelength.

Table 28: Transponder Client Configurations and Mapping for 100G-LC-C and 100G-CK-C Cards

Client			Trunk	
Format	Rate (Gbps)	Mapping	Format	Rate with 7% GFEC, 20% GFEC, or EFEC OH (Gbps)
100GE LAN-PHY	101.125	Bit transparent through standard G.709v3 mapping	OTU4	111.809
OTU4	111.809	Transparent G.709 standard		

Table 29: Transponder Client Configurations and Mapping for a 10x10G-LC Card

Client		Mapping
Format	Rate (Gbps)	
10GE LAN-PHY (MXP-10x10G mode)	10.3125	CBR-BMP clause 17.2.4 (ex G sup43 7.1) + GMP ODU2e to OPU3e4
10GE LAN-PHY (MXP-10x10G mode)	10.3125	GFP-F clause 17.4.1 (ex G sup43 7.3) + GMP ODU2 to OPU3e4
10GE LAN-PHY (TXP-10G mode)	10.3125	CBR-BMP clause 17.2.4 (ex G sup43 7.1)

Client		Mapping
Format	**Rate (Gbps)**	
10GE LAN-PHY (TXP-10G mode)	10.3125	GFP-F clause 17.4.1 (ex G sup43 7.3)
OTU2	10.709	ODU transparent + GMP ODU2 to OPU3e4
OTU2e	11.095	ODU transparent + GMP ODU2e to OPU3e4
IB-5G	5.0000	GMP ODU2e to OPU3e4

Table 30: Client Configurations and Mapping for CFP-LC Card

Client			Trunk	
Format	**Rate (Gbps)**	**Mapping**	**Format**	**Rate with 7% GFEC or EFEC OH (Gbps)**
100GE LAN-PHY	101.125	Bit transparent through standard G.709v3 mapping	OTU4	111.809
OTU4	111.809	Transparent G.709 standard		
40GE LAN-PHY	41.250	1024b/1027b transc + OPU4 GMP G709 Appendix VIII		
OTU3	43.018	Transparent G.709 standard		

- Flow-Through Timing—The cards allow the timing to flow through from the client to line optical interface. The received timing from the client interface is used to time the line transmitter interface. This flow-through timing allows multiple cards to be placed in the same shelf but be independently timed fully, independent of the NE timing.
- Far-End Laser Control (FELC)—FELC is supported on the cards.
- Performance Monitoring—The 100-Gbps DWDM trunk provides support for both transparent and non-transparent signal transport performance monitoring. The Digital Wrapper channel is monitored according to G.709 (OTN) and G.8021 standards. Performance Monitoring of optical parameters on the client and DWDM line interface include loss of signal (LOS), Laser Bias Current, Transmit Optical Power, and Receive Optical Power. Calculation and accumulation of the performance monitoring data is supported in 15-minute and 24-hour intervals as per G.7710. Physical system parameters measured at the wavelength level, like Mean PMD, accumulated Chromatic Dispersion, or Received OSNR, are also included in the set of performance monitoring parameters. These measurements can greatly simplify troubleshooting operations and enhance the set of data which can be collected directly from the equipment. The performance monitoring for the CFP-LC card takes into account the fact that the two CFP-LC cards

are a host board supporting CFP client equipment. The digital monitoring takes into account the fact that if the incoming client is implemented on the 100G cards. There is a virtual port connection that displays the Digital Wrapper monitoring according to G.709 (OTN) and the RMON for Ethernet signals, while the optical performance monitoring is directly available on the two CFP-LC cards. Calculation and accumulation of the performance monitoring data is supported in 15 minute and 24 hour intervals according to G.7710.

- Loopback—The terminal, facility, or backplane loopback can be provisioned on all the ports of the 100G-LC-C, 100G-CK-C, 10x10G-LC, 100GS-CK-C, and 200G-CK-C cards, configured in any operating mode except for the low latency mode. The backplane facility loopback cannot be configured on the 10x10G -LC card that is configured in the MXP-10x10G mode. The loopback can be provisioned only when the port is in OOS-MT state. A new port cannot be provisioned when the backplane loopback is configured on the 10x10G-LC card. For the CFP-LC card configured in the CFP-TXP or CFP-MXP mode, the facility or terminal loopback can be configured on the backplane of the peer 100G-LC-C, 100G-CK-C, 100GS-CK-C, and 200G-CK-C cards. Terminal and facility loopback can be provisioned on MR-MXP cards that are configured in any operating mode.
- Fault propagation on 10GE, 40GE, and 100GE clients—A new squelch option that is named LF is supported for GigE payloads. A local fault (LF) indication is fowarded to the client port in the downstream direction when a failure on the trunk port occurs. The LF option is supported for:
  - 10GE payloads on 10x10G-LC cards configured in the:
    - RGN-10G or TXP-10G mode
    - MXP-10x10G mode (paired with 100G-LC-C, 100G-CK-C, or 100GS-CK-C card)
    - MXP-10x10G-100G mode (paired with a 100GS-CK-C or 200G-CK-C card)
  - 100GE payloads on:
    - 100G-LC-C, 100G-CK-C, 100GS-CK-C, or 200G-CK-C cards configured in the TXP-100G mode
    - CFP-LC cards configured in the CFP-TXP mode (paired with 100G-LC-C or 100G-CK-C card)
  - 40GE payloads on:
    - CFP-LC card configured in the 2x40G Muxponder mode (paired with a 100G-LC-C or 100G-CK-C card)
    - 100G-CK-C card configured in the MXP-2x40G mode
- Trail Trace Identifier—The Trail Trace Identifier (TTI) in the path monitoring overhead is supported in OTU, and ODU OTN frames.
  - 10x10G-LC—OTU4 and ODU4 payloads
  - CFP-LC—OTU4, ODU4, OTU3, and ODU3 payloads
  - 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C—OTU4 and ODU4 payloads

  The Trail Trace Identifier Mismatch (TTIM) alarm is raised after checking only the SAPI bytes.

- Automatic Laser Shutdown (ALS) can be configured on all ports. ALS is supported only on the ports that are configured with OTU2 and OTU4 payloads.
- GCC channels—can be provisioned on the OTU2 client and trunk ports of the 10 x10G-LC card, OTU3 port (virtual port on the peer 100G-LC-C or 100G-CK-C card) of the CFP-LC card, and the OTU4 client and trunk ports of the 100G-LC-C or 100G-CK-C card.
- Pseudo Random Binary Sequence (PRBS)—PRBS allows you to perform data integrity checks on their encapsulated packet data payloads using a pseudo-random bit stream pattern. PRBS generates a bit pattern and sends it to the peer router that uses this feature to detect whether the sent bit pattern is intact or not. The supported PRBS patterns are PRBS_NONE and PRBS_PN31.
- Multivendor Interoperability - The 200G-CK line card can be configured to interoperate with other vendor interfaces. A new option called, Interop Mode is available to disable or enable interoperability. This option is available when the:
  - Modulation format is 100G-QPSK.
  - FEC is set to 7% High Gain FEC.
  - Admin state of the trunk port is set to OOS-DSBLD (Out of service and disabled).

  The behavior and performance of the card that is configured with HG-FEC Multivendor FEC is the same as the old HG-FEC mode. There is no optical performance variation.

Operating Modes for 100G-LC-C, 100G-CK-C, 100GS-CK-C, and 200G-CK-C Cards

Each operating mode can be configured using the specific set of cards and client payloads. The Key Features of 100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C, 10x10G-LC, CFP-LC, and MR-MXP Cards section lists the valid port pair for a specific operating mode and the supported payloads, and describes how each mode can be configured.

100G Operating Modes

The 100G-LC-C, 100G-CK-C, 100GS-CK-C, and 200G-CK-LC cards support the following 100G operating modes. You can perform the operating mode configuration for the 100G operating modes on the client card.

- TXP-100G (Standalone 100GE Transponder)
- RGN-100G (100G Regenerator)

TXP-100G (Standalone 100GE Transponder)

You can configure the cards as a standalone 100-Gigabit Ethernet transponder. CXP or CPAK and coherent optical trunk supports the 100-Gigabit Ethernet traffic. The 100-Gigabit Ethernet or OTU4 payload traffic is routed from the CXP or CPAK to the optical trunk, passing through the T100 framer and the opposite way. The supported client signals in this mode are 100-Gigabit Ethernet LAN-PHY or OTU4 data rates.

RGN-100G (100G Regenerator)

You can configure the cards as a regenerator. You can connect the two cards to work in back-to-back mode connecting through the chassis backplane in the same shelf. The allowed slot pairs are 2–3, 4–5, 6–7, 8–9, 10–11, 12–13, or 14–15.

The card supports 100-Gigabit Ethernet or OTU4 client signals. Regeneration is performed leveraging on the OTU4 backplane interconnection. OTU4 overhead is terminated, allowing ODU4 to transparently pass through. GCC0 is terminated, while GCC1 and GCC2 are allowed to pass through.

The CXP client is not required because communication between the two cards acting as a regeneration group is supported through the chassis backplane.

MXP-2x40G

The 100G-CK-C card supports the MXP-2x40G operating mode. The 100G-CK-C card can be configured as a 2-port 40 GE muxponder. Two 40 GE flows through the CPAK client interface and are multiplexed in the 100G trunk interface. You can configure the traffic on the second client interface only after provisioning the traffic on the first client interface. This operating mode is not supported on the 100GS-CK-C card.

Note The synchronization for the 100G-CK-C card is derived only from port 1. Hence, the traffic on port 2 must originate from the same synchronization source as port 1. The two ports must carry traffic from the same synchronization source.

200G Operating Modes

The 100GS-CK-C and 200G-CK-LC cards also support the 200G operating modes. You can perform the operating mode configuration for these modes on the trunk card.

- MXP-200G
- MXP-10x10G-100G
- MXP-CK-100G

MXP-200G

Three cards such as a trunk card, a peer card, and a skip card are required to configure this operating mode. The skip card is next to the peer card.

The trunk card is a 100GS-CK-C or 200G-CK-LC card; the peer card and skip cards are MR-MXP. You can use the first 10x10G from the two SFP and two QFSP+ ports of the peer MR-MXP card. You can use the second 10x10G from the two SFP and two QFSP+ ports of the skip MR-MXP card.

The 200G-CK-LC card supports another configuration in the MXP_200G operating mode. In this configuration, 2x40GE clients on QSFP+ ports and 2x10GE clients on SFP+ ports of both peer MR-MXP and skip MR-MXP cards are multiplexed into 200G traffic on the trunk 200G-CK-LC card.

You can provision the operating mode on the following slots:

- NCS 2006: 100GS-CK-C or 200G-CK-LC card in slots 2 or 7. The peer and skip MR-MXP cards in adjacent slots 3, 4 or 5, 6.
- NCS 2015: 100GS-CK-C or 200G-CK-LC card in slots 2, 7, 8, 13, or 14. The peer and skip MR-MXP cards in adjacent slots.

MXP-10x10G-100G

You require three cards such as the trunk card, peer card, and skip card to configure this operating mode.

The trunk card is a 100GS-CK-C or 200G-CK-LC card; the peer card is a 10x10G-LC and the skip card is a MR-MXP.card You can use the first 10x10G from the ten SFP ports of the peer 10x10G-LC card. You can use the second 10x10G from the two SFPs and two QFSP+ ports of the skip MR-MXP card.

You can provision the operating mode on the following slots:

- NCS 2006: The 100GS-CK-C or 200G-CK-LC card in slots 2 or 7, peer, and skip MR-MXP cards in adjacent slots 3, 4 or 5, 6.
- NCS 2015: The 100GS-CK-C or 200G-CK-LC card in slots 2, 7, 8, 13, or 14, peer, and skip MR-MXP cards in adjacent slots.

MXP-CK-100G

Two cards, trunk and peer cards, are required to configure this operating mode. The trunk card is 100GS-CK-C or 200G-CK-LC; the peer card is MR-MXP. The first 100G is taken from the CPAK client port of the trunk 100GS-CK-C or 200G-CK-LC card and the second 100G is taken from the CPAK client port of the MR-MXP card.

200G-CK-LC card supports another configuration in the MXP_CK_100G operating mode. In this configuration, 10x10GE clients on QSFP+ or SFP+ ports of the peer MR-MXP card and 100GE client on the CPAK port of the 200G-CK-LC card are multiplexed into a 200G configuration on the trunk 200G-CK-LC card.

The operating mode can be provisioned on the following slots:

- NCS 2006: 100GS-CK-C or 200G-CK-LC card and the peer MR-MXP card must be in adjacent slots 2–3, 4–5, and 6–7.
- NCS 2015: 100GS-CK-C or 200G-CK-LC card and the peer MR-MXP card must be in adjacent slots 2–3, 4–5, 6–7, 8–9, 10–11, 12–13, and 14–15.

400G-XP-LC400G-XP Card

In this chapter, "400G-XP" refers to the NCS2K-400G-XP card.

The 400G-XP-LC400G-XP card is a tunable DWDM trunk card that simplifies the integration and transport of 10 Gigabit and 100 Gigabit Ethernet interfaces and services to enterprises and service provider optical networks. The card is a double-slot unit that provides 400 Gbps of client and 400 Gbps of trunk capacity. The card supports six QSFP+ based client ports that can be equipped with 4x 10 Gbps optics and four QSFP28 or QSFP+ based client ports that can be equipped with 100 Gbps QSFP28 and 4x 10 Gbps QSFP+ optics. The card is capable of aggregating client traffic to either of the two 200 Gbps coherent CFP2 trunk ports. The CFP2 - 11 trunk port of the 400G-XP-LC400G-XP card can interoperate with the 10x10G-LC card through the chassis backplane. To enable this interoperability between the 400G-XP-LC400G-XP and 10x10G-LC cards, the OPM_PEER_ODU2 and OPM_PEER_ODU2e slice modes are supported on Slice 2 when the 400G-XP-LC400G-XP card is configured in the MXP mode.

The table below details the layout constraints when the 400G-XP-LC400G-XP card is paired with the 10x10G-LC card in the Cisco NCS 2006 and Cisco NCS 2015 chassis.

Table 31: Slot Constraints for the 400G-XP-LC400G-XP and 10x10G-LC Cards

Chassis	Slot (10x10G-LC)	Slot (400G-XP)	Notes
Cisco NCS 2006	2	3-4	Only one of these two combinations can be deployed at a time.
	4	5-6	
NCS 2015	2	3-4	A maximum of four of these combinations can be deployed at a time.
	4	5-6	
	6	7-8	
	8	9-10	
	10	11-12	
	12	13-14	
	14	15-16	

The 400G-XP-LC400G-XP card supports the following client signals:

- 10 GE: The payload can be provisioned for the OPM_10x10G, OPM_PEER_ODU2, or OPM_PEER_ODU2e slice mode for any trunk configuration. 10GE is provisioned for the OPM_PEER_ODU2 and OPM_PEER_ODU2e slice modes in the GFP and CBR mapping modes respectively. The cross-connect circuit bandwidth is ODU2e.
- 100 GE: The payload can be provisioned for the OPM_100G slice mode for any trunk configuration. The cross-connect circuit bandwidth is ODU4.
- OTU2: This payload is supported only on the QSFP-4X10G-MLR pluggable. The payload can be provisioned for the OPM_10x10G or OPM_PEER_ODU2 slice mode for any trunk configuration. The cross-connect circuit bandwidth is ODU2.
- OTU2e: This payload is supported only on the QSFP-4X10G-MLR pluggable. The payload can be provisioned for the OPM_10x10G or OPM_PEER_ODU2e slice mode for any trunk configuration. The cross-connect circuit bandwidth is ODU2e.
- OC192/STM64: This payload is supported only on the QSFP-4X10G-MLR pluggable. The payload can be provisioned for the OPM_10x10G or OPM_PEER_ODU2 slice mode for any trunk configuration. The cross-connect circuit bandwidth is ODU2.

Note This payload is not supported for R 12.0.

- OTU4: This payload is supported only on the ONS-QSFP28-LR4 pluggable. The payload can be provisioned for the OPM_100G slice mode for any trunk configuration. The cross-connect circuit bandwidth is ODU4.

Note For any card mode except REGEN with slide mode as OPM-10x10G, you can configure a mix of 10G payloads (OTU2, 10GE) on the same slice or client port with the exception of CDR ports (7, 8, 9, and 10). On CDR ports, the first configured 10G lane would determine the configurable payloads for the other three port lanes.

Note If a slice is configured using the OPM_10x10G slice mode, it can be used only for 10G circuit creation whereas if a slice is configured using the OPM_100G slice mode, it can be used only for 100G circuit creation.

Note Until R11.1, ODU alarms and PMs on cross-connected trunks ODUs are raised under the OTU4C2 trunk port of the 400G-XP card for both near-end and far-end directions. From R11.1, ODU alarms and PMs are raised under the specific cross-connected trunks ODUs for both near-end and far-end directions for OTU4 client payload. OTN alarms and PMs are raised under the OTU4C2 trunk port of the 400G-XP card for both near-end and far-end directions.

Note GCC Rate in the Edit GCC Termination Window is shown as 192K instead of the supported 1200K. This is a known behavior.

The 400G-XP-LC400G-XP card is supported on Cisco NCS 2002, Cisco NCS 2006, and Cisco NCS 2015 platforms.

One 400G-XP-LC400G-XP card can be installed in the Cisco NCS 2002 DC chassis that is powered by NCS2002-DC or NCS2002-DC-E. Three 400G-XP-LC400G-XP cards can be installed in the Cisco NCS 2006 chassis that is powered by NCS2006-DC, NCS2006-DC40, or NCS2006-AC (180V AC to 264V AC). Seven 400G-XP-LC400G-XP cards can be installed in the Cisco NCS 2015 chassis that is powered by DC 2 + 2, DC 3 + 1, or AC 2 + 2 PSU.

Limitations

- Terminal loopback on the client port is not supported for the QSFP28-FRS pluggable.
- Terminal loopback is not supported on the client port having non-FRS pluggable at the near-end node when the peer client port at the far-end node has QSFP28-FRS pluggable or vice versa.
- Encrypted traffic is not supported on the client port with a QSFP28-FRS pluggable.

Note The maximum short term operating temperature of the Cisco NCS 2002 shelf must not exceed 50 degrees when the 400G-XP card is installed.

Note You may observe traffic glitches on the receiving direction of client ports 7, 8, 9, and 10 on the 400G-XP-LC card that you connect to CXP port of a 10x10G-LC card in fanout mode. To bringup traffic in such cases, change the admin state of the CXP port from **OOS-DSBLD** state to **IS-NR** state. Repeat the same action if you continue to observe glitches.

For more information about the 400G-XP card, see http://www.cisco.com/c/en/us/products/collateral/optical-networking/network-convergence-system-2000-series/datasheet-c78-736916.html.

Key Features

The 400G-XP card supports the following key feature:

- • Operating Modes—The card can be configured in various operating modes. The cards can be equipped with pluggables for client and trunk ports, and offer a large variety of configurations. When you configure the card, make sure that the following tasks are completed:
  - The trunk port PPMs must be preprovisioned before configuring the card operating mode. When the 400G-XP card is paired with the 10x10G-LC card, all the operating mode provisioning must performed on the 400G-XP card. The client payloads can be provisioned after configuring the operational mode on the card.

  The table below details the configurations supported on the 400G-XP card for the supported card modes.

Table 32: Configuration Options for the 400G-XP Card Modes

Configuration	**Options**			
Card configuration	MXP	OTNXC [1]	REGEN	MXP_2x150G (8QAM)
Trunk configuration (per trunk)	None	None	None	M_150G
	M_100G	M_100G	M_100G	
	M_200G	M_200G	M_200G	

Configuration	Options			
Slice configuration	None	None	Slice configuration is not supported	None
	OPM_2x40G_2x10G	OPM_100G		OPM_100G
	OPM_100G	OPM_10x10G		OPM_10x10G
	OPM_10x10G			OPM_6x16G_FC
	OPM_6x16G_FC			
	OPM_PEER_ODU2 (Available only for Slice 2 when 400G-XP is paired with 10x10G-LC)			
	OPM_PEER_ODU2e (Available only for Slice 2 when 400G-XP is paired with 10x10G-LC)			

[1] Not supported in R12.0

For more information about the trunk and slice configuration, see Slice Definition and Line Card Configuration for 400G-XP Card, on page 213.

- Each trunk port functions as a muxponder instance has the following features:
  - The trunk port supports Analog Coherent Optical (ACO) CFP2 coherent pluggable.

Note Before removing the CFP2 pluggable from any of two trunk ports, ensure that the relevant trunk port is set to the OOS (Out-of-service) state. Wait until the trunk port LED turns off. Wait for a further 120 seconds before extracting the CFP2 pluggable.

  - Configurable trunk capacity:
    - 100 Gbps coherent DWDM transmission with quadrature phase shift keying (QPSK)modulation.
    - 200 Gbps coherent DWDM transmission with 16-state quadrature amplitude modulation (16-QAM) modulation.
  - Configurable trunk FEC: SD-FEC with 15% or 25% overhead.
  - Configurable differential/non-differential line encoding.
  - Nyquist shaping if channels at trunk TX.
  - Flex spectrum tunability over the full extended C-Band.
  - 100 Gbps through 100 Gbps QSFP28 client ports.

- 10 Gbps through 4x 10 Gbps QSFP+ client ports.
- 16 Gbps through 4 x 16 Gbps QSFP+ client ports.

- The supported CD ranges are detailed in the table below:

Table 33: CD Range for 400G-XP Card

	200G 16-QAM		100G QPSK	
	Low	High	Low	High
Default Working CD Range	-10000	50000	-20000	90000
Default CD Thresholds	-9000	45000	-18000	72000
Allowed CD Range (Working and Thresholds)	-60000	60000	-280000	280000

- Loopback—The following loopback types are supported:
  - Client ports - Terminal (Inward), Facility (Line)
  - Trunk ports - Terminal (Inward)
  - Iports - Facility (Line), Terminal loopback (Drop)

Note Before you provision loopback on the iports, place the relevant trunk ports in the OOS-MT state. This causes the iports to move to the OOS-MT state.

- Automatic Laser Shutdown (ALS) can be configured on all the ports.
- 100GE ethernet client ports can be provisioned with or without IEEE 802.3 bj FEC. The options are Auto, Force-Fec-On, Force-Fec-Off.
- Trail Trace Identifier (TTI)—TTI in the section monitoring overhead is supported . Source Access Point Identifer (SAPI), Destination Access Point Identifer (DAPI), and User Operator Data fields are supported in Release 10.6.2 and later releases.
- Trunk Port Interworking—The two CFP2 trunk ports can interoperate with each other when the source and destination 400G-XP cards have the same trunk mode and slice mode configuration. For more information, see Trunk Port Interworking in 400G-XP Cards, on page 218.
- GCC0 Support—The 400G-XP card supports provision of GCC0 channel on the trunk port. For more information, see GCC0 Support on the 400G-XP Card, on page 221.
- Interoperability—The 400G-XP card is interoperable with the NC55-6X200-DWDM-S card supported on NCS 5500 and the NCS4K-4H-OPW-QC2 Card supported on NCS 4000.

  The following table describes the configurations, payload types, and pluggables supported for interoperability between the 400G-XP card and the NCS4K-4H-OPW-QC2 card.

Table 34: 400G-XP Interoperability with the NCS4K-4H-OPW-QC2 card.

Payload type	Trunk configuration	Pluggables for trunk ports on 400G-XP	Pluggables for client ports on 400G-XP	Pluggables for trunk ports on 4H-OPW-QC2	Pluggables for client ports on 4H-OPW-QC2
100GE	OTU4	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S
100GE	OTU4C2	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S
OTU2	OTU4	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP28-LR4
OTU2	OTU4C2	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP28-LR4
10GE	OTU4	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP-4X10 MLR
10GE	OTU4C2	CFP2	ONS-QSFP-4X10 MLR	CFP2	ONS-QSFP-4X10 MLR

The following table describes the configurations, payload types, and pluggables supported for interoperability between the 400G-XP card and the NC55-6X200-DWDM-S card.

Table 35: 400G-XP Interoperability with the NC55-6X200-DWDM-S card.

Payload type	Trunk configuration	Pluggables for trunk ports on 400G-XP	Pluggables for client ports on 400G-XP	Pluggables for trunk ports on 6X200-DWDM-S	Pluggables for client ports on 6X200-DWDM-S
100GE	OTU4	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S
100GE	OTU4C2	CFP2	QSFP-100G-SR4-S	CFP2	QSFP-100G-SR4-S

For a detailed list of the supported pluggables, see http://www.cisco.com/c/en/us/td/docs/optical/spares/gbic/guides/b_ncs_pluggables.html .

Interoperability

The 400G-XP card has two trunk ports, each supporting up to 20 ODU2es. These ODU2es are numbered from 1 through 20. ODU2es 1 through 10 belong to the first ODU4 slice and ODU2es 11 through 20 belong to the second ODU4 slice. Each ODU number has a pre-defined group of timeslots as seen in the following table.

Trunk Port	ODU4 Slice	ODU Trunk Number	ODU Trunk FAC	Tributary Port Number	Timeslots
Trunk 1 (FAC 10)	Slice 1	1	96	1	1 11 21 31 41 51 61 71

Trunk Port	ODU4 Slice	ODU Trunk Number	ODU Trunk FAC	Tributary Port Number	Timeslots
		2	97	2	2 12 22 32 42 52 62 72
		3	98	3	3 13 23 33 43 53 63 73
		4	99	4	4 14 24 34 44 54 64 74
		5	100	5	5 15 25 35 45 55 65 75
		6	101	6	6 16 26 36 46 56 66 76
		7	102	7	7 17 27 37 47 57 67 77
		8	103	8	8 18 28 38 48 58 68 78
		9	104	9	9 19 29 39 49 59 69 79
		10	105	10	10 20 30 40 50 60 70 80
	Slice 2	11	106	1	1 11 21 31 41 51 61 71
		12	107	2	2 12 22 32 42 52 62 72
		13	108	3	3 13 23 33 43 53 63 73
		14	109	4	4 14 24 34 44 54 64 74
		15	110	5	5 15 25 35 45 55 65 75
		16	111	6	6 16 26 36 46 56 66 76
		17	112	7	7 17 27 37 47 57 67 77
		18	113	8	8 18 28 38 48 58 68 78

Trunk Port	ODU4 Slice	ODU Trunk Number	ODU Trunk FAC	Tributary Port Number	Timeslots
		19	114	9	9 19 29 39 49 59 69 79
		20	115	10	10 20 30 40 50 60 70 80
Trunk 2 (FAC 11)	Slice 1	1	116	1	1 11 21 31 41 51 61 71
		2	117	2	2 12 22 32 42 52 62 72
		3	118	3	3 13 23 33 43 53 63 73
		4	119	4	4 14 24 34 44 54 64 74
		5	120	5	5 15 25 35 45 55 65 75
		6	121	6	6 16 26 36 46 56 66 76
		7	122	7	7 17 27 37 47 57 67 77
		8	123	8	8 18 28 38 48 58 68 78
		9	124	9	9 19 29 39 49 59 69 79
		10	125	10	10 20 30 40 50 60 70 80
	Slice 2	11	126	1	1 11 21 31 41 51 61 71
		12	127	2	2 12 22 32 42 52 62 72
		13	128	3	3 13 23 33 43 53 63 73
		14	129	4	4 14 24 34 44 54 64 74
		15	130	5	5 15 25 35 45 55 65 75

Trunk Port	ODU4 Slice	ODU Trunk Number	ODU Trunk FAC	Tributary Port Number	Timeslots
		16	131	6	6 16 26 36 46 56 66 76
		17	132	7	7 17 27 37 47 57 67 77
		18	133	8	8 18 28 38 48 58 68 78
		19	134	9	9 19 29 39 49 59 69 79
		20	135	10	10 20 30 40 50 60 70 80

When the 400G-XP card interoperates with the NCS4K-4H-OPW-QC2 card, the first ODU4 slice of the 400G-XP trunk is connected to the second ODU4 slice of the same NCS4K-4H-OPW-QC2 trunk.

Note The ODU circuit between the 400G-XP and NCS4K-4H-OPW-QC2 cards is created even when the ODU number is incorrect. Please ensure that the correct source and destination ODU numbers are selected.

Regeneration Mode for 400G-XP

From Release 10.8.0, the 400G-XP can be configured as a regenerator. The regeneration functionality is available only on the trunk ports. A new card operating mode, REGEN, is available. No client ports are involved. The two trunk ports must have the same rate to achieve regeneration (wavelengths and FEC of the trunks can vary).

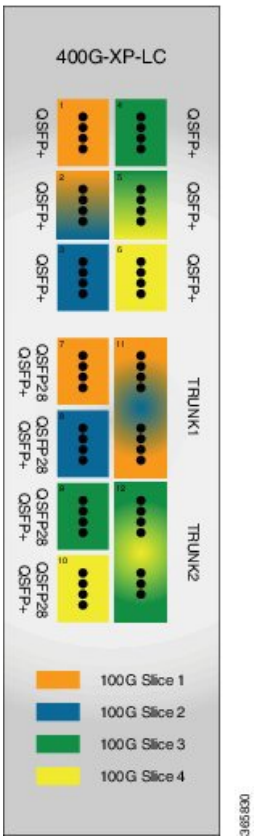
Note For traffic to flow in the REGEN mode, it is mandatory that the 400G-XP should be running on firmware (SCP) version 5.24 or later.

We recommend that you use the REGEN mode only with the MXP operating mode (the output from the MXP trunk of a 400G-XP can be connected to trunk ports in REGEN mode).

Slice Definition and Line Card Configuration for 400G-XP Card

The image below displays the client and trunk ports of the 400G-XP card.

Figure 18: 400G-XP Card



The client to trunk port mapping is fixed in the 400G-XP card as detailed in this table:

Table 36: Trunk -Client Port Mapping on the 400G-XP Card

Trunk	Client Port	Pluggable Type
Trunk 1 (CFP2-11)- Slice 1 and Slice 2	Ports 1, 2, 3	QSFP+
	Ports 7, 8	QSFP+ or QSFP28 [2]
Trunk 2 (CFP2-12) - Slice 3 and Slice 4	Ports 4, 5, 6	QSFP+
	Ports 9, 10	QSFP+ or QSFP28

[2] QSFP+ and QSFP28 share the same form factor.

The trunk ports can be configured with either 100G or 200G rates. The client ports are grouped into four slices. The slice mode defines the aggregation capacity and can be configured independently.

The configuration of each of the two trunk ports is independent of the configuration of the other and is done using either one of the two trunk operating modes.

Trunk Operating Modes (trunk capacity)

- M-100G: 100G QPSK. One slice is enabled on the trunk. Slice 2 is enabled for Trunk 1 and Slice 4 is enabled on Trunk 2.

- M-200G: 200G 16 QAM. Two slices are enabled on the trunk.
- provision a ONS-QC-16GFC-SW= pluggable on the shared ports and have 6x 16G-FC payloads and 8x 10G payloads (10GE or OTU2)
- provision a QSFP-4X10G-MLR (or ONS-QSFP-4X10G-LR-S) pluggable on the shared ports and have 4x 16G-FC + 10x 10G payloads (10GE and/or OTU2)

Slice Mode:

- OPM-100G: Enables 100G client on the QSFP 28 port.
- OPM-10x10G: Enables 10G client over a set of QSFP+ ports.
- OPM_2x40G_2x10G: Enables 40G client over a set of QSFP+ ports.

Traffic from the client ports are aggregated on the 100G or 200G trunk at the intermediate ports. There are four intermediate ports (iports), two per trunk. The iports are automatically configured when the slices are configured.

The relation between the two trunk ports (Ports 11 and 12), client ports (Ports 1 through 10) and the four slices are represented in the tables below.

The OPM-6x16G_FC mode is referred to as 6x16G_FC and OPM_2x40G_2x10G mode is referred to as 2x40G_2x10G in this table.

Table 37: Trunk, Slice, and Port Configuration for Trunk 1 of the 400G-XP Card

Trunk 1			Client Ports				
Trunk Mode	Slice Operation Mode		1	2 [3]	3	7	8
	Slice 1	Slice 2	Port Lanes				

M-200G	OPM-100G	OPM-100G	-	-	-	4x [4]	4x
	OPM-100G	OPM-10x10G	-	3,4	1 to 4	4x	1 to 4
	OPM-10x10G	OPM-100G	1 to 4	1, 2	-	1 to 4	4x
	OPM-10x10G	OPM-10x10G	1 to 4	1 to 4	1 to 4	1 to 4	1 to 4
	6x16G_FC [5]	OPM-100G	1 to 4	1,2			4x
	6x16G_FC	OPM-10x10G	1 to 4	1,2 or 3,4 [6]	1 to 4		1 to 4
	OPM-100G	6x16G_FC	-	3,4	1 to 4	4x	
	OPM-10x10G	OPM-6x16G [7]	1 to 4	1,2 or 3,4 [8]	1 to 4	1 to 4	
	OPM-6x16G	6x16G_FC	1 to 4	1,2 and 3,4	1 to 4		
	2x40G_2x10G	2x40G_2x10G	40G	1,2 + 3,4	40G	40G	40G
	2x40G_2x10G	OPM-10x10G	40G	1,2 + 3,4	1 to 4	40G	1 to 4
	2x40G_2x10G	OPM_100G	40G	1,2	-	40G	4x
	OPM-10x10G	2x40G_2x10G	1 to 4	1,2 + 3,4	40G	1 to 4	40G
	OPM_100G	2x40G_2x10G	-	3,4	40G	4x	40G
M-100G	NA	OPM-100G		-	-		4x
		OPM-10x10G		3,4	1 to 4		1 to 4
		6x16G_FC		3,4	1 to 4		
		2x40G_2x10G	-	3,4	40G	-	40G

[3] Port 2 is shared between Slice 1 and Slice 2.
[4] 4x refers to all four lanes of the QSFP28 pluggable.
[5] This slice mode is not supported in R12.0.
[6] Depending on the PPM provisioned, ports 1 and 2 can be 16G FC or ports 3 and 4 can be 10GE/OTU2.
[7] This slice mode is not supported in R12.0.
[8] Depending on the PPM provisioned, ports 3 and 4 can be 16G FC or ports 1 and 2 can be 10GE/OTU2.

The OPM-6x16G_FC mode is referred to as 6x16G_FC and OPM_2x40G_2x10G mode is referred to as 2x40G_2x10G in this table.

Table 38: Trunk, Slice, and Port Configuration for Trunk 2 of the 400G-XP Card

Trunk 2	Client Ports

Trunk Mode	Slice Operation Mode		4	5 [9]	6	9	10
	Slice 3	Slice 4	Port Lanes				
M-200G	OPM-100G	OPM-100G	-	-	-	4x	4x
	OPM-100G	OPM-10x10G	-	3,4	1 to 4	4x	1 to 4
	OPM-10x10G	OPM-100G	1 to 4	1, 2	-	1 to 4	4x
	OPM-10x10G	OPM-10x10G	1 to 4	1 to 4	1 to 4	1 to 4	1 to 4
	6x16G_FC [10]	OPM-100G	1 to 4	1,2	-	-	4x
	6x16G_FC	OPM-10x10G	1 to 4	1,2 or 3,4 [11]	1 to 4	-	1 to 4
	OPM-100G	6x16G_FC	-	3,4	1 to 4	4x	-
	OPM-10x10G	6x16G_FC	1 to 4	1,2 or 3,4 [12]	1 to 4	1 to 4	-
	6x16G_FC	6x16G_FC	1 to 4	1,2 and 3,4	1 to 4	1 to 4	-
	2x40G_2x10G	2x40G_2x10G	40G	1,2 + 3,4	40G	40G	40G
	2x40G_2x10G	OPM-10x10G	40G	1,2 + 3,4	1 to 4	40G	1 to 4
	2x40G_2x10G	OPM_100G	40G	1,2	-	40G	4x
	OPM-10x10G	2x40G_2x10G	1 to 4	1,2 + 3,4	40G	1 to 4	40G
	OPM_100G	2x40G_2x10G	-	3,4	40G	4x	40G
M-100G	NA	OPM-100G	-	-	-	-	1 to 4
		OPM-10x10G		3,4	1 to 4		1 to 4
				3,4	1 to 4		
		2x40G_2x10G	-	3,4	40G	-	40G

[9] Port 5 is shared between Slice 3 and Slice 4.
[10] This slice mode is not supported in R12.0.
[11] Depending on the PPM provisioned, ports 1 and 2 can be 16G FC or ports 3 and 4 can be 10GE/OTU2.
[12] Depending on the PPM provisioned, ports 3 and 4 can be 16G FC or ports 1 and 2 can be 10GE/OTU2.

Trunk Port Interworking in 400G-XP Cards

To provide greater flexibility on the network design and deployment, the two CFP2 trunk ports of the 400G-XP card can interoperate with each other when the same trunk operating mode and slice configurations exist on both source and destination cards.

OCHCC circuits can be created between compatible client ports as detailed in the tables below.

Table 39: Compatible Client Ports for M-100G Trunk Port Configuration

Trunk 1 - CFP2 Port 11		**Source/Destination Client Ports**	**Source/Destination Client Ports**	**Trunk 2 - CFP2 Port 12**	
Slice configuration 1	Slice 2: OPM_100G	8	10	Slice 4: OPM_100G	Slice configuration 1
Slice configuration 2	Slice 2: OPM_10x10G	2-3	5-3	Slice 4: OPM_10x10G	Slice configuration 2
		2-4	5-4		
		3-1	6-1		
		3-2	6-2		
		3-3	6-3		
		3-4	6-4		
		8-1	10-1		
		8-2	10-2		
		8-3	10-3		
		8-4	10-4		
Slice configuration 2	Slice 2: OPM_6x16G_FC [13]	2-3	5-3	Slice 4: OPM_6x16G_FC	Slice configuration 2
		2-4	5-4		
		3-1	6-1		
		3-2	6-2		
		3-3	6-3		
		3-4	6-4		

[13] This slice mode is not supported in R12.0.

Table 40: Compatible Client Ports for M-200G Trunk Port Configuration

Trunk 1 - CFP2 Port 11		Source/Destination Client Ports	Source/Destination Client Ports	Trunk 2 - CFP2 Port 12	
Slice configuration 1	Slice1: OPM_100G	7	9	Slice 3: OPM_100G	Slice configuration 1
	Slice 2: OPM_10x10G	2-3	5-3	Slice 4: OPM_10x10G	
	Slice 1: OPM_100G	7	9	Slice 3: OPM_100G	
Slice configuration 2	Slice 2: OPM_10x10G	2-3	5-3	Slice 4: OPM_10x10G	Slice configuration 2
		2-4	5-4		
		3-1	6-1		
		3-2	6-2		
		3-3	6-3		
		3-4	6-4		
		8-1	10-1		
		8-2	10-2		
		8-3	10-3		
		8-4	10-4		
Slice configuration 3	Slice 1: OPM_10x10G	1-1	4-1	Slice 3: OPM_10x10G	Slice configuration 3
		1-2	4-2		
		1-3	4-3		
		1-4	4-4		
		2-1	5-1		
		2-2	5-2		
		7-1	9-1		
		7-2	9-2		
		7-3	9-3		
		7-4	9-4		
	Slice 2: OPM_100G	8	10	Slice 4: OPM_100G	

Trunk 1 - CFP2 Port 11		Source/Destination Client Ports	Source/Destination Client Ports	Trunk 2 - CFP2 Port 12	
Slice configuration 4	Slice 1: OPM_10x10G	1-1	4-1	Slice 3: OPM_10x10G	Slice configuration 4
		1-2	4-2		
		1-3	4-3		
		1-4	4-4		
		2-1	5-1		
		2-2	5-2		
		7-1	9-1		
		7-2	9-2		
		7-3	9-3		
		7-4	9-4		
	Slice 2: OPM_10x10G	2-3	5-3	Slice 4: OPM_10x10G	
		2-4	5-4		
		3-1	6-1		
		3-2	6-2		
		3-3	6-3		
		3-4	6-4		
		8-1	10-1		
		8-2	10-2		
		8-3	10-3		
		8-4	10-4		
Slice configuration 1	Slice 1:OPM_6x16G_FC [14]	1-1	4-1	Slice 3: OPM_6x16G_FC	Slice configuration 3
		1-2	4-2		
		1-3	4-3		
		1-4	4-4		
		2-1	5-1		
		2-2	5-2		

Trunk 1 - CFP2 Port 11		Source/Destination Client Ports	Source/Destination Client Ports	Trunk 2 - CFP2 Port 12	
Slice configuration 2	Slice 2: OPM_6x16G_FC	2-3	5-3	Slice 4: OPM_6x16G_FC	Slice configuration 4
		2-4	5-4		
		3-1	6-1		
		3-2	6-2		
		3-3	6-3		
		3-4	6-4		

[14] This slice mode is not supported in R12.0.

GCC0 Support on the 400G-XP Card

- The 400G-XP card supports provision of one GCC0 channel for each of the trunk ports on the operating modes-MXP, and MXP-2x150G(8QAM).
- In case of the OTU4C3 (8QAM) payload, only one GCC0 channel is configurable on the first trunk port (Port-11). The configuration on the second trunk port (Port-12) is automatically blocked.
- In case of the MXP-2x150G(8QAM) payload, the GCC0 channel is configurable only on the second trunk port (Port-12); no GCC0 channel configuration is supported on the first trunk port (Port-11).
- The OTU4 and OTU2 client ports do not support GCC0 channels on the card.
- The 400G-XP card supports a maximum of two GCC0 channels on each trunk port.
- The OTU4C2 trunk port supports the Low Speed GCC 196K and High Speed GCC 1200K. The 400G-XP card supports only the High Speed GCC rate, 1200K. So, GCC0 channels provisioning on 400G-XP cards, which are part of 15454-M12 as Node Controller (NC) configurations, is not supported.
- The OTNXC or OCHTRAIL circuits are not supported over the direct GCC0 link on the 400G-XP card.
- The GCC0 channel provisioning is not supported on REGEN card mode on the 400G-XP-LC card. However, GCC0 tunneling is enabled.
- From R11.1.1.2, the GCC0 channel provisioning is supported on the REGEN card mode on the 400G-XP-LC card. If the GCC0 provisioning is not provisioned, it acts transparent for GCC0 channel.
- GCC0 channels provisioning is supported with hardware FPGA image version > 0.28. GCC provisioning will fail with a deny error message if FPGA version is = < 0.28.
- In presence of the TIM-SM alarm, GCC0 link remains down.

2x150G Support on the 400G-XP Card

From Release 10.9, the 400G-XP card supports the configuration of 2x150G mode in 8QAM modulation format. It is configurable on the trunk ports of the card by selecting M_150G as the Trunk Operating mode.

The M_150G mode does not support muxponder, cross connection, and regeneration configurations.

The M_150G trunk mode configuration supports client slices 1, 3 and 4. The available ports 1[1:4], 2[1:2], 4[1:4], 5[1:4], 6[1:4], 7[1:4], 9[1:4], 10[1:4]. When the M_150G trunk mode in configured, the slices 1, 3 and 4 are independently configurable as OPM_100G, OPM_10x10G or OPM_6x16G-FC. It is possible to change a slice mode without it being traffic affecting on the other provisioned slices. The admin state of both trunk ports are aligned.

On a M_150G configured trunk mode, all client payloads or options are the same as the standard M_200G MXP mode.

The M_150G trunk mode is applicable to both trunk ports. This is required because this mode splits the ODU4line frames into two interleaved 150G signals transported separately by the two trunk ports.

The trunk ports configured as M_150G support the same optical and FEC alarms or monitors provided by the M_200G mode. An LOS-P or LOF alarm on any of the two trunk ports of M_150G correlates all the OTU4C3 container OTN alarms.

The Line OTN Alarms and Performance Monitors of the 2x150G mode container frame (OTU4C3) is evaluated as the summarization of the Alarms or PMs related to the 3 embedded ODU4 internal ports 1, 3, and 4. The resulting values are available at the OTN layer of Trunk12.

Limitations of 2x150G Support on the 400G-XP Card

- The trunk ports are put in the Out-of-Service state before unplugging any CFP2 trunk. Extracting an In-Service CFP2 trunk results in shutting down of the other trunk.
- The loopback setting of both M_150G trunks are aligned. However, the internal loopback ports are configurable independently with the same limitations as that of M_100G and the M_200G modes.
- The TTI-SM of the OTU4C3 container is configurable and is monitored only on Trunk 12.
- The GCC0 provisioning is supported only for Trunk-12.
- The FEC setting of both M_150G trunks are aligned.

OTN Cross-Connect Operation Mode on 400G-XP Card

Table 41: Feature History

Feature Name	Release Information	Feature Description
Support for OTN Cross-Connect Operation Mode on 400G-XP Card	Cisco NCS 2000 Release 12.3	The 400G-XP card supports the OTN cross-connect (OTNXC) operation mode. This mode supports ODU4, ODU2, and ODU2e bandwidths. This mode allows ODU switching between client to trunk ports or trunk to trunk ports within a single 400G-XP card for 100G and 200G trunk rates.

Feature Name	Release Information	Feature Description
Additional payloads in OTN Cross-Connect Operating Mode on 400G-XP Card	Cisco NCS 2000 Release 12.3.1	The OTN cross-connect (OTNXC) operating mode on the 400G-XP card supports OTU2E, OC-192, STM-64, and OTU-4 payloads. With these additional payloads, the 400G-XP Card is fully functional with OTN Cross-Connect functionality for 10/100G client protocols over 100/200G DWDM wavelengths. You can have optimized utilization of the DWDM trunk capacity in the network.

The 400G-XP card supports the OTN cross-connect (OTNXC) operating mode. You cannot edit the trunk and slice mode after the 400G-XP card is configured in OTNXC mode. This mode supports ODU4, ODU2, and ODU2e bandwidths and allows ODU2e switching between client to trunk ports or trunk to trunk ports within a single 400G-XP card for 100G and 200G trunk rates. Both trunk ports are configured with the same rate (100G or 200G).

10GE, OTU2, 100GE, OTU2E, OC-192, STM-64, and OTU-4 are supported as client payloads. Each 10GE is mapped to an ODU or ODU2e channel. Each 10G client port of the 400G-XP card consists of only one ODU or ODU2e and each OTU4C2 (200G) trunk port of the 400G-XP card consists of 20 ODUs or ODU2es.

As part of the OTNXC operating mode, after defining the operation mode on the card, you can create 20xODU or 20xODU2e trunk-to-trunk cross-connections or up to 40x10GE client-to-trunk cross-connections. You can create the ODU connections only through a NETCONF client. For more information on the NETCONF client, see Cisco NCS 2000 Series SVO Data Models Configuration Guide.

OTNXC operating mode allows ODU2, ODU2e, and OTDU4 switching between client to trunk ports or trunk to trunk ports within a single 400G-XP-LC card for 100G and 200G trunk rates. In OTNXC operating mode both trunk ports are configured with the same rate (100G or 200G). You can create a trunk-to-trunk cross-connections or client-to-trunk cross-connections.

Client-to-trunk cross-connections can be protected or unprotected. The card supports up to 20x10GE circuits with SNC-N 1+1 bidirectional protection. The ODU connections are always bidirectional.

The OTNXC card mode requires a new trunk FPGA image. Make sure that the 400G-XP card is running on firmware (SCP) version 5.24 or above. A Condition message warns the user about availability of a new image.

OTNXC operating mode is not supported in EPNM Release 6.0. Hence, we cant create WSON/SSON OCH trail directly from EPNM, and an end-to-end ODU connection cannot be created from EPNM. For SVO Release 12.3, and EPNM Release 6.0, you can create the ODU connections only through a NETCONF client at each node which is part of OTNXC services.

Ensure that you adhere to the following ODU interface naming conventions when you create an ODU connection through the NETCONF client:

ODU Type	Trunk or Client	Rate	ODU Format	ODU4 Range	ODU2 Range	Example	Interface Created
ODU4	Trunk	200G	shelf/slot/port/ODU4Num	1–2	NA	shelf/slot/11/1 shelf/slot/11/2 shelf/slot/12/1 shelf/slot/12/2	Yes
ODU4	Trunk	100G	shelf/slot/port	1	NA	shelf/slot/11 shelf/slot/12	No
ODU4	Client	100G	shelf/slot/port	1	NA	shelf/slot/7 shelf/slot/8	No
ODU2	Trunk	200G	shelf/slot/port/ODU4Num/ODU2Num	1–2	1–10	shelf/slot/11/1 or 2/1–10 shelf/slot/12/1 or 2/1–10	Yes
ODU2	Trunk	100G	shelf/slot/port/ODU4Num/ODU2Num	1	1–10	shelf/slot/11/1 or 2/1–10 shelf/slot/12/1 or 2/1–10	Yes
ODU2	Client	10G	shelf/slot/port-subline	NA	1	shelf/slot/7/1–4 shelf/slot/8/1–4	No

OTNXC Constraints

The following constraints apply to ODU circuit creation between 400G-XP cards configured in the OTNXC mode.

- Both trunk ports of the 400G-XP card are configured with the same rate (100G or 200G)
- An ODU circuit cannot be created between two client ports of the 400G-XP card.
- Each client port belongs to one of the four card slices. Slice 1 and Slice 2 are linked to the first trunk port and Slice 3 and Slice 4 are linked to the second trunk port. Cross-connecting between slices of the same trunk is not allowed. The possible cross-connections that can be created are within the same client slice or between the client slice and any of the other trunk slices.
- There is a bandwidth limitation between the two internal ASICs of the 400G-XP card due to which a maximum of 20x10G interlink connections can be defined. These resources are consumed by either trunk-to-trunk cross-connects or client-to-trunk cross-connects when the client does not belong to the trunk slice.
- Protected cross-connects are restricted to client ports 1, 2, 3, 7, and 8 belonging to slices 1and 2.
- Do not provision more than one path for nonprotected circuits.

- The NE defaults thresholds for ODU interfaces cannot be set for cross-connected ODUs.
- With 100GE payload on QSFP-100G-FR-S on 400G-XP card with OTNXC mode, protection switching time is high during Manual/Force switching (varies between 2.5 to 3.5 seconds); however auto switching time is less than 50 ms.
- When non-revertive mode is configured or the cross connection is not protected, NETCONF output shows the default revertive timer or the previously configured revertive timer. The SVO web UI displays **NA** in such cases.

OTNXC Exceptions

The following exceptions apply to ODU circuits between 400G-XP cards configured in the OTNXC mode:

- If the circuit protection type is SNC-N, the circuit service state is OOS-PARTIAL (Locked-partial) if the source or destination nodes have a fault on both the trunk ports causing the port service state to change to OOS-AU, FLT (ANSI) or Unlocked-disabled, failed (ETSI)) or if three or more intermediate nodes have the service state as FLT.

  If the circuit protection type is None, the circuit service state is OOS-PARTIAL (Locked-partial) if the source or intermediate nodes have the service state as FLT.
- When the traffic is manually switched to the protect path in a protected revertive ODU circuit, the WKSWPR alarm is raised on the node. The alarm may not persist after a control card reset.
- Performing a database restore operation, may not clear the WKSWPR alarm.
- If you create a protected OTN-XC connection from the NETCONF client with same destination, the system considers both destinations as the same and creates a nonprotected OTN-XC connection.

40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C Cards

Table 42: Feature History

Feature Name	Release Information	Feature Description
40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C Cards	Cisco NCS 2000 Release 12.2	The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards are supported on SVO. The cards have CP-DQPSK extended performance.

The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards aggregate a variety of client service inputs (10GE, OTU2, OTU2e, and OC-192) into a single 40-Gbps OTU3/OTU3e signal on the trunk side.

Note The 40E-MXP-C, 40EX-MXP-C, or 40ME-MXP-C card is displayed with the same card name, _15454-40E-MXP-C.

The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards support aggregation of the following signals:

- With overclock enabled on the trunk port:

- OTU2e
- 10 Gigabit Ethernet LAN-Phy (CBR mapping)

- With overclock disabled on the trunk port:
  - OC-192/STM-64
  - OTU2

You can install and provision the cards in:

- Slots 2 to 6 in Cisco NCS 2006 chassis
- Slots 2 to 15 in Cisco NCS 2015 chassis

The client ports of the 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards interoperate with all the existing TXP or MXP (OTU2 trunk) cards.

For OTU2 and OTU2e client protocols, Enhanced FEC (EFEC) is not supported on Port 1 of the 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards.

Client Port	FEC Configuration
Port 1	Only Standard FEC
Port 2	Standard and Enhanced FEC
Port 3	Standard and Enhanced FEC
Port 4	Standard and Enhanced FEC

Key Features

The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards provide the following key features:

- The cards use the CP-DQPSK modulation format.
- Onboard E-FEC processor—The E-FEC functionality improves the correction capability of the transponder to improve performance, allowing operation at a lower OSNR compared to the standard RS (239,255) correction algorithm. A new BCH algorithm implemented (according to G.975.1 I.7) in E-FEC allows recovery of an input BER up to 1E-3. The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards support both the standard RS (specified in ITU-T G.709) and E-FEC standard, which allows an improved gain on trunk interfaces with a resultant extension of the transmission range on these interfaces.
- Automatic Laser Shutdown (ALS)—A safety mechanism, Automatic Laser Shutdown (ALS), is used in the event of a fiber cut. The Auto Restart ALS option is supported only for OC-192/STM-64 and OTU2 payloads. The Manual Restart ALS option is supported for all payloads.
- Automatic timing source synchronization—The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards synchronize to the card clocks. Because of a maintenance or upgrade activity, if the control cards are not available, the cards automatically synchronize to one of the input client interface clocks.
- Squelching policy—The cards are set to squelch the client interface output if there is LOS at the DWDM receiver, or if there is a remote fault. In the event of a remote fault, the card manages MS-AIS insertion.

- The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards are tunable across the full C-band wavelength.

Wavelength Identification

The 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C cards use trunk lasers that are wave-locked, which allows the trunk transmitter to operate on the ITU grid effectively. These cards implement the UT2 module; they use a C-band version of the UT2. The laser is tunable over 82 wavelengths in the C-band at 50-GHz spacing on the ITU grid.

Table 43: 40E-MXP-C, 40EX-MXP-C, and 40ME-MXP-C Trunk Wavelengths

Channel Number	Frequency (THz)	Wavelength (nm)	Channel Number	Frequency (THz)	Wavelength (nm)
1	196.00	1529.55	42	193.95	1545.72
2	195.95	1529.94	43	193.90	1546.119
3	195.90	1530.334	44	193.85	1546.518
4	195.85	1530.725	45	193.80	1546.917
5	195.80	1531.116	46	193.75	1547.316
6	195.75	1531.507	47	193.70	1547.715
7	195.70	1531.898	48	193.65	1548.115
8	195.65	1532.290	49	193.60	1548.515
9	195.60	1532.681	50	193.55	1548.915
10	195.55	1533.073	51	193.50	1549.32
11	195.50	1533.47	52	193.45	1549.71
12	195.45	1533.86	53	193.40	1550.116
13	195.40	1534.250	54	193.35	1550.517
14	195.35	1534.643	55	193.30	1550.918
15	195.30	1535.036	56	193.25	1551.319
16	195.25	1535.429	57	193.20	1551.721
17	195.20	1535.822	58	193.15	1552.122
18	195.15	1536.216	59	193.10	1552.524
19	195.10	1536.609	60	193.05	1552.926
20	195.05	1537.003	61	193.00	1553.33
21	195.00	1537.40	62	192.95	1553.73

Channel Number	Frequency (THz)	Wavelength (nm)	Channel Number	Frequency (THz)	Wavelength (nm)
22	194.95	1537.79	63	192.90	1554.134
23	194.90	1538.186	64	192.85	1554.537
24	194.85	1538.581	65	192.80	1554.940
25	194.80	1538.976	66	192.75	1555.343
26	194.75	1539.371	67	192.70	1555.747
27	194.70	1539.766	68	192.65	1556.151
28	194.65	1540.162	69	192.60	1556.555
29	194.60	1540.557	70	192.55	1556.959
30	194.55	1540.953	71	192.50	1557.36
31	194.50	1541.35	72	192.45	1557.77
32	194.45	1541.75	73	192.40	1558.173
33	194.40	1542.142	74	192.35	1558.578
34	194.35	1542.539	75	192.30	1558.983
35	194.30	1542.936	76	192.25	1559.389
36	194.25	1543.333	77	192.20	1559.794
37	194.20	1543.730	78	192.15	1560.200
38	194.15	1544.128	79	192.10	1560.606
39	194.10	1544.526	80	192.05	1561.013
40	194.05	1544.924	81	192.00	1561.42
41	194.00	1545.32	82	191.95	1561.83

1.2T-MXP Card

Table 44: Feature History

Feature	Release Information	Description
1.2T-MXP Card	Cisco NCS 2000 Release 12.2	This card triples the per slot throughput of the NCS 2000 system from 200 Gbps to 600 Gbps. The DCO trunk ports of the card can support up to 400-Gbps data-rate with multiple modulation formats, encoding types, and FEC options. This card can be installed in the NCS 2006 and NCS 2015 chassis.

In this chapter, "1.2T-MXP" refers to the NCS2K-1.2T-MXP card.

The 1.2Tbps Transponder or Muxponder line card (1.2T-MXP) is the first line card to have a 400G trunk and 400GE client interface in the NCS 2000 platform. It is a two-slot card that triples the per slot throughput of the NCS 2000 system from 200 Gbps to 600 Gbps.

The 1.2T-MXP card has three QSFPDD56 or QSFP28 client ports, five QSFP28 client ports, and three CFP2 DWDM Digital Coherent Optics (DCO) trunk ports. The QSFPDD56 client ports can also be used alternately as QSFP28 ports on an individual port. The DCO ports can support up to 400-Gbps data-rate with multiple modulation formats, encoding types, and FEC options. You can configure the 1.2T-MXP card in different ways with a maximum of 1.2Tbps total traffic on the client side (QSFP-DD/28) and the 1.2Tbps total traffic on the trunk side.

The 1.2T-MXP card can be installed in:

- NCS 2006 chassis that can accommodate a maximum of three 1.2T-MXP cards.
- NCS 2015 chassis that can accommodate a maximum of seven 1.2T-MXP cards.

The 1.2T-MXP card coexists with other NCS 2000 line cards without restricting their functionalities. However, it does not interoperate with any other line cards.

Operating Modes and Slice Definition in the 1.2T-MXP Card

Table 45: Feature History

Feature	Release Information	Description
Support for 6x100GE Operation Mode	Cisco NCS 2000 Release 12.3	The 1.2T-MXP card supports the 6x100G operation mode that enables100GE clients over 6 QSFP28 ports, when the trunk is at 200G rate.

Table 46: Feature History

Feature	Release Information	Description
Suboperating Modes on 1.2T-MXP card	Cisco NCS 2000 Release 12.3.1	The new suboperating mode OPM-2x100G-DD is introduced on the 1.2T-MXP card to configure 6x100GE muxponder mode exclusively for QDD clients. Also, the 9x100GE muxponder mode can now be configured using OPM-3x100G-DD suboperating mode. These muxponder modes add the capability to configure QDD-400G-DR4-S pluggable in the breakout mode on all three slices with different data rates.

Operating Modes

You can configure the 1.2T-MXP card in the TXPMXP mode. The following are the suboperating modes:

- OPM-400G—Enables 400GE client on the QSFP DD port, when the trunk is at 400G rate.
- OPM-4x100G-DD—Enables four 100GE clients that use four-level Pulse Amplitude Modulation (PAM4), on one QSFP DD port, when the trunk is at 400G rate.
- OPM-2x100G-DD—Enables two 100GE clients that use PAM4, on one QSFP DD port, when the trunk is at 200G rate.
- OPM-3x100G-DD—Enables three 100GE clients that use PAM4, on one QSFP DD port, when the trunk is at 300G rate.
- OPM-4x100G—Enables 100GE clients over four QSFP28 ports, when the trunk is at 400G rate.
- OPM-3x100G—Enables 100GE clients over three QSFP28 ports, when the trunk is at 300G rate.
- OPM-2x100G—Enables100GE clients over two QSFP28 ports, when the trunk is at 200G rate.

The slices are configured based on the required data path configuration. The following table explains the suboperating modes that are enabled on trunk ports for each slice:

Table 47: Sub-Operating Modes

Slice	Trunk Port	Supported Sub-Operating Modes
Slice 1	9	• OPM-400G • OPM-4x100G-DD • OPM-2x100G-DD • OPM-3x100G-DD • OPM-2x100G

Slice	Trunk Port	Supported Sub-Operating Modes
Slice 2	10	• OPM-400G • OPM-4x100G • OPM-4x100G-DD • OPM-2x100G-DD • OPM-3x100G-DD • OPM-3x100G • OPM-2x100G
Slice 3	11	• OPM-400G • OPM-4x100G • OPM-3x100G • OPM-2x100G • OPM-2x100G-DD • OPM-3x100G-DD

You can use the 1.2T-MXP card in different configurations. The following table describes the combinations of suboperating modes, the trunk ports, and client ports for each slice:

Note In the combinations described, you can also choose to configure only one of the slices 1–3.

Table 48: Different Combinations of Sub-Operating Modes

Configuration	Sub-Operating Modes	Trunk Ports	Client Ports
400GE Transponder—Includes 3x400G trunk, 3x400GE client with 3xQSFP-DD pluggables	Slice 1: OPM-400G	9	6
	Slice 2: OPM-400G	10	7
	Slice 3: OPM-400G	11	8
12x100GE Muxponder—Includes 3x400G trunk, 12x100GE client with 2xQSFP-DD breakout + 4xQSFP28 pluggables	Slice 1: OPM-4x100G-DD	9	Port-6 lanes (6.1, 6.2, 6.3, 6.4)
	Slice 2: OPM-4x100G-DD	10	Port-7 lanes (7.1, 7.2, 7.3, 7.4)
	Slice 3: OPM-4x100G	11	2, 3, 4, 8

Configuration	Sub-Operating Modes	Trunk Ports	Client Ports
9x100GE Muxponder—Includes 3x300G trunk, 9x100GE client with 1xQSFP-DD breakout + 6xQSFP28 pluggables	Slice 1: OPM-3x100G-DD	9	Port-6 lanes (6.1, 6.2, 6.3) 6.4 is unused.
	Slice 2: OPM-3x100G	10	1, 5, 7
	Slice 3: OPM-3x100G	11	3, 4, 8
Mixed Configuration 1	Slice 1: OPM-400G	9	6
	Slice 2: OPM-4x100G-DD	10	Port-7 lanes (7.1, 7.2, 7.3, 7.4)
	Slice 3: OPM-3x100G	11	3, 4, 8
6x100GE Muxponder—Includes 3x200G trunk, 6x100GE client with 6xQSFP28 pluggables	Slice 1: OPM-2x100G	9	1, 6
	Slice 2: OPM-2x100G	10	5, 7
	Slice 3: OPM-2x100G	11	4, 8
9x100GE Muxponder - Includes 3x300G trunk, 9x100GE client with 3xQDD-400G-DR4-S pluggables in breakout mode	Slice 1: OPM-3x100G-DD	9	Port-6 lanes (6.1, 6.2, 6.3)
	Slice 2: OPM-3x100G-DD	10	Port-7 lanes (7.1, 7.2, 7.3)
	Slice 3: OPM-3x100G-DD	11	Port-8 lanes (8.1, 8.2, 8.3)
6x100GE Muxponder - Includes 3x200G trunk,6x100GE clients with 3xQDD-400G-DR4-S pluggables in breakout mode	Slice 1: OPM-2x100G-DD	9	Port-6 lanes (6.1, 6.2)
	Slice 2: OPM-2x100G-DD	10	Port-7 lanes (7.1, 7.2)
	Slice 3: OPM-2x100G-DD	11	Port-8 lanes (8.1, 8.2)
Mixed Configuration 2	Slice 1: OPM-3x100G-DD	9	Port-6 lanes (6.1, 6.2, 6.3)
	Slice 2: OPM-4x100G-DD	10	Port-7 lanes (7.1, 7.2, 7.3,7.4
	Slice 3: OPM-2x100G-DD	11	Port-8 lanes (8.1, 8.2)
Mixed Configuration 3	Slice 1: OPM-3x100G-DD	9	Port-6 lanes (6.1, 6.2, 6.3)
	Slice 2: OPM-3x100G-DD	10	Port-7 lanes (7.1, 7.2, 7.3)
	Slice 3: OPM-2x100G-DD	11	Port-8 lanes (8.1, 8.2)

Key Features of 1.2T-MXP

The key features are:

- Enhanced muxponder or transponder capabilities while enabling double-slot card with 100GE or 400GE client type.
- O-FEC encoding on the trunk interface.
- Nyquist filtering for OSNR.
- Supports configurable modulation format such as 300 8QAM, 400 16QAM, PAM4, and 16QAM in both Open ROADM and 400ZR+ framing mode.
- Flex spectrum support with Nyquist filtering.
- ZR+ based framing on trunk.
- 3x400GE client bandwidth using QSFP-DD or 12x100GE client bandwidth using QSFP-DD (break-out mode)
- LLDP support on 100GE or 400GE clients.
- Supports secure boot.
- Alarms for ZR interface and, Alarms, Performance, and Statistics for GE interface as well as Optical Pluggable.
- Diagnostics and maintenance support.
- Supports GroupId that uniquely identifies a group of physical ports in a ZR frame.
- Performance Monitoring—Supports monitoring of temperature, Rx optical power, Tx optical power, and the following parameters:

Note The following data is applicable to the ONS-CFP2D-400G-C pluggable connected to the trunk port of 1.2T-MXP card.

Table 49: Optical PM Parameters Supported by 1.2T-MXP Card

Optical PM Parameters	Description	Traffic Mode	Range of values	
			Minimum	Maximum
Central Frequency Offset (CFO) (MHz)	Deviation of actual wavelength from tuned wavelength	All	-3600 MHz	3600 MHz
Differential Group Delay (DGD) (ps)	The delay caused by different arrival times of optical signals, which in turn causes dispersion	All	0 ps	+60 ps Accuracy = +/-10 ps

Optical PM Parameters	Description	Traffic Mode	Range of values	
			Minimum	Maximum
Optical Signal to Noise Ratio (OSNR) (dB)	Ratio of signal power to background noise power	400G 16QAM ZR+	N/A	23.1dB (Accuracy = +/-2dB)
		300G 8QAM ZR+	N/A	19.5dB (Accuracy = +/-2dB)
		200G QPSK ZR+	N/A	14.5dB(Accuracy = +/-2dB)
Polarization Dependent Loss (PDL) (dB)	Maximum variation of insertion loss due to a variation of the state of polarization (SOP) over all SOPs	All	0	6dB (Accuracy of +/-1.5db for 0-3 db range) (Accuracy of +/-2db for 3-6 db range)
Q Factor (dB)	Combination of OSNR for both 0-bit and 1-bit signals	All	0 dB	100 dB
Polarization Change Rate (PCR) (10*rad/s)	The polarization change rate during the PM time interval	All	N/A	N/A
Second-Order Polarization Mode Dispersion (SOPMD) (ps^2)	The signal distortion caused by variation in optical frequency and time delays due to laser chirp (the change in frequency of a signal over time).	All		
Laser Bias (%)	The percentage of laser bias current.	All		

Note

- The available values for SOPMD and Laser bias are not accurate.
- For PCR, the values are not supported.

Supported Pluggables

The supported pluggables are:

- Three CFP2 400G DCO trunk pluggables
- Eight QSFP28 or three QSFP-DD pluggables

- Five QSFP28 client pluggables

Limitations of 1.2T-MXP Card

The following are the limitations of the 1.2T-MXP card:

- Optics PMs are not supported by Active Optical Cable (AOC) PPM.
- GroupID feature is not supported for 400GE transponder configuration.
- I-port management is not supported.
- OTN is not supported on trunk.
- Traffic does not go down when FlexO-SR Interface Trail Trace Identifier Mismatch (FOIC-TIM) alarm is raised.
- Starting from Release 12.3, the CFP2-DCO detection takes 20–25 seconds (5 seconds longer than the earlier release).
- There might be traffic fluctuations affecting some switches and routers due to the following scenario:

  When there is a 400GE or 4x100GE traffic congestion on the pluggables, an electrical squelch or unsquelch is performed for one second on the transmit side of the pluggables. This operation relocks the transmit Clock and Data Recovery (CDR) of the pluggables. This results in an out-of-range frequency on the client for four to six seconds before the traffic clears.

  This issue occurs in pluggables such as QSFP-DD DR4, QDD-400G-FR4, QDD-400G-LR8, QDD-400-AOC1M, QDD-400-AOC2M, QDD-400-AOC3M, QDD-400-AOC5M, QDD-400-AOC7M, QDD-400-AOC10M, and QDD-400-AOC15M.

OTU2-XP Card

Table 50: Feature History

Feature Name	Release Information	Feature Description
OTU2-XP Card	Cisco NCS 2000 Release 12.2	The OTU2-XP card simplifies the integration and transport of 10 Gigabit Ethernet (10GE), OC192, and STM64 services into metro and regional service provider networks. This card can be installed in Cisco NCS 2006 and NCS 2015 chassis.

In this chapter, "OTU2-XP" refers to the 15454-M-OTU2-XP card.

The OTU2-XP card is a single-slot card that can be installed in slots 2 to 7 in NCS 2006 and slots 2 to 16 in NCS 2015 chassis. All the four ports in the card are ITU-T G.709 compliant and support 40 channels (wavelengths) at 100-GHz channel spacing in the C-band (that is, the 1530.33 to 1561.42 nm wavelength range).

The following operating modes are supported on the OTU2-XP card.

- **OTU2XP-2XP**—This is the default card mode. In this mode, both the port pairs (1-3 and 2–4) are configured in Transponder mode.
- **OTU2XP-2REG**—In this mode, both the port pairs (1-3 and 2–4) are configured in Regenerator mode.
- **OTU2XP-XP-REG**—In this mode, port pair 1–3 is configured in Transponder mode and port pair 2–4 is configured in Regenerator mode.
- **OTU2XP-REG-XP**—In this mode, port pair 1–3 is configured in Regenerator mode and port pair 2–4 is configured in Transponder mode.

Table 51: OTU2-XP Card Configurations and Ports

Configuration	Port 1	Port 2	Port 3	Port 4
2 x 10G transponder	Client port 1	Client port 2	Trunk port 1	Trunk port 2
2 x 10G regenerator (with enhanced FEC (E-FEC) only on one port)	Trunk port 1	Trunk port 2	Trunk port 1	Trunk port 2

Key Features

The OTU2-XP card has the following key features:

- 10G transponder and regenerator capability.
- Four ports with multirate (OC-192/STM-64, 10G) client interface. The client signals are mapped into an ITU-T G.709 OTU2 signal using standard ITU-T G.709 multiplexing.
- The supported payloads are TEN-GE, OTU2, OTU2e, OC192, and STM64. 10G FC and IB-5 payloads are not supported.
- The default configuration is transponder, with trunk ports configured as ITU-T G.709 standard FEC.
- In transponder or regenerator configuration, if one of the ports is configured, the corresponding port is automatically created.
- In regenerator configuration, only ports 3 and 4 can be configured as E-FEC (Standard ITU-T G.975.1 (subclause I.7)). The ports 1 and 2 can be configured only with standard FEC (Standard ITU-T G.709).
- When the port pair 1–3 or 2–4 is configured as regenerator, the default configuration on ports 3 and 4 is automatically set to standard FEC.
- The following OTU2 link rates are supported on the OTU2-XP trunk port:
  - Standard G.709 (10.70923 Gbps) when the client is provisioned as “SONET” (including 10G Ethernet WAN PHY) (9.95328 Gbps).
  - G.709 overclocked to transport 10GE as defined by ITU-T G. Sup43 Clause 7.2 (11.0491 Gbps) and ITU-T G. Sup43 Clause 7.1 (11.0957 Gbps) when the client is provisioned as “10G Ethernet LAN Phy” (10.3125 Gbps).
- The Fixed Stuff parameter is applicable only in transponder operating mode with TEN-GE payload. The trunk port is OTU2e when this parameter is set to Enable (default).

OTU2-XP Card Configuration Rules

The following rules apply to OTU2-XP card configurations:

- When you provision port pairs 1-3 or 2-4, they come up in the default Transponder mode.
- The port pairs 1–3 and 2–4 can be configured in different modes only when the card configuration is Mixed. If the card configuration is Mixed, you must choose different modes on port pairs 1–3 and 2–4 (that is, one port pair in Transponder mode and the other port pair in Regenerator mode).

  The Mixed card configurations are as follows:

  - **OTU2XP-XP-REG**—In this mode, port pair 1–3 is configured in Transponder mode and port pair 2–4 is configured in Regenerator mode.
  - **OTU2XP-REG-XP**—In this mode, port pair 1–3 is configured in Regenerator mode and port pair 2–4 is configured in Transponder mode.

- If the card is in Transponder configuration, you can change the configuration to Regenerator or Mixed.
- If the card is in Regenerator configuration and you have configured only one port pair, then configuring payload rates for the other port pair automatically changes the card configuration to Mixed, with the new port pair in Transponder mode.
- If the card is in Regenerator configuration, you cannot change the payload rate of the port pairs. You must change the configuration to Transponder, change the payload rate, and then move the card configuration back to Regenerator.
- If the card is in Transponder configuration with TEN-GE payload, the trunk port interfaces 3 and 4 are created as OTU2e.
- If the card is in Regenerator configuration with TEN-GE payload, all the port interfaces are created as OTU2e.
- If the card is in Transponder configuration, the **OTN Disable** parameter can be set to True (G.709 disabled). In this case, both the port pairs (1-2 and 3–4) does not have OTU and ODU interfaces.
- If any of the affected ports are in IS (ANSI) or Unlocked-enabled (ETSI) state, you cannot change the card configuration.

ODU Transparency

A feature of the OTU2-XP card is the ability to configure the ODU overhead bytes (EXP bytes and RES bytes 1 and 2) using the ODU Transparency parameter. SVO supports ODU Transparency parameter on OTU client interfaces 1 and 2 when the card mode is set as Regenerator. The valid values are Disable (Cisco Extended Use) or Enable (Transparent Standard Use).

- Cisco Extended Use—ODU overhead bytes are terminated and regenerated on both the ports of the regenerator group.
- Transparent Standard Use—ODU overhead bytes are transparently passed through the card. This option allows the OTU2-XP card to act transparently between the two trunk ports when the card is configured in Regenerator mode.

The ODU Transparency parameter is configurable only for Regenerator configuration. For Transponder and Mixed configurations, this parameter defaults to Interop-None and cannot be changed.

Installing the Card

Use this task to install the card.

Warning During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself. Statement 94

Warning Class 1 laser product. Statement 1008

Warning Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Statement 1056

Warning Class I (CDRH) and Class 1M (IEC) laser products. Statement 1055

Note You can install the cards on the NCS 2006 chassis that is mounted with either of the following:

- Standard brackets on a 19-inch or 23-inch ANSI rack configuration or on an ETSI rack configuration.
- Inlet air deflectors on a 23-inch ANSI rack configuration or on an ETSI rack configuration. The exhaust air deflectors cannot be used.

Note

Note For US installations, complies with the US Federal Drug Administration Code of Federal Regulations Title 21, Sections 1040.10 and 1040.11, except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If you install a card incorrectly, the FAIL LED flashes continuously.

Note Until a card is provisioned, the card is in the standby condition and the ACT or STBY LED remains amber in color.

Procedure

Step 1 Open the card latches or ejectors.

Step 2 Use the latches or ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

Step 3 Verify that the card is inserted correctly and simultaneously close the latches or ejectors on the card.

Note It is possible to close the latches and ejectors when the card is not plugged into the backplane. Ensure that you have inserted the card all the way.

Note If you install the card in the wrong slot, an MEA alarm is raised. To clear this alarm, open the latches, slide out the card, then insert it in the correct slot.

After you install the card, the FAIL, ACT, and SF LEDs go through a sequence of activities. They turn on, turn off, and blink at different points. After approximately two or three minutes, the ACT or ACT/STBY LED turns on. The SF LED might persist until all card ports connect to their far-end counterparts and a signal is present.

Note Until a card is provisioned, it is in the standby condition, and the ACT or STBY LED remains amber in color.

Step 4 If the card does not boot up properly or the LEDs do not progress through the activities described in Step 2, check the following:

- When a physical card type does not match the type of card that is provisioned for that slot in the nodal craft, the card might not boot, and the nodal craft displays a MEA alarm. If the card does not boot, open the nodal craft and ensure that the slot is not provisioned for a different card type before assuming that the card is faulty.
- If the red FAIL LED does not turn on, check the power.
- If you insert a card into a slot that is provisioned for a different card, turn all LED off.
- If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly.

If any of these conditions are present, remove the card and repeat Steps 1 to 3. If the card does not boot up properly the second time, contact your next level of support.

Step 5 If the card requires a pluggable, complete one of the following tasks:

- DLP-G723 Install PPM on a Line Card—Complete this task to install the physical pluggable post module into the transponder or muxponder card.

- Provision PPM, on page 240—(Optional) Complete this task if you do not have the physical pluggable and must preprovision the PPM slot.

Note Pluggable port modules are hot-swappable I/O devices that plug into a transponder or muxponder card.

Provision PPM

Use this task to provision a PPM on a line card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Pluggable Port Modules** tabs.

Step 2 In the Pluggable Port Modules area, click the + button.

The Create PPM dialog box appears.

Step 3 Choose the PPM port from the **PPM** drop-down list, and click **Apply**.

The newly created PPM appears in the Pluggable Port Modules area.

Step 4 Repeat the steps to provision additional PPMs, if needed.

Provision an Operating Mode

Use this task to provision an operating mode on the card.

The following table lists the operating modes that are supported on the cards.

Card	Operating Mode	Peer Cards	Client-Trunk Ports
MR-MXP	TXP-100G	200G-CK-LC card or 100GS-CK-C card	—
	MXP-100G	200G-CK-LC card or 100GS-CK-C card	—
	100G-B2B-CPAK	MR-MXP	CPAK
	100G-B2B-SFP-QSFP	MR-MXP	2xSFP+2xQSFP
	MXP-2X40G-2X10G	200G-CK-LC	—
100G-CK-C	TXP-100G	—	—
	RGN-100G	100G-CK-C, 100G-LC-C	—
	MXP-2x40G	—	—
100G-LC-C	TXP-100G	—	—
	RGN-100G	100G-LC-C, 100G-CK-C	—
100GS-CK-C	TXP-100G	—	—
	RGN-100G	200G-CK-LC or 100GS-CK-C	—
	MXP-CK-100G-SFP-QSFP	MR-MXP	2xSFP+2xQSFP
	MXP-CK-100G-CPAK	MR-MXP	CPAK
	MXP-200G	MR-MXP Skip card is MR-MXP.	—
	MXP-10x10G-100G	10x10G-LC Skip card is MR-MXP.	—
10x10G-LC	MXP-10x10G	100G-LC-C, 100G-CK-C, 100GS-CK-C, 200G-CK-C	—
	RGN-10G	—	1–2, 3–4, 5–6, 7–8, 9–10
	TXP-10G	—	1–2, 3–4, 5–6, 7–8, 9–10
	Low Latency	—	1–2, 3–4, 5–6, 7–8, 9–10
	Fanout-10X10G	—	—
	TXPP-10G	—	3–4–6, 7–8–10

Card	Operating Mode	Peer Cards	Client-Trunk Ports
200G-CK-LC	TXP-100G	—	—
	RGN-100G	200G-CK-C or 100GS-CK-C	—
	MXP-200G	MR-MXP Skip card is MR-MXP. OPM-10x10G or OPM-2x40G-2x10G sub OpMode is required.	—
	MXP-CK-100G-CPAK	MR-MXP	CPAK
	MXP-CK-100G-SFP-QSFP	MR-MXP	2xSFP+2xQSFP
	MXP-10x10G-100G	10x10G-LC + MR-MXP	—
CFP-LC	CFP-TXP	One or two 100G-LC-C, 100G-CK-C	—
	CFP-MXP	Only one 100G-LC-C, 100G-CK-C	—
400G-XP	REGEN-200G	—	No slices
	REGEN-100G	—	No slices
	OTNXC	—	Two slices
	MXP-2x150G	—	Three slices
	MXP	—	Four slices
1.2T-MXP	TXPMXP	—	Three Slices

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70
- Complete the Provision PPM, on page 240 task to provision the PPM on the ports of the card.
- For 1.2T-MXP card, you must pre-povision the pluggable ports, port 9, port 10 amd port 11.

Procedure

Step 1 Click the **Provisioning** > **Card Modes** tabs.

Step 2 In the Card Modes area, click the + button.

The Create Card Mode dialog box appears.

Step 3 Choose the operating mode from the **Card Mode** drop-down list.

The operating mode options vary depending on the card.

The supported card operating modes for 400G-XP are REGEN-200G, REGEN-100G, MXP-2x150G, OTNXC, and MXP. For the REGEN card mode on the 400G-XP, both trunk ports are configured with the same rate (100G or 200G). The trunk port configuration that is created for CFP2-11 is copied to CFP2-12. For the MXP 2x150G card mode on 400G-XP, both trunk ports are configured at 150G.

Step 4 Choose the Sub Mode from the **Slice** drop-down lists.

These fields are visible only for the operating modes that are supported on the 400G-XP card.

Step 5 Choose the peer card(s) from the **Peer** drop-down list.

This field is visible only if a peer card or peer cards are required for the configuration.

Step 6 Choose the sub mode from the drop-down list.

This field is visible only for the MXP-200G operating mode.

Step 7 Choose the skip peer card from the **Peer** drop-down list.

This field is visible only if a skip card is required for the configuration. This field is applicable to the MXP-200G and MXP-10x10G-100G operating modes.

Step 8 Select the port pair from the drop-down list(s).

This field is visible only if a port pair is required for the configuration. The 10x10G-LC card supports a maximum of five TXP-10G modes, two TXPP-10G modes, five RGN-10G modes, five LOW LATENCY modes, or a combination of five TXP-10G, RGN-10G, and LOW LATENCY modes.

For the TXPP-10G mode configuration on the 10x10G-LC card, client ports can be port 3, port 7, or both. You can select the port 4 and port 6 as trunk ports, when port 3 is selected as the client port. You can select port 8 and port 10 as trunk ports, when port 7 is selected as the client port.

Step 9 Click **Apply**.

The selected operating mode is provisioned on the card.

What to do next

Complete the Provision Pluggable Ports, on page 245 task.

Provision an Operating Mode

Use this task to provision an operating mode on the 40E-MXP-C, 40EX-MXP-C, or 40ME-MXP-C card.

The following operating modes are supported on the cards.

- **XM-40G-OTU3E2**—This is the default card mode. Overclock is enabled on the trunk port.
- **XM-40-OTU3**—Overclock is disabled on the trunk port.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70
- Complete the Provision PPM, on page 240 task to provision the PPM on the ports of the card.

Procedure

Step 1 Click the **Provisioning** > **Card Mode** tabs.

Step 2 Choose the operating mode from the **Card Mode** drop-down list.

Step 3 Choose the timing source from the **TimeSource** drop-down list.

The values are:

- **System-clock**—The cards synchronize to the control cards.
- **Internal-clock**—The cards automatically synchronize to one of the input client interface clocks.

Step 4 Click **Apply**.

The selected operating mode is provisioned on the card.

What to do next

Complete the Provision Pluggable Ports, on page 245 task.

Provision an Operating Mode on the OTU2-XP Card

Use this task to provision an operating mode on the OTU2-XP card.

Note Enhanced FEC and 10GE LAN to WAN operating modes are not supported by SVO.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70
- Complete the Provision PPM, on page 240 task to provision the PPM on the ports of the card.
- Complete the Provision Pluggable Ports, on page 245 task to provision at least one payload on the ports of the card.

Procedure

Step 1 Click the **Provisioning** > **Card Mode** tabs.

Step 2 Choose the operating mode from the **Card Mode** drop-down list.

Step 3 Click **Apply**.

The selected operating mode is provisioned on the card.

Provision Pluggable Ports

Use this task to provision the payloads supported on the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70
- Provision an Operating Mode, on page 240

Procedure

Step 1 Click the **Provisioning** > **Pluggable Ports** tabs.

Step 2 In the Pluggable Ports area, click the + button.

The Create Port dialog box appears.

Step 3 Choose the port number from the **Port ID** drop-down list.

Step 4 Choose the supported payload from the **Port Type** drop-down list.

Note For 1.2T-MXP card, if you try to choose a payload which is not supported by the sub operating mode of the pluggable, you will see an error message.

Step 5 Choose the number of lanes from the drop-down list.

This field is visible only in specific configurations.

Step 6 Click **Apply**.

Step 7 Repeat Step 1 through Step 6 to configure the rest of the port rates as needed.

Enable Proactive Protection

Use this task to modify the proactive protection settings of the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Proactive Protection** tabs.

Step 2 Modify required settings described in the following table.

Table 52: Proactive Protection Regen Settings

Parameter	Description	Options
Port	(Display only) Displays the port name.	—
Trigger Threshold	Sets the maximum BER threshold to trigger proactive protection.	• 1E-3 • 9E-2 to 1E-2 • 9E-3 to 1E-3 • 9E-4 to 1E-4 • 9E-5 to 1E-5 • 9E-6 to 1E-6 • 9E-7 to 1E-7
Trigger Window (ms)	Sets the duration when BER is monitored before triggering the proactive protection. The trigger window value must be a multiple of: • 10 ms for trigger thresholds between 1E-3 and 6E-6 • 100 ms for a trigger threshold between 5E-6 to 1E-7 Trigger window must be less than or equal to 500 ms for trigger thresholds between 1E-3 and 6E-6. The trigger window must be less than or equal to 3900 ms for trigger thresholds between 5E-6 to 1E-7.	Time in milliseconds.

Parameter	Description	Options
Revert Threshold	Sets the revert threshold value of BER. **Note** The revert threshold settings must be less than the trigger threshold values.	• 1E-4 • 9E-3 to 1E-3 • 9E-4 to 1E-4 • 9E-5 to 1E-5 • 9E-6 to 1E-6 • 9E-7 to 1E-7 • 9E-8 to 5E-8
Revert Window (ms)	Sets the duration when BER is monitored for settings that are less than the revert threshold value before which, proactive protection that is provided to the router is removed. The revert window value must be at least 2000 ms and a multiple of: • 10 ms for a revert threshold of 1E-4 to 6E-7. • 100 ms for a revert threshold of 5E-7 to 5E-8. The revert window must be less than or equal to 3900 ms.	Time in milliseconds.
Enable Proactive Protection	Enables proactive protection.	• Disabled • FRR Proactive Protection • Pre-FEC PSM Proactive Protection

Step 3 Click **Apply**.

Provision ODU Interfaces

Use this task to modify the ODU settings of the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **ODU Interfaces** tabs.

Step 2 Modify required settings described in the following table.

Table 53: ODU Interface Settings

Parameter	Description	Options
Port	(Display only) Displays the port name.	—
SF BER	Sets the signal fail (SF) bit error rate (BER).	Only 1E-5 is allowed.
SD BER	Sets the signal degrade (SD) bit error rate (BER).	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Squelch Mode	When a LOS is detected on the near-end client input, the far-end client laser is turned off. It is said to be squelched. Alternatively, an AIS can be invoked. The OTU2-XP card supports Squelch Mode parameter when the card mode is set as Regenerator. The valid values are Squelch and AIS. When the card mode is set to Transponder or Mixed, the Squelch Mode cannot be changed and the parameter defaults to the Squelch value.	• Squelch • AIS
SquelchHold Off Time	Sets the period in milliseconds that the client interface waits for resolution of issues on the trunk side. The client squelching starts after this period.	• Disable • 50 ms • 100 ms • 250 ms • 500 ms
Framing Type (Only OTU2-XP)	(Display only) Contains details of the encapsulated payload inside the OTN framer.	ETHERNET

Step 3 Click **Apply**.

Provision OTU Interfaces

Use this task to modify the OTU settings of the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **OTU Interfaces** tabs.

Step 2 Modify required settings described in the following table.

Table 54: OTU Interface Settings

Parameter	Description	Options
Port	(Display only) Displays the port name.	—
HD FEC	Sets the OTN lines to forward error correction (FEC). **Note** When you change the FEC mode, you will see a pop-up alerting that the change will impact the traffic. Confirm whether you want to proceed.	• DISABLE_FEC • EFEC • EFEC_14 • EFEC_17 • HG_FEC_20 • HG_FEC_7 • STANDARD_FEC **Note** Only the FEC modes applicable for the card are displayed.
Interop Mode	Enables interoperability between line cards and other vendor interfaces.	• InteropNone • InteropEnable
Supports Sync	(Display only) Displays the SupportsSync card parameter. If the value is true, the card is provisioned as a NE timing reference.	• true • false
Sync Msg In	Sets the EnableSync card parameter. Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• true • false

Parameter	Description	Options
Admin SSM In	Overrides the synchronization status message (SSM) and the synchronization traceability unknown (STU) value. If the node does not receive an SSM signal, it defaults to STU.	• G811 • STU • G812T • G812L • SETS • DUS • PRS • ST2 • ST3E • ST3 • SMC • ST4 • RES • STU_SDH • DUS_SDH • SSM_FAILED • RES_SDH • TNC
ODU Transparency (Only OTU2-XP)	Configures the ODU overhead bytes (EXP bytes and RES bytes 1 and 2). This parameter is supported only when the card is configured in Regenerator mode. The two options available for this parameter are: • Transparent Standard Use—ODU overhead bytes are transparently passed through the card. This option allows the OTU2-XP card to act transparently between the two trunk ports. • Cisco Extended Use—ODU overhead bytes are terminated and regenerated on both the ports of the regenerator group.	• Enabled (Transparent Standard Use) • Disabled (Cisco Extended Use)

Step 3 Click **Apply**.

Provision G.709 Thresholds

Use this task to provision the G.709 PM thresholds for the OTN ports.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **G.709 Thresholds** tabs.

Step 2 Choose the value for the G.709 PM thresholds, and click **Apply**.

You can set the thresholds for Near End or Far End, for 15 minutes or 1 day intervals, or for SM (OTUk) or PM (ODUk).

Table 55: G.709 PM Thresholds

Parameter	Description
ES	Errored Seconds shows the number of errored seconds recorded during the PM time interval.
SES	Severely Errored Seconds shows the severely errored seconds recorded during the PM time interval.
UAS	Unavailable Seconds shows the unavailable seconds recorded during the PM time interval.
BBE	Background block error shows the number of background block errors that are recorded during the PM time interval.
FC	Failure Counter shows the number of failure counts recorded during the PM time interval.

Provision FEC Thresholds

Use this task to provision the FEC thresholds for the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **FEC Thresholds** tabs.

Step 2 Choose the value for the FEC PMs and click **Apply**.

You can set the FEC thresholds for 15 minutes or one-day intervals.

The possible PM types are:

- BIT-EC—Sets the value for bit errors corrected.
- UNC-WORDS—Sets the value for uncorrectable words.

Provision Trail Trace Monitoring

This task provisions the trail trace monitoring parameters that are supported for both the OTU and ODU payloads. Trail trace monitoring is supported on all the cards except CFP-LC.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Trail Trace Monitoring** tabs.

Step 2 From the Level drop-down list, choose **Section** to list all the OTU interfaces and **Path** to list all the ODU interfaces.

Step 3 Modify required settings as described in the following table.

Table 56: Trail Trace Identifier Settings

Parameter	Description	Options
Port	Displays the port number.	—
Tx-SAPI (All cards except 40E-MXP-C and OTU2-XP)	Displays the current Source Access Point Identifier (SAPI) transmit string of the TTI or sets a new transmit string.	0–15 bytes
Tx-DAPI (All cards except 40E-MXP-C and OTU2-XP)	Displays the current Destination Access Point Identifier (DAPI) transmit string of the TTI or sets a new transmit string.	0–15 bytes
Tx-Operator (All cards except 40E-MXP-C and OTU2-XP)	User operator data of the TTI.	0–32 bytes
Legacy Tx-TTI (Only 40E-MXP-C and OTU2-XP)	Displays the current transmit string of the TTI or sets a new transmit string.	0-64 bytes
Expected-SAPI (All cards except 40E-MXP-C and OTU2-XP)	Displays the current expected SAPI string or sets a new expected string.	0–15 bytes
Expected-DAPI (All cards except 40E-MXP-C and OTU2-XP)	Displays the current expected DAPI string or sets a new expected string.	0–15 bytes
Legacy Expected-TTI (Only 40E-MXP-C and OTU2-XP)	Displays the current expected string or sets a new expected string.	0-64 bytes
Rx-SAPI (All cards except 40E-MXP-C and OTU2-XP)	(Display only) Displays the current received SAPI string.	—

Parameter	Description	Options
Rx-DAPI (All cards except 40E-MXP-C and OTU2-XP)	(Display only) Displays the current received DAPI string.	—
Rx-Operator (All cards except 40E-MXP-C and OTU2-XP)	(Display only) User operator data of the TTI.	—
Legacy Rx-TTI (Only 40E-MXP-C and OTU2-XP)	(Display only) Displays the current received string.	—
Alarm Propagation	If a discrepancy is detected between the expected and received trace, it raises an alarm. If set to True, the alarm is propagated downstream to the other nodes.	• True • False
Detect Mode	Sets the mode for detecting the discrepancy between the expected and received trace.	• Disabled • Enabled • SAPI (All cards except 40E-MXP-C and OTU2-XP) • DAPI (All cards except 40E-MXP-C and OTU2-XP) • SAPI-and-DAPI (All cards except 40E-MXP-C and OTU2-XP)

Step 4 Click **Apply**.

Provision SONET/SDH Interfaces

Table 57: Feature History

Feature Name	Release Information	Feature Description
OC192 and STM64 Payload Support for MR-MXP Card	Cisco NCS 2000 Release 12.3	OC192 and STM64 payloads are now supported on the MR-MXP card. This feature allows you to: • Provision SONET/SDH interfaces. • Provision SONET/SDH trace monitoring parameters for OC192 and STM64 payloads. • Provision SONET/SDH thresholds.

Use this task to provision the parameters for the SONET/SDH interfaces of 10x10G-LC, 40E-MXP, 400G-XP, MR-MXP and OTU2-XP cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **SONET/SDH Interfaces** tab.

Step 2 Modify required settings as described in the following table.

Table 58: Card SONET/SDH Settings

Parameter	Description	Options
Port	Displays the port number.	—
Type	(Display only) Reports the current payload for the port. OC192 is displayed for SONET systems and STM64 is displayed for SDH systems.	• OC192 • STM64

Parameter	Description	Options
SF BER	Sets the signal fail (SF) bit error rate (BER).	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade (SD) bit error rate (BER).	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-8
Squelch Mode	When a LOS is detected on the near-end client input, the far-end client laser is turned off. It is said to be squelched. Alternatively, an AIS can be invoked.	• Squelch • AIS
Squelch Hold Off Time	Sets the period in milliseconds that the client interface waits for resolution of issues on the trunk side. The client squelching starts after this period.	• Disable • 50 ms • 100 ms • 250 ms • 500 ms
ProvidesSync	(Display only) Displays the ProvidesSync card parameter.	• true • false
Send DoNotUse	When checked, sends a “Do Not Use for Synchronization (DUS)” message on the S1 byte.	• true • false
Sync SyncMsgIn	Sets the ProvidesSync card parameter. Enables synchronization status messages, which allow the node to choose the best timing source.	• true • false

Parameter	Description	Options
Admin SSM	Overrides the synchronization status message (SSM) and the synchronization traceability unknown (STU) value. If the node does not receive an SSM signal, it defaults to STU.	• DUS • PRS • RES • SMC • ST2 • ST3 • ST3E • ST4 • STU • TNC
Termination Mode	Sets the termination mode. When a session is terminated, the signal is reinitialized or is passed through without any changes. For 400G-XP, 10x10G-LC, and OTU2-XP cards it is Transparent by default. For 40E-MXP card, it is Transparent by default but can be set to the other values as required.	For SONET: • Transparent • Line • Session For SDH: • Transparent • Multiplex Section • Regeneration Section

Step 3 Click **Apply**.

Provision SONET/SDH Trace Monitoring

This task provisions the trace monitoring parameters that are supported for both the OC192 and STM64 payloads. SONET/SDH trace monitoring is supported on 10x10G-LC, 40E-MXP, 400G-XP, MR-MXP and OTU2-XP cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **SONET/SDH Trace Monitoring** tabs.

Step 2 Modify required settings as described in the following table.

Table 59: SONET/SDH Trace Identifier Settings

Parameter	Description	Options
Port	Displays the port number.	—
Tx-String	Sets a new transmit string.	0–15 bytes
Expected-String	Sets a new expected string.	0–15 bytes
Rx-String	(Display only) Displays the current received string.	
Detect-Mode	Sets the mode for detecting the discrepancy between the expected and received trace.	• True • False
Trace-Format	Sets the format in which the received string is displayed.	• 1BYTE • 16BYTE • 64BYTE

Step 3 Click **Apply**.

Provision ZR Plus Interfaces

Use this task to provision the parameters for the ZR Plus interfaces of the 1.2T-MXP card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **ZR Plus Interfaces** tabs.

Step 2 Modify any of the ZR Plus settings as described in the following table. These parameters depend on the card mode.

Table 60: Card ZR Plus Settings

Parameter	Description	Options
Port	(Display only) Displays the port number	—
Squelch Mode	(Display only) Displays the squelch mode	• LF
Squelch Hold Off Time	Sets the period in milliseconds that the client interface waits for resolution of issues on the trunk side. The client squelching starts after this period	• Disable
FEC	Sets the FEC mode	OFEC_15_DE_ON
GroupId	Sets the GroupId that uniquely identifies a group of physical ports in a ZR frame. This makes sure that noncompliant groups do not interoperate. When a mismatch in the group is identified, GIDM alarm is raised.	1–255

Step 3 Click **Apply**.

Provision ZR Plus Trail Trace Monitoring

This task provisions the trail trace monitoring parameters that are supported for the ZR plus payloads on the 1.2T-MXP card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **ZR Plus Trail Trace Monitoring** tabs.

Step 2 Modify any of the ZR Plus settings as described in the following table.

Table 61: ZR plus Trail Tracing Settings

Parameter	Description	Options
Port	(Display only) Displays the port number.	—
Send-Tti	Sets the transmit TTI String.	0–32 Bytes
Expected-Tti	Sets the expected TTI String.	0–32 Bytes
Received-Tti	(Display only) Displays the received TTI String.	0–32 Bytes

Note
- When the trunk port is in OOS-DSBL state, its received TTI is not displayed in the GUI.
- Sometimes, the received TTI value takes up to ten seconds to get displayed in the GUI.

Step 3 Click **Apply**.

Provision Optical Channels

Use this task to provision the parameters for the optical channels on the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Optical Channel** tabs.

Step 2 Modify required settings described in the following table.

Table 62: Optical Channel Settings

Parameter	Description	Options
Port	(Display only) Displays the port name.	—
Reach	Indicates the distance from one node to another node.	• Auto Provision • List of reach values

Parameter	Description	Options
SD FEC	Indicates the standard FEC.	• SD_FEC_15_DE_OFF • SD_FEC_15_DE_ON • SD_FEC_20 • SD_FEC_25_DE_OFF • SD_FEC_25_DE_ON • SD_FEC_7
Tx Power (dBm)	Sets the Tx power on the trunk port.	The range is –10.0 to 0.25 dBm.
PSM Info	When enabled on a TXP or MXP trunk port that is connected to a PSM card, it allows fast switching on the cards.	• NA • Enable • Disable
Frequency (THz)	Sets the frequency in THz	-
Wavelength (nm)	(Display only) Wavelength is set based on the frequency.	-
Tx Shutdown	(Display only)	• true • false
Width (GHz)	(Display only)	-
CD (Working Range) High (ps/nm)	Sets the threshold for maximum chromatic dispersion.	-
CD (Working Range) Low (ps/nm)	Sets the threshold for minimum chromatic dispersion.	-
Admin State	Sets the port service state unless network conditions prevent the change.	• Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/ OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/ OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)

Parameter	Description	Options
OTN Enabled (Only OTU2-XP)	Sets the OTN lines according to ITU-T G.709.	• true • false

Step 3 Click **Apply**.

Provision Optics Thresholds

Use this task to provision the optics thresholds of all the payload ports of the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Optics Thresholds** tabs.

Step 2 Choose the types (Alarm or TCA) and 15-minute or one-day intervals, and click **Apply**.

Step 3 Modify required settings described in the following table.

Table 63: Optics Threshold Settings

Parameter	Description
Port	(Display only) Displays the port name
RX Power High (dBm)	Sets the maximum optical power received
RX Power Low (dBm)	Sets the minimum optical power received
TX Power High (dBm)	Sets the maximum optical power transmitted
TX Power Low (dBm)	Sets the minimum optical power transmitted
CD (Working Range) High (ps/nm)	Sets the threshold for maximum chromatic dispersion
CD (Working Range) Low (ps/nm)	Sets the threshold for minimum chromatic dispersion
Laser Bias High (%)	Sets the maximum laser bias
OSNR Power High (dBm)	Maximum Optical Signal to Noise Ratio (OSNR) during the PM time interval

Parameter	Description
OSNR Power Low (dBm)	Minimum OSNR during the PM time interval
PMD High (ps)	Maximum Polarization Mode Dispersion (PMD) during the PM time interval
PMD Low (ps)	Minimum PMD during the PM time interval

Step 4 Click **Apply**.

Provision Ethernet Interfaces

Use this task to provision the parameters for the Ethernet interfaces of the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the tabs.

Step 2 Modify any of the Ethernet settings as described in the following table. These parameters appear depends on the card mode.

Table 64: Card Ethernet Settings

Parameter	Description	Options
Port	(Display only) Displays the port number	—
Speed	Sets the expected port speed.	—
FEC	Sets the FEC mode. When set to On, FEC is enabled.	• NA • Auto (default) • On • Off
MTU	Sets the maximum size of the Ethernet frames that are accepted by the port. The port must be in OOS/locked state.	Numeric. Default: 1548 Range 64–9700
Duplex	Sets the expected duplex capability of ports.	• Full • Half

Parameter	Description	Options
Mapping	Sets the mapping mode.	• CBR • GFP
Autonegotiation	Enables or disables autonegotiation on the port.	• Disabled • Enabled
Squelch Mode	Sets the squelch mode.	• Disable • Squelch • LF
Squelch Hold Off time	Sets the period in milliseconds that the client interface waits for resolution of issues on the trunk side. The client squelching starts after this period or local fault is sent.	• Disable • 50 ms • 100 ms • 250 ms • 500 ms

Step 3 Click **Apply**.

Provision RMON Thresholds

Use this task to create and list the RMON thresholds of the Ethernet ports of the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **RMON Thresholds** tabs.

Step 2 Click the + button.

The Create RMON Threshold dialog box appears.

Step 3 From the **Port ID** drop-down list, choose the Ethernet port.

Step 4 From the **Variable** drop-down list, choose a variable. The following tables lists the available variables.

Table 65: Card Ethernet Variables

Variable	Description
ifInOctets	Number of bytes received since the last counter reset.
RxTotalPkts	Total number of received packets.
IfInUcastPkts [15]	Total number of packets that are delivered by this sublayer to a higher sublayer that is not addressed to a multicast or broadcast address.
IfInMulticastPkts [1]	Total number of packets that are delivered by this sublayer to a higher sublayer that is addressed to a multicast address. For a MAC layer protocol, this includes both group and functional addresses.
IfInBroadcastPkts [1]	Total number of packets that are delivered by this sublayer to a higher sublayer that is addressed to a broadcast address.
IfInErrors	Total number of received errors.
IfOutOctets	Total number of octets transmitted out of the interface, including framing characters.
TxTotalPkts	Total number of transmitted packets.
IfOutUcastPkts	Total count of packets that are transmitted to a unicast group destination address.
IfOutMulticastPkts	Total number of packets that higher-level protocols requested to be transmitted, which are addressed to a multicast address at this sublayer. These include packets that are discarded or not sent. For a MAC layer protocol, this includes both group and functional addresses.
IfOutBroadcastPkts	Total number of packets that higher-level protocols requested to be transmitted, which are addressed to a broadcast address at this sublayer. These include packets that are discarded or not sent.
Dot3StatsAlignmentErrors	Total number of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. This counter is only valid for FE modes of operation.
Dot3StatsFCSErrors	Total number of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
Dot3StatsFrameTooLong	Total number of frames received on a particular interface that exceed the maximum permitted frame size.

EtherStatsUndersizePkts	Total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and are otherwise well formed.
EtherStatsFragments	Total number of packets received that are less than 64 octets in length (excluding framing bits, but including FCS octets) and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error). Note that it is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
EtherStatsPkts	Total number of frames that are received on an interface in both Rx and Tx directions.
EtherStatsPkts64Octets	Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits, but including FCS octets).
EtherStatsPkts65to127Octets	Total number of packets (including bad packets) received that are from 65 through 127 octets in length inclusive (excluding framing bits, but including FCS octets).
EtherStatsPkts128to255Octets	Total number of packets (including bad packets) received that are from 128 through 255 octets in length inclusive (excluding framing bits, but including FCS octets).
EtherStatsPkts256to511Octets	Total number of packets (including bad packets) received that are from 256 through 511 octets in length inclusive (excluding framing bits, but including FCS octets).
EtherStatsPkts512to1023Octets	Total number of packets (including bad packets) received that are from 512 through 1023 octets in length inclusive (excluding framing bits, but including FCS octets).
EtherStatsPkts1024to1518Octets	Total number of packets (including bad packets) received that are from 1024 through 1518 octets in length inclusive (excluding framing bits, but including FCS octets).
EtherStatsBroadcastPkts	Total number of good packets received that are directed to the broadcast address. This total number does not include multicast packets.
EtherStatsMulticastPkts	Total number of good packets received that are directed to a multicast address. This total number does not include packets that are directed to the broadcast address.
EtherStatsOversizePkts	Total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets) and are otherwise well formed.

EtherStatsJabbers	Total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).
EtherStatsOctets	Total number of octets of data (including those data in bad packets) received on the network (excluding framing bits, but including FCS octets).
EtherStatsPkts1519toMaxOctets	Total number of packets (including bad packets) received that were 1591 octets in length (excluding framing bits, but including FCS octets).

[15] The counter does not increment for traffic with incorrect Ethertype and packet size of more than 64 bytes on the 10x10G-LC and 100G-LC-C cards.

Table 66: 10x10G-LC FC/FICON Variables

Variable	Description
RxTotalPkts	Total number of received packets.
TxTotalPkts	Total number of transmitted packets.
MediaIndStatsRxFramesBadCRC	Total number of received data frames with payload CRC errors when an HDLC framing is used.
MediaIndStatsTxFramesBadCRC	Total number of transmitted data frames with payload CRC errors when the HDLC framing is used.
MediaIndStatsRxFramesTruncated	Total number of frames received that are less than 5 bytes. This value is a part of the High-Level Data Link Control (HDLC) and GFP port statistics.
MediaIndStatsTxFramesTruncated	Total number of transmitted data frames that exceed the MTU. This value is a part of the HDLC and GFP port statistics.
MediaIndStatsRxFramesTooLong	Total number of received frames that exceed the maximum transmission unit (MTU). This value is part of the HDLC and GFP port statistics.
MediaIndStatsTxFramesTooLong	Total number of transmitted data frames that are less than 5 bytes. This value is a part of the HDLC and GFP port statistics.
IfInOctets	Total number of octets received on the interface, including the framing octet.
IfOutOctets	Total number of octets transmitted out of the interface, including framing characters.
IfInErrors	Total number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.

Variable	Description
IfOutErrors	Total number of outbound packets or transmission units that could not be transmitted because of errors.

Table 67: 10x10G-LC GFP RMON Variables

Variable	Description
GfpStatsRxFrame	Total number of received data frames.
GfpStatsTxFrame	Total number of transmitted data frames.
GfpStatsRxCRCErrors	Total number of CRC errors with the receive transparent GFP frame.
GfpStatsRxOctets	Total number of GFP data octets received.
GfpStatsTxOctets	Total number of GFP data octets transmitted.
GfpStatsRxSBitErrors	Received GFP frames with single bit errors in the core header (these errors can be corrected).
GfpStatsRxMBitErrors	Received GFP frames with multiple bit errors in the core header (these errors cannot be corrected).
GfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when we expect Fibre Channel data.
GfpRxCmfFrame	—
GfpRxCmfFrame	—

Step 5 From the **Alarm Type** drop-down list, indicate whether the event is triggered by the rising threshold, falling threshold, or both rising and falling thresholds.

The available options are Rising Threshold, Falling Threshold, and Rising and Falling Threshold.

Step 6 From the **Sampling Type** drop-down list, choose either **Relative** or **Absolute**.

Relative restricts the threshold to use the number of occurrences in the user-set sample period. **Absolute** sets the threshold to use the total number of occurrences, regardless of the time period.

Step 7 Enter the appropriate number of seconds in the **Sampling Period** field.

Step 8 Enter the appropriate number of occurrences in the **Rising Threshold** field.

For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1000 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

Step 9 Enter the appropriate number of occurrences in the **Falling Threshold** field. In most cases, a falling threshold is set to a lower value than the value of the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15-seconds subsides and creates only 799 collisions in 15 seconds, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15-second period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise, a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 10 Click **Apply**.

Provision SONET/SDH Thresholds

Use this task to provision the SONET/SDH thresholds of the OC192 and STM64 payload ports of the card. SONET/SDH threshold provisioning is supported on 10x10G-LC, 40E-MXP, 400G-XP, MR-MXP and OTU2-XP cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **SONET/SDH Thresholds** tabs.

Step 2 Thresholds can be set for near-end or far-end directions for either the 15-minute or 1-day intervals. For SONET/ANSI and OC192 systems, you can select Line or Section types. For SDH/ETSI and STM64 systems, you can select Regeneraion or Multiplex types.

Table 68: SONET/SDH Threshold Settings

Parameter	Description	Options
Interface Name	Displays the interface name.	—
PM Type	Sets the PM type.	• ES • SES • UAS • EB • SEFS
Low	Sets the low threshold value.	—
High	Sets the high threshold value.	—

Step 3 Click **Apply**.

Provision Loopback

Use this task to provision loopback on the card.

Caution This task is traffic-affecting.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70
- Perform the loopback configuration only in the maintenance service state. To place the trunk ports in the Locked, maintenance state, see Provision Optical Channels, on page 260.

Procedure

Step 1 Click the **Maintenance** > **Loopback** tabs.

From R12.1, the colomns **Admin State** and **Service State** are added to the **Loopback** table.

Step 2 From the **Loopback Type** drop-down list, choose Terminal, Facility, Terminal-Drop, or Facility-Drop for each port required.

Step 3 Click **Apply**.

Provision Optical Safety

Use this task to provision the optical safety parameters for cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Optical Safety** tabs.

Step 2 Modify required settings described in the following table:

Table 69: Optical Safety Parameters for Cards

Parameter	Description	Options
Interface	(Display only) Displays the port name, port type, and direction.	—
Supported Safety	(Display only) Displays the supported safety mechanism.	• ALS for line cards and control cards. • ALS-OSRI for amplifier cards.
ALS Mode	Automatic laser shutdown mode. The ALS mode is disabled for RX ALS interfaces.	From the drop-down list, choose one of the following: • ALS-Disabled—Deactivates ALS. • Automatic Restart—(Default) ALS is active. The power is automatically shut down when needed, and it automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart
OSRI	Optical safety remote interlock. The default value is OSRI-OFF. When set to OSRI-ON, the TX output power is shut down. **Note** OSRI configuration is not supported on the transponder and muxponder cards.	From the drop-down list, choose one of the following: • OSRI-OFF • OSRI-ON
ALS Status	(Display only) ALS status of the device.	• Working • Shutdown
Recovery Pulse Interval	Displays the interval between two optical power pulses.	60 to 300 seconds.
Recovery Pulse Duration	Displays the duration of the optical power pulse that begins when an amplifier restarts.	2 to 100 seconds

Parameter	Description	Options
Manual Restart	Triggers manual restart action for the ALS interface. However, manual restart does not happen if Mode is set to Automatic Restart or Disabled.	—

Step 3 Click **Apply** to save the changes.

Provision PRBS

This task provisions the Pseudo Random Binary Sequence (PRBS) settings on the card.

PRBS supports the following cards:

- 100G-LC-C, 100G-CK-C, and 200G-CK-C cards in TXP-100G operating mode
- 200G-CK-C and MR-MXP card combination in MXP-CK-100G-CPAK operating mode

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Change the admin state on the trunk port to Locked, disabled (ETSI) /OOS,DSBLD (ANSI). See Provision Optical Channels, on page 260.

Step 2 Click the **Maintenance** > **PRBS** tabs.

From R12.1, the colomns **Admin State** and **Service State** are added to the **PRBS** table.

Step 3 From the Generator Pattern drop-down list, choose a pattern for each port.The supported patterns are PRBS_NONE and PRBS_PN31.

Apply the same pattern in both source and destination trunk ports.

Step 4 Click **Apply**.

The Pattern Sync Status field displays one of the following values:

- PATTERN_OK: When the port is receiving one of the recognized patterns.
- PATTERN_ERROR—When the port is receiving a recognized pattern but the pattern contains errors. This error also occurs when there is a pattern mismatch.
- PATTERN_NONE—When the port is not receiving a recognized PRBS pattern.

In case of pattern errors, the card provides a PRBS error counter. The counter zeroes itself when the PRBS is disabled.

Step 5 Change the admin state on the trunk port to Unlocked (ETSI) /IS (ANSI). See Provision Optical Channels, on page 260.

Provision ODU Circuit

Use this task to provision ODU circuit created through NETCONF client, in the OTNXC mode of the 400G-XP card.

Both unprotected and protected ODU connections or OTNXC circuits that are created in CTC will be available in the SVO, Release 12.3 user interface after the NCS2000 device is upgraded from CTC to SVO and the device sync is completed. The ODU connection data that is displayed in the SVO user interface has the following discrepancies:

- When ODU connections are discovered, SVO autogenerates the connection name as "device-name/object index" (an integer number) and displays the connection name as Circuit ID.
- CTC allows creating a protected ODU connection with two trunk ODU sources and one client ODU destination. But SVO considers this protected ODU connection as invalid. Hence as part of discovery, SVO recreates the protected ODU connection with one source client and two destination trunk ODUs, by swapping.

Use this task to provision ODU circuit created in the OTNXC mode of the 400G-XP card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **OTN Circuit** tabs.

The **OTN Circuit** tab displays the following information:

- Circuit ID—Unique identifier for the end-to-end circuit
- Connection label—Unique identifier for ODU connections
- Bandwidth—Bandwidth of the circuit. Supported values are ODU4, ODU2, ODU2e
- Direction—Only bidirectional is supported
- Source—Source ODU port
- Destination—Destination ODU port
- Protection Reference—Displays the Protection port

- Admin State—Displays the admin state
- Service State—Displays the service state
- ILK Usage—Displays interlink port usage

Step 2 Click the plus icon to view the **Protection Attributes** of the circuit.

Step 3 (Optional) Edit the **Connection label** and the **Admin State**.

Step 4 (Optional) Click **ODU Utilization** to view ODU Utilization information.

An ODU utilization window for the 400G-XP-LC card is displayed where you can get information about the availability of each port for ODU circuit creation. All ODU ports are displayed according to the slice configuration that was configured. Each row represents 100G or ODU4 bandwidth. The client ports are listed first followed by the trunk ports. The ports that are already used by the ODU circuit are displayed in green, the ports that are available for circuit creation are displayed in orange and the ports that are not applicable nor configured are displayed in gray.

To view Bandwidth Utilization using the NETCONF client, use the following RPCs:

- To show the utilization under odu-interface which is part of otn-xc connection:

```
<action xmlns="urn:ietf:params:xml:ns:yang:1">
    <svo xmlns="http://cisco.com/yang/svo">
      <odu-connection-commands>
        <interface-otnxc-utilization>
          <interface-name>1/3/11/1-1</interface-name>
        </interface-otnxc-utilization>
      </odu-connection-commands>
    </svo>
  </action>
```

- To show card level utilization (You enter the shelf and slot info.):

```
<action xmlns="urn:ietf:params:xml:ns:yang:1">
    <svo xmlns="http://cisco.com/yang/svo">
      <odu-connection-commands>
        <module-otnxc-utilization>
          <uid>1</uid>
          <module-id>3</module-id>
        </module-otnxc-utilization>
      </odu-connection-commands>
    </svo>
  </action>
```

Step 5 Click **Apply**.

You can edit only the Admin State and the Connection label in the SVO user interface. For protected ODU connection, Protection group Name, Revertive mode, and Revertive time can be edited from NETCONF, and web user interface (under the **Provisioning** > **Protection** tabs in the shelf view).

Note From Cisco NCS 2000 Release 12.3.1, you can configure Hold Off Timer for OTN-XC protection groups from **Chassis > Provisioning > Protection** tab in the SVO user interface and using the NETCONF client.

View Circuit Protection Parameters

Use this task to display the protection parameters of ODU circuit created in the OTNXC mode of the 400G-XP card. The protection parameters are defined when a protected ODU circuit is created through NETCONF client.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Maintenance** > **Protection** tabs to view the following protection parameters:

- **Name**—Name of the protection group.
- **Protection Type**—Type of the protection.
- **Active Interfaces**—The interfaces on which the traffic is present.
- **Working Interfaces**—The working interfaces are the active interfaces when the protection group is created.
- **Protection Interfaces**—The protection interfaces when the protection group is created.
- **Switch Type**—The switch type is bidirectional-switching.
- **Revertive**—Choose True or False. If set to true, the traffic reverts to the working port after failure conditions remain corrected for the amount of time that is entered in the Reversion Time field.
- **Reversion Time (min)**—Reversion time is the amount of time that will elapse before the traffic reverts to the working port. The reversion timer starts after conditions causing the switch are cleared. The range is from one to 12 minutes.
- **Reversion Pulse Width (sec)**—Reversion Pulse Width is not applicable for the ODU circuit.

Note The following fields in the protection group are editable in the **Chassis view** > **Provisioning** tab:

- Name
- Revertive
- Reversion Time
- Reversion Pulse Width

Step 5 Click + to view the protection group data.

The interfaces of the protection group are displayed.

- **Interface**—Displays the name of the interface
- **Entity**—Displays the entity of the interface, whether it is working or protect
- **Entity Status**—Displays the status of the entity, whether it is active or Standby
- **Switch Status**—Displays the switch status when a switch operation is performed.

Step 6 To perform a switch operation between the interfaces of a protection group, perform these steps:

a. Check the check box of the interface that has **Entity Status** as active.

b. Click **Edit**.

The **Switch Command** dialog box appears.

c. Select an option from the **Action** drop-down list.

The options available are—Lock-Out, Force-Switch, Manual-Switch, and Release.

d. Click **Apply**.

Note SVO does not support the Y-cable protection type. If a Y-cable protected circuit is available in the system, SVO cannot fetch the data when you expand the protection data.

Retrieve MAC Addresses through LLDP

Use this task to retrieve the source MAC address of the host connected to the 100GE or 400GE ports of 1.2T-MXP card, after a Link Layer Discovery Protocol (LLDP) packet is received on the client port.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **LLDP** tabs.

Step 2 Click **Refresh**.

The table displays the following fields:

- Port—Displays the port number.
- Source MAC Address—Displays the MAC address of the node to which the port is connected.

Limitations of LLDP Support on the 1.2T-MXP Card

The LLDP support on the 1.2T-MXP card has the following limitations:

- The 1.2T-MXP card can handle only one LLDP packet of 2000byte size per client every four seconds.
- LLDP packet is not detected when the client ports if moved to from IS to OOS.
- After the trunk port transits from OOS to IS, there is a delay of 12 to15 seconds to detect the LLDP packet and display it on the GUI.
- LLDP capture does not happen when CFP2 DCO associated with the client port is not plugged in.
- The 1.2T-MXP card captures the LLDP packets only when:
  1. The value of ETH TYPE header is 0x88CC.
  2. The destination Multicast addresses are:
     - 01:80:C2:00:00:00
     - 01:80:C2:00:00:0e
     - 01:80:C2:00:00:03

Provision FPD Upgrade for the Ports

Table 70: Feature History

Feature	Release Information	Description
Selective FPD Upgrade Support	Cisco NCS 2000 Release 12.3	You can select any DCO port for the FPD upgrade, based on the requirement.

When the firmware version on the DCO trunk port is earlier than the NCS 2000 package firmware version, an alarm "FPD-UPG-REQUIRED" is raised on that trunk port in the **Alarms** tab. Each trunk port has separate upgrade alarm.

You can view the DCO running firmware version and the NCS 2000 package firmware version under the **Maintenance** > **FPD upgrade** tabs.

Use this task to upgrade DCO (trunk ports) on the 1.2T-MXP card with the latest firmware released as part of the NCS 2000 software release.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **FPD Upgrade** tabs.

Step 2 Choose the DCO ports that you want to upgrade.

You can consider the following use cases to choose the DCO ports for upgrade:

- When the DCO ports have both traffic-affecting and non-traffic affecting upgrade alarms, you can select only the DCO ports with non-traffic affecting upgrade alarms and proceed with the firmware upgrade without affecting traffic on the node.
- If the upgrade is required only for a DCO on a specific circuit, you can select that particular DCO and perform the upgrade without disturbing any other DCO ports.

Step 3 Click **FPD upgrade** to perform firmware upgrade for the chosen ports.

After the firmware upgrade is completed successfully, the "FPD-UPG-REQUIRED" alarm gets cleared in the **Alarms** tab and you can view the updated running firmware version in the **FPD Upgrade** table.

Provision FPD Upgrade for MR-MXP Card

Table 71: Feature History

Feature	Release Information	Description
FPD Upgrade for MR-MXP Card	Cisco NCS 2000 Release 12.3.1	The SVO web interface now displays the running firmware information for the MR-MXP card. It also displays the latest available firmware for the NCS 2000 software release. You can compare and upgrade the firmware to the required release directly from SVO.

When the firmware version on the MR-MXP card is earlier than the NCS 2000 package firmware version, an alarm "TRAF-AFFECT-RESET-REQUIRED" is raised on that card in the **Alarms** tab.

You can view the running firmware version and the NCS 2000 package firmware version under the **Maintenance** > **FPD upgrade** tabs.

Use this task to upgrade the MR-MXP card with the latest firmware released as part of the NCS 2000 software release.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **FPD Upgrade** tabs.

Step 2 Click **FPD upgrade** to perform firmware upgrade for the card.

After the firmware upgrade is completed successfully, the "TRAF-AFFECT-RESET-REQUIRED" alarm gets cleared in the **Alarms** tab and you can view the updated running firmware version in the **FPD Upgrade** table.

Functional Module Group

Table 72: Feature History

Feature Name	Release Information	Feature Description
Functional Module Group Stepper	Cisco NCS 2000 Release 12.3	The Functional Module Group stepper enables you to configure a card mode for a primary card when adding the primary card to the chassis. You can configure the compatible peer cards, pluggables and sub modes for the primary card.

Functional Module Group (FMG) stepper simplifies the process of configuring the operating modes for transponder and muxponder cards. In the previous releases, you must navigate through multiple tabs in the SVO application to make the appropriate selections. With the FMG stepper, you can configure the operating modes and sub operating modes of different cards with specific client payloads in simple steps.

Configure Card Mode using Functional Module Group

Use this task to configure the operating mode and sub operating modes of a card while adding it to the NCS 2006 or NCS 2015 chassis.

Before you begin

- Log into the SVO Web Interface, on page 67
- Add a Chassis, on page 73

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack title to zoom into the required rack in the left panel.

The enlarged view of the rack appears.

Use the plus and minus icons to zoom in and out of the rack.

Step 3 Left-click the empty slot in the chassis where you want to add the card.

The dialog box for the selected slot appears.

Note Configuration of card mode cannot start from slot 16 in NCS 2015 chassis.

Step 4 Click **FMG Provision** to add a card to the chassis and configure its card mode.

The **Functional Module Group** wizard appears.

Step 5 In **Add primary module**, perform the steps to choose a primary card.

a) Choose a primary card from the **Select primary module** drop-down list.

Note When adding the NCS2K-400G-XP or NCS2K-100GS-CK-C card, ensure to follow the correct slot combinations in NCS 2006 and NCS 2015 chassis. If correct slot combinations are not available, the **Select primary module** drop-down list does not display the NCS2K-400G-XP or NCS2K-100GS-CK-C card. For more details on slot combinations, see 400G-XP-LC400G-XP Card, on page 204 and Operating Modes for 100G-LC-C, 100G-CK-C, 100GS-CK-C, and 200G-CK-C Cards, on page 202 sections.

A preview of the selected card appears below the drop-down list.

b) Click **Next**.

Step 6 In **Select card mode**, perform the steps to configure a card mode.

a) Choose the required card mode configuration from the drop-down list.

Note The number of available card mode configurations differ based on the primary card selected. For more information on the card mode configurations, see Provision an Operating Mode, on page 240.

b) Click **Add**.

When adding the 15454-M-10x10G-LC card, you can choose multiple card mode configurations. You must choose trunk ports for the RGN-10G, TXP-10G, Low Latency and TXPP-10G card modes, and client port for TXP-10G card mode.

When adding the NCS2K-400G-XP card, you must choose slice configurations for the card mode selected. For more information on NCS2K-400G-XP slice configurations, refer to the *Configuration Options for the 400-XP Card Modes* table in Key Features, on page 207.

c) Click **Next**.

Step 7 In **Add secondary modules**, perform the steps to configure the required peer card.

a) Choose the peer card from the **Select secondary modules** drop-down list.

Note The **Functional Module Group** wizard lists the compatible peer cards for the selected primary card and its card mode configuration. For NCS2K-100GS-CK-C and NCS2K-200G-CK-C cards, you must choose sub operating modes for MXP-200G card mode from the **Submode** drop-down list.

A preview of the selected peer card appears below the drop-down list.

b) Click **Next**.

Note For standalone card modes, the **Functional Module Group** wizard skips the **Add secondary modules** step.

Step 8 In **Add pluggables**, perform the following steps to configure the pluggable parameters.

Note You need to configure the pluggable port modules and pluggables ports for the primary card followed by the secondary cards.

a) In the **Pluggable Port Modules** pane, choose from the **PPM** drop-down list and click **Add**.

The added port modules appear below the drop-down list.

b) In the **Pluggable Ports** pane, choose from the **Port ID** and **Port Type** drop-down lists and click **Add**.

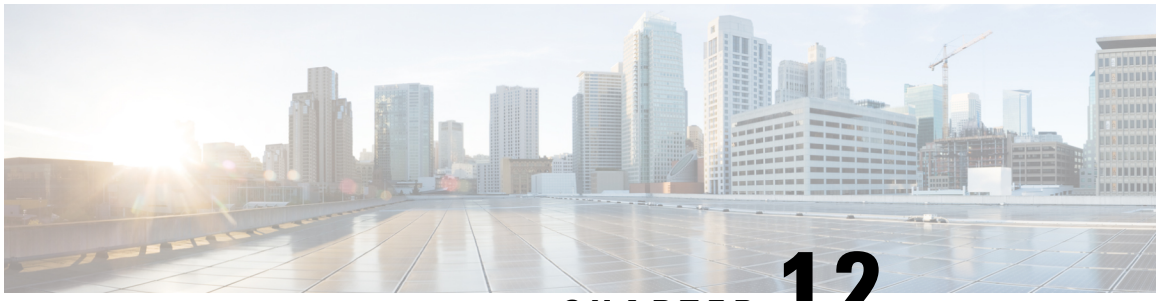
The added Port ID and Port Type appear below the drop-down list.

c) Click **Next**.

A preview of the configured cards, pluggable port modules and pluggable ports appear in **Configuration recap**. If sub modes and slices are configured, then a preview of the sub modes and slices are also displayed.

Step 9 Click **Finish**.

Note Errors are displayed if the configuration is inaccurate.



CHAPTER 12

Provision Optical Service Channel Cards

This chapter describes the Optical Service Channel cards used in Cisco NCS 2000 SVO and its related tasks.

This table lists the package support for the OSC-CSM card.

Card	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
OSC-CSM		✓

OSC-CSM Card

Table 73: Feature History

Feature Name	Release Information	Description
OSC-CSM Card	Cisco NCS 2000 Release 12.2	The OSC-Combiner or Splitter Module (OSC-CSM) card provides access to the OSC received signal, while expressing the remaining wavelengths and its transmitted signal is optically coupled into the fiber together with the transmitted wavelengths, in an unamplified node. The OSC-CSM card is used in nodes without a booster amplifier for OSC-CSM operation. The optical interface of the card provides extended optical reach to meet the node-to-node distances that are found in typical metro and regional networks. The OSC-CSM card can be installed in NCS 2006 and NCS 2015 chassis.

The OSC-CSM receives the optical signal and separates the optical service channel from the optical payload. The card is supported only on the Multiservice Transport Platforms (MSTP) package. The optical interfaces of the card support threshold, performance monitoring, and safety parameters. The OSC-CSM can be installed in Slots 2–7 of M6 shelf. The card supports OSC-RX and OSC-TX as internal interfaces.

The OSC-CSM supports the following features:

- Optical combiner and separator module for multiplexing and demultiplexing the optical service channel to or from the wavelength division multiplexing (WDM) signal
- OC-3/STM-1 formatted OSC
- Optical safety: Signal loss detection and alarming, fast transmitted power shut down by an optical 1x1 switch
- Optical safety remote interlock (OSRI), a feature capable of shutting down the optical output power
- Automatic laser shutdown (ALS), a safety mechanism used in the event of a fiber cut.

You can provision OSC only on OC-3/STM-1 UDC at the node configuration level. To manage provisioning of the OSC-CSM card, see Manage OSC.

For more information, such as the block diagrams and the card specifications, see the OSC-CSM card.

Provision Interface Parameters

Use this task to change the optical interface parameters of OSC-CSM cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Interface** tabs.

Step 2 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

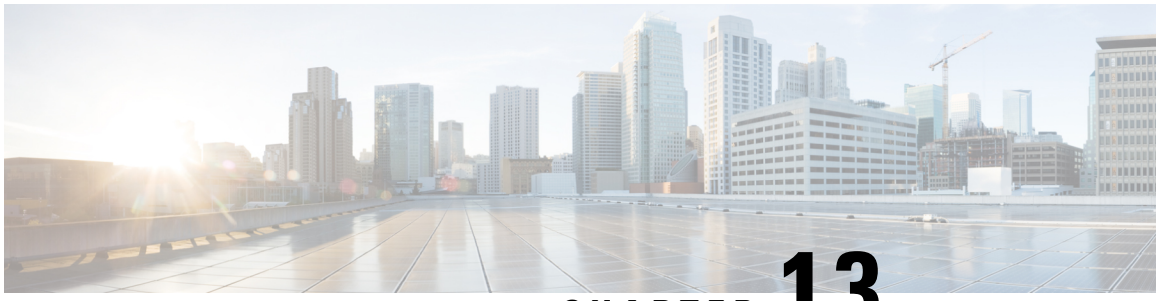
Table 74: Interface Options

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (RX or TX)	All the RX and TX ports

Parameter	Description	Options
Admin State	Sets the administrative state of the port.	From the drop-down list, choose one of the following: • Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ Locked-enabled,maintenance
Optical Power (dBm)	(Display only) Displays the optical power for each port.	—
OSC Power (dBm)	(Display only) Displays the service-channel power level for each port.	—
Optical PSD Setpoint (dBm/GHz)	Target output Power Spectral Density requested by the user.	-50 to 10
Attenuator Value (dB)	Sets the attenuator value.	—
Optical Power Threshold Low (dBm)	Fail low threshold used to detect the LOS alarm on the port.	—
OSC Power Threshold Low (dBm)	(Display only) Displays the OSC power level for each port.	—

Parameter	Description	Options
Current Power Degrade High (dBm)	(Display only) Shows the current value of the optical power degrade high threshold configured in the card. Power Degrade High refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Degrade Low (dBm)	(Display only) Shows the current value of the optical power degrade low threshold configured in the card. Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Failure Low (dBm)	(Display only) Shows the optical power failure low threshold for the port.	—
VOA Attenuation Setpoint (dB)	Sets the VOA attenuation value	0 to 25
VOA Attenuation Offset (dB)	Sets the offset with respect to the set setpoint	—
VOA Current Attenuation (dB)	(Display only) Shows the VOA current attenuation	—

Step 3 Click **Apply** to save the changes.



CHAPTER 13

Provision PSM Cards

This chapter describes the PSM card used in Cisco NCS 2000 SVO and its related tasks.

Table 75: Feature History

Feature Name	Release Information	Feature Description
PSM	Cisco NCS 2000 Release 12.3	The PSM card performs splitter protection functions and supports the standalone protection configuration. The card provides channel protection for the 100G-LC-C, 100G-CK-C, 100GS-CK-LC, 200G-CK-C, and 400G-XP-LC cards. It also provides channel protection for alien wavelengths.

This table lists the package support for the PSM card.

Card	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
PSM	✓	✓

In this chapter, "PSM" refers to the 15454-PSM= card.

PSM Card

The PSM card performs splitter protection functions. In the transmit (TX) section of the PSM card, the signal received on the common receive port is duplicated by a hardware splitter to both the working and protect transmit ports. In the receive (RX) section of the PSM card, a switch is provided to select one of the two input signals (on working and protect receive ports) to be transmitted through the common transmit port.

The PSM card supports the Standalone protection configuration. The card provides channel protection for the 100G-LC-C, 100G-CK-C, 100GS-CK-LC, 200G-CK-C, and 400G-XP-LC cards. It also provides channel protection for alien wavelengths.

The PSM card is a single-slot card that can be installed in any service slot in the NCS 2006 and NCS 2015 chassis. The PSM card includes six LC-PC-II optical connectors on the front panel. In channel protection configuration, the PSM card can be installed in a different shelf from its peer TXP/MXP card.

Key Features

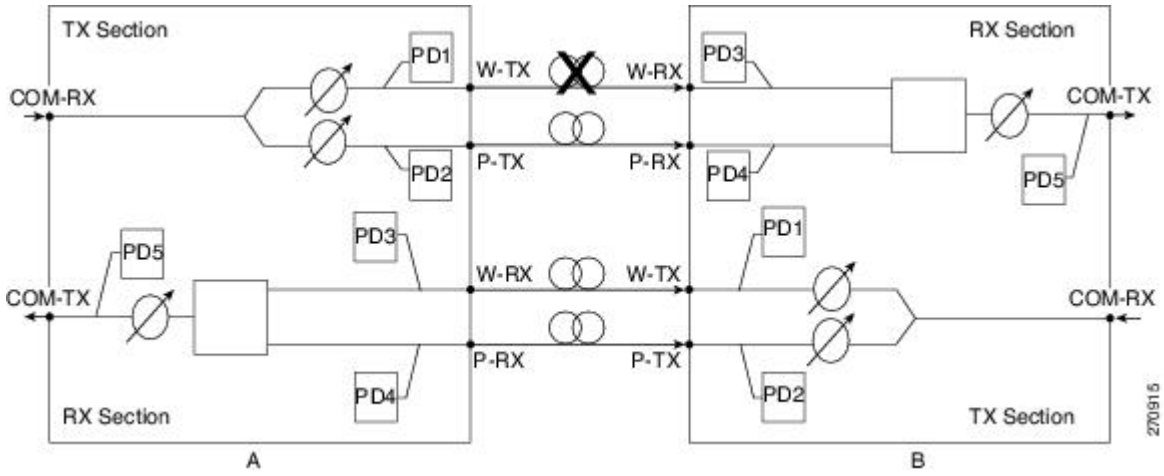
The PSM card provides the following features:

- Operates over the C-band (wavelengths from 1529 nm to 1562.5 nm) and L-band (wavelengths from 1570.5 nm to 1604 nm) of the optical spectrum.
- Implements bidirectional revertive protection scheme.
- Supports automatic creation of a splitter protection group when the PSM card is provisioned.
- Supports switching priorities based on ITU-T G.873.1.
- Supports performance monitoring and alarm handling with settable thresholds.

PSM Bidirectional Switching

A VOA is equipped after the hardware splitter within the PSM card. The VOA implements bidirectional switching when there is a single fiber cut in a protection configuration involving two peer PSM cards. The following figure shows a sample configuration that explains the bidirectional switching capability of the PSM card.

Figure 19: PSM Bidirectional Switching



In this example, there is a fiber cut in the working path from Station A to Station B. As a result of the fiber cut, an LOS alarm is raised on the W-RX port of Station B and it immediately switches traffic on to its P-RX port. Station B simultaneously also stops transmission (for approximately 25 milliseconds) on its W-TX port, which raises an LOS alarm on the W-RX port of Station A. This causes Station A to also switch traffic to its P-RX port. In this way, PSM implements bidirectional switching without any data Exchange between the two stations.

Because the two stations do not communicate using signaling protocols (overhead bytes), a Manual or Force protection switch on the PSM card is implemented by creating a traffic hit. For example, consider that you perform a Manual or Force protection switch on Station A. The TX VOA on the active path is set to automatic VOA shutdown (AVS) state for 25 milliseconds. This causes Station B to switch traffic to the other path because it cannot differentiate between a maintenance operation and a real fail. After 25 milliseconds, the VOA in Station A is automatically reset. Now Station B does not revert back by itself if the non-revertive switching protection scheme is used in the PSM card. However, if the automatic reversion feature on the PSM card is enabled, Station B reverts back to the working path once Wait To Restore (WTR) timer is over.

To effectively implement switching, the Lockout and Force commands must be performed on both the stations. If these commands are not performed on both the stations, the far-end and near-end PSMs can be misaligned. In case of misalignment, when a path recovers, traffic might not recover automatically. You might have to perform a Force protection switch to recover traffic.

Note The order in which you repair the paths is important in the event of a double failure (both the working and protect paths are down due to a fiber cut) on the PSM card in line protection configuration when the active path is the working path. If you repair the working path first, traffic is automatically restored. However, if you repair the protect path first, traffic is not automatically restored. You must perform a Force protection switch to restore traffic on the protect path.

Automatic PSM Reversion

The PSM cards support automatic bidirectional switching. When the fault on the working path clears, traffic automatically switches from the protection path to the working path. The reversion takes place after the Wait To Restore (WTR) timer is over. The key features of automatic PSM reversion are:

- Only normal and standalone modes of PSM card support automatic reversion.
- Protection cannot be provisioned as revertive if automatic laser shutdown (ALS) is enabled in standalone mode, and vice versa.
- Revertive feature is supported for only OCH protection.
- By default, the protection in PSM is non-revertive.
- Reversion parameters that include revertive/non-revertive protection, WTR, pulse width, and interval can be configured only when the working path is active.
- WTR time can be set to a duration between one to 12 minutes and is configurable only if the protection is revertive. By default, the timer is set to five minutes.
- Reversion Pulse Width is between 10 to 200 seconds and is configurable only if the protection is revertive. By default, the duration is set to 60 seconds. This parameter value can be calculated using the following formula:

  Minimum reversion pulse width = ROADM delay + 10 seconds

  ROADM delay = N x 5 x 2

  N=number of filter cards in the network between the source and destination PSM nodes on the working path.

  5 = maximum startup delay in seconds

  2=bidirectional communication

For example, if a network has four ROADM nodes with the end nodes having PSM cards on the working path as depicted below:

[PSM - Node 1 - FILTER 1] ==== [FILTER 2 - Node 2 - FILTER 3] ==== [FILTER 4 - Node 3 - FILTER 5] ==== [FILTER 6 - Node 4 - PSM]

then N = 6

ROADM delay = 6 x 5 x 2= 60

Minimum reversion pulse width = 60 + 10 = 70 seconds

- Recovery Pulse Interval for reversion is auto-calculated and the user cannot configure the thresholds.

Provision the Card Mode on the PSM Card

Use this task to configure the card mode on the PSM card. There are two card modes available.

- PSM-NORMAL—Sets the PSM card in normal configuration. In this configuration, the PSM card supports channel protection, line protection, and multiplex section protection configurations.
- PSM-STANDALONE—Sets the PSM card in standalone configuration. In this configuration, the PSM card can be equipped in any slot and supports all node configurations.

Note In Release 12.3, only the PSM-STANDALONE card mode is supported. A PROV-MISMATCH alarm is raised if the PSM-NORMAL card mode is configured or an upgrade is performed with this operating mode from an earlier release.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Card Mode** tabs.

Step 2 Select the PSM-STANDALONE option from the **Mode** drop-down list.

Step 3 Click **Apply**.

Provision Interface Parameters

Use this task to change the optical interface parameters of cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Interface** tabs.

Step 2 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 76: Interface Options

Parameter	Description	Options
Port	(Display only) Displays the port type and direction (RX or TX)	—
Admin State	Sets the administrative state of the port.	From the drop-down list, choose one of the following: • Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ Locked-enabled,maintenance
Optical Power (dBm)	Displays the optical power for each port.	—
OSC Power (dBm)	NA	—

Parameter	Description	Options
Optical PSD Setpoint (dBm/GHz)	NA	—
Attenuator Value (dB)	Sets the attenuator value.	—
Optical Power Threshold Low (dBm)	Fail low threshold used to detect the LOS alarm on the port.	—
OSC Power Threshold Low (dBm)	NA	—
Current Power Degrade High (dBm)	NA	—
Current Power Degrade Low (dBm)	NA	—
Current Power Failure Low (dBm)	(Display only) Shows the optical power failure low threshold for the port.	—
VOA Attenuation Setpoint (dB)	Sets the VOA attenuation value	0 to 25
VOA Attenuation Offset (dB)	Sets the offset with respect to the set setpoint	—
VOA Current Attenuation (dB)	(Display only) Shows the VOA current attenuation	—

Step 3 Click **Apply** to save the changes.

Provision Optics Thresholds

Use this task to configure the optics thresholds for the card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Optics Thresholds** tabs.

Step 2 Choose the type of threshold that you want to change, 15 Min or 1 Day.

Step 3 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 77: Threshold Options

Parameter	Description	Options
Interface Name	(Display only) Displays the port type and direction (RX or TX)	—
PM Type	(Display only)Type of interface	• oscPowerPMTh • opticalPowerPMTh
Low	Sets the low power warning level.	Numeric. The default is -50 dBm. Double-click the parameter, enter a value, and press Enter.
High	Sets the high power warning level.	Numeric. The default is 30 dBm. Double-click the parameter, enter a value, and press Enter.

Step 4 Click **Apply** to save the changes.

Note Click **Reset** to reset the default settings.

Provision Optical Safety

Use this task to provision the optical safety parameters for cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Optical Safety** tabs.

Step 2 Modify required settings described in the following table:

Table 78: Optical Safety Parameters for Cards

Parameter	Description	Options
Interface	(Display only) Displays the port name, port type, and direction.	—

Parameter	Description	Options
Supported Safety	(Display only) Displays the supported safety mechanism.	• ALS for line cards and control cards. • ALS-OSRI for amplifier cards.
ALS Mode	Automatic laser shutdown mode. The ALS mode is disabled for RX ALS interfaces.	From the drop-down list, choose one of the following: • ALS-Disabled—Deactivates ALS. • Automatic Restart—(Default) ALS is active. The power is automatically shut down when needed, and it automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart
OSRI	Optical safety remote interlock. The default value is OSRI-OFF. When set to OSRI-ON, the TX output power is shut down. **Note** OSRI configuration is not supported on the transponder and muxponder cards.	From the drop-down list, choose one of the following: • OSRI-OFF • OSRI-ON
ALS Status	(Display only) ALS status of the device.	• Working • Shutdown
Recovery Pulse Interval	Displays the interval between two optical power pulses.	60 to 300 seconds.
Recovery Pulse Duration	Displays the duration of the optical power pulse that begins when an amplifier restarts.	2 to 100 seconds
Manual Restart	Triggers manual restart action for the ALS interface. However, manual restart does not happen if Mode is set to Automatic Restart or Disabled.	—

Step 3 Click **Apply** to save the changes.

View Insertion Loss Parameters

Use this task to view the insertion loss parameters of cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Click the **Maintenance** > **Insertion Loss** tabs to view the insertion loss parameters.

The Insertion Loss tab displays the following information:

- **Insertion Loss Path**—Displays the insertion loss path.
- **IL Value (dB)**—Displays the insertion loss value.

Note When the card is removed, the last retrieved Insertion Loss values are displayed in the SVO web UI. When the card is replaced, the Insertion Loss values are updated in the SVO web UI.

Manage the Protection Group

Use this task to view the protection group that is automatically created when a new PSM card is provisioned. You can also perform a switch operation on the interfaces.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Protection** tabs to view the parameters of the PSM protection group.

The Protection tab displays the following information:

- **Name**—Name of the protection group
- **Protection Type**—The protection type is splitter

- **Active Interfaces**—The interfaces on which the traffic is present
- **Working Interfaces**—The working interfaces are the active interfaces when the protection group is created.
- **Protection Interfaces**—The protection interfaces when the protection group is created.
- **Switch Type**—The switch type is bidirectional-switching.
- **Revertive**—If set to true, the traffic reverts to the working port after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- **Reversion Time (min)**—Reversion time is the amount of time that will elapse before the traffic reverts to the working card. The reversion timer starts after conditions causing the switch are cleared. The range is from one to 12 minutes.
- **Reversion Pulse Width (sec)**—Reversion Pulse Width is between 10 to 200 seconds and is configurable only if the protection is revertive. By default, the duration is set to 60 seconds.

Note The following fields in the protection group are editable in the Chassis view > Provisioning tab:

- Name
- Revertive
- Reversion Time
- Reversion Pulse Width

Step 2 Click + to view the protection group data.

The interfaces of the protection group are displayed.

- **Interface**—displays the name of the interface
- **Entity**—Displays the entity of the interface, whether it is working or protect
- **Entity Status**—Displays the status of the entity, whether it is active or Standby
- **Switch Status**—Displays the switch status when a switch operation is performed.

Step 3 To perform a switch operation between the interfaces of a protection group, perform these steps:

Note A switch operation can only be performed if revertive is set to false.

a. Check the check box corresponding to the interface you want to perform a switch operation.

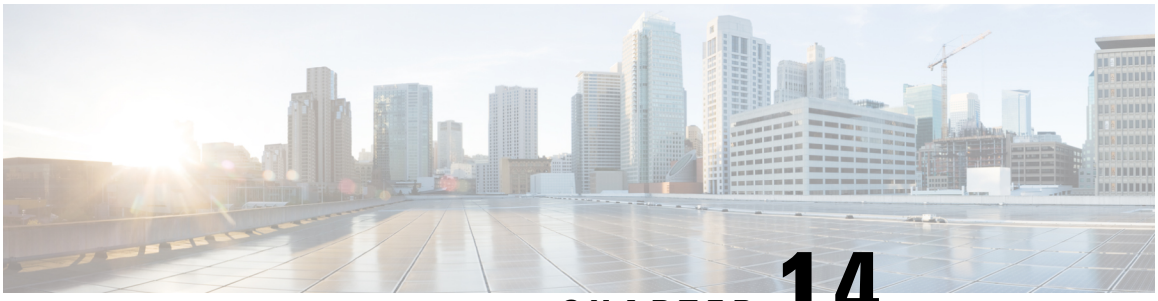
b. Click **Edit**.

The Switch Command dialog box appears.

c. Select an option from the **Action** drop-down list.

The options available are—Lock-Out, Force-Switch, Manual-Switch, and Release.

d. Click **Apply**.



CHAPTER 14

Provisioning Optical Amplifier Cards

This chapter describes the optical amplifier cards used in Cisco NCS 2000 SVO and its related tasks.

Table 79: Feature History

Feature Name	Release Information	Feature Description
OPT-AMP-17-C and OPT-BST-E Cards	Cisco NCS 2000 Release 12.3	The OPT-AMP-17-C card can be used as a preamplifier or as a booster amplifier, providing a total output power of 17 dBm. It integrates an optical service channel splitter and combiner to allow the OSC to be sent to and received from the OSCM card. It employs a single-stage amplifier design to optimize the noise figure and operates with a fixed gain of 17 dB. The OPT-BST-E card amplifies the outgoing composite DWDM signal to overcome the attenuation of the fiber network, providing a total output power of 20 dBm. It integrates an optical service channel splitter and combiner to allow the OSC to be sent to and received from the OSC-CSM card and/or the OSC derived from the control cards.

Feature Name	Release Information	Feature Description
OPT-PRE and OPT-BST Cards	Cisco NCS 2000 Release 12.2	The OPT-PRE card amplifies the incoming composite DWDM signal to allow sufficient optical power level to optical receivers on dropped wavelengths. It overcomes the insertion losses of the reconfigurable or fixed optical filters in the node. The OPT-BST card amplifies the outgoing composite DWDM signal to overcome the attenuation of the fiber network, providing a total output power of 17 dBm. It integrates an optical service channel splitter and combiner to allow the OSC to be sent to and received from the OSC-CSM card. Both the cards can be installed in NCS 2006 and NCS 2015 chassis.

The following table lists the package support for the optical amplifier cards.

Card	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
OPT-AMP-C	✓	✓
OPT-AMP-17C		✓
OPT-PRE		✓
OPT-BST		✓
OPT-BST-E		✓
OPT-EDFA-17	✓	✓
OPT-EDFA-24	✓	✓
OPT-EDFA-35	✓	
RAMAN-CTP	✓	✓
RAMAN-COP	✓	
RMN-CTP-CL	✓	
EDRA-1-xx	✓	
EDRA-2-xx	✓	

OPT-AMP-C Card

In this chapter, "OPT-AMP-C" refers to the _15454-OPT-AMP-C card.

The OPT-AMP-C card is a 20-dB output power, C-band, DWDM EDFA amplifier or preamplifier. It contains midstage access loss for a Dispersion Compensation Unit (DCU). A Variable Optical Attenuator (VOA) is used to control gain tilt. The VOA can also be used to attenuate the signal of the DCU to a reference value. The amplifier module also includes the OSC add (TX direction) and drop (RX direction) optical filters.

The features of the card include:

- Fast transient suppression
- Nondistorting low-frequency transfer function
- Mid-stage access for DCU
- Constant pump current mode (test mode)
- Fixed output power mode
- Constant gain mode
- Amplified spontaneous emissions (ASE) compensation in Constant Gain and Constant Output Power modes
- Programmable tilt
- Full monitoring and alarm handling capability
- Gain range with gain tilt control of 12–24 dB

- Extended gain range (with uncontrolled tilt) of 24–35 dB
- Full monitoring and alarm handling with settable thresholds
- Optical Safety Remote Interlock (OSRI)—Shuts down optical output power or reduces the power to a safe level
- Automatic laser shutdown (ALS)—Safety mechanism used in case of fiber cut

You can install the OPT-AMP-C card in the following slots:

- Slots 2–7 in NCS 2006

For more information about the OPT-AMP-C card, see http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/prod_data_sheet0900aecd8072b322.html. and Card Features.

OPT-AMP-17-C Card

In this chapter, "OPT-AMP-17-C" refers to the _15454-OPT-AMP-17-C card.

The OPT-AMP-17-C is a 17-dB gain, C-band, DWDM EDFA amplifier or preamplifier with OSC add-and-drop capability. It supports 80 channels at 50-GHz channel spacing in the C-band (that is, the 1529 to 1562.5 nm wavelength range). When the system has an OPT-AMP-17-C card that is installed, an OSCM card and/or OSC derived from the controller card is needed to process the OSC.

The features of the card include:

- Fixed gain mode (no programmable tilt)
- Standard gain range of 14–20 dB at startup when configured as a preamplifier
- Standard gain range of 20–23 dB in transient mode when configured as a preamplifier
- Gain range of 14–23 dB (with no transient gain range) when configured as a booster amplifier
- True variable gain
- Fast transient suppression
- Nondistorting low-frequency transfer function
- Settable maximum output power
- Fixed output power mode
- Amplified spontaneous emissions (ASE) compensation in fixed gain mode
- Full monitoring and alarm handling with settable thresholds
- Optical Safety Remote Interlock (OSRI)—Shuts down optical output power or reduces the power to a safe level
- Automatic laser shutdown (ALS)—Safety mechanism used in case of fiber cut

You can install the OPT-AMP-17-C card in the following slots.

- Slots 2–7 in NCS 2006

- Slots 2–16 in NCS 2015

For more information about the OPT-AMP-17-C card, see https://www.cisco.com/c/en/us/products/collateral/optical-networking/ons-15454-series-multiservice-provisioning-platforms/prod_data_sheet0900aecd8072b322.html and Card Features.

OPT-PRE Card

In this chapter, "OPT-PRE" refers to the _15454-OPT-PRE card.

The OPT-PRE is a C-band, DWDM, two-stage erbium-doped fiber amplifier (EDFA) with midamplifier loss (MAL). This card can be connected to a dispersion compensating unit (DCU). The OPT-PRE is equipped with a built-in Variable Optical Attenuator (VOA) that controls the gain tilt and attenuates the signal of the DCU to a reference value. The card is designed to support up to 80 channels at 50-GHz channel spacing.

The features of the card include:

- Fixed gain mode with programmable tilt
- True variable gain
- Fast transient suppression
- Nondistorting low-frequency transfer
- Settable maximum output power
- Fixed output power mode
- MAL for fiber-based DCU
- Amplified spontaneous emissions (ASE) compensation in fixed gain mode
- Full monitoring and alarm handling with settable thresholds
- An optical output port for external monitoring

Note The optical splitter has a ratio of 1:99, resulting in about 20-dB lower power at the MON port than at the COM TX port.

You can install the OPT-PRE card in the following slots.

- Slots 2 and 3 in NCS 2002
- Slots 2–7 in NCS 2006
- Slots 2–16 in NCS 2015

For more information about the OPT-PRE card, see https://www.cisco.com/c/en/us/products/collateral/optical-networking/ons-15454-series-multiservice-provisioning-platforms/prod_data_sheet0900aecd8072b322.html and Card Features.

OPT-BST and OPT-BST-E Cards

In this chapter, "OPT-BST" refers to the _15454-OPT-BST card and "OPT-BST-E" refers to the _15454-OPT-BST-E card.

The OPT-BST is designed to support up to 80 channels at 50-GHz channel spacing. The OPT-BST-E amplifier card is a gain-enhanced version of the OPT-BST card. It is designed to support up to 80 channels at 50-GHz channel spacing.The cards are C-band, DWDM EDFA with optical service channel (OSC) add-and-drop capability.

The features of the cards include:

- Fixed gain mode (with programmable tilt)
- Gain range of 5–20 dB in constant gain mode and output power mode
- The standard gain range with tilt control is 8–23dB. The extended gain range without tilt control is 23–26 dB.
- True variable gain
- Built-in VOA to control gain tilt
- Fast transient suppression
- Nondistorting low-frequency transfer function
- Settable maximum output power
- Fixed output power mode
- ASE compensation in fixed gain mode
- Full monitoring and alarm handling with settable thresholds
- Optical Safety Remote Interlock (OSRI)—Shuts down optical output power or reduces the power to a safe level
- Automatic laser shutdown (ALS)—Safety mechanism used in case of fiber cut

Note Each optical splitter has a ratio of 1:99. The result is that MON TX and MON RX port power is about 20 dB lower than COM TX and COM RX port power.

You can install the cards in the following slots:

- Slots 2–7 in NCS 2006
- Slots 2–16 in NCS 2015

For more information about the cards, see https://www.cisco.com/c/en/us/products/collateral/optical-networking/ons-15454-series-multiservice-provisioning-platforms/prod_data_sheet0900aecd8072b322.html .

OPT-EDFA-17, OPT-EDFA-24, and OPT-EDFA-35 Cards

In this chapter, "OPT-EDFA-17" refers to the _15454-OPT-EDFA-17 card. "OPT-EDFA-24" refers to the _15454-OPT-EDFA-24 card. "OPT-EDFA-35" refers to the NCS2K-OPT-EDFA-35 card.

The OPT-EDFA-17, OPT-EDFA-24, and OPT-EDFA-35 cards are C-band DWDM EDFA amplifiers and preamplifiers. The cards are true variable gain amplifiers, offering an optimal equalization of the transmitted optical channels over a wide gain range. They support 96 channels at 50-GHz channel spacing in the C-band (that is, 1528.77 to 1566.72-nm wavelength range). The OPT-EDFA-17 and OPT-EDFA-24 cards deliver 20-dBm output powers and the OPT-EDFA-35 card delivers +23-dBm output power. These cards do not contain mid-stage access loss for a Dispersion Compensation Unit (DCU). The cards provide a noise-figure optimized version of the EDFA amplifiers to cope with new modulation formats like PM-DQPSK, which do not need dispersion compensation. To control gain tilt, a VOA is used. The amplifier module also includes the OSC add (TX direction) and drop (RX direction) optical filters.

The OPT-EDFA-17, and OPT-EDFA-24 cards share the same hardware platform and firmware architecture, but they differ in their operative optical gain range, which is 17 and 24 dB respectively.

The OPT-EDFA-35 card includes two identical amplification sections to serve two fiber directions simultaneously. Each section has a switchable gain range that allows its usage over a wide gain range. The OPT-EDFA-35 card is bidirectional. The card acts on both pairs of fibers entering and exiting from the node.

The OPT-EDFA-35 card has two possible gain ranges: gain range 1 from 12–24, gain range 2 from 20–35. The card also has extended gain range up to 40 dB without tilt control.

The OPT-EDFA-35 card is managed in a similar way as the OPT-EDFA-17 and OPT-EDFA-24 cards. For each EDFA unit inside the OPT-EDFA-35 card, the following settings are allowed:

- Configuration of PRE or BST role
- Configuration of Constant Gain working mode
- Configuration of Gain Range

The main functionalities of the OPT-EDFA-17, OPT-EDFA-24, and OPT-EDFA-35 cards are:

- (OPT-EDFA-17 and OPT-EDFA-24) Amplification of the input signal at the COM-RX port toward the LINE-TX port through a true-variable gain EDFA block.

  (OPT-EDFA-35) Two EDFA amplifier units embedded into the card, amplification of the input signal at the LINE-1-RX port toward the LINE-2-TX port through a true-variable gain EDFA-2 block, and amplification of the input signal at the LINE-2-RX port toward the LINE-1-TX port through a true-variable gain EDFA-1 block.
- Multiplexing the OSC to the LINE-TX port
- Demultiplexing the OSC from the LINE-RX port
- Monitoring of the LINE input or output signal with 1% TAP splitters

The features of the OPT-EDFA-17, OPT-EDFA-24, and OPT-EDFA-35 cards are:

- Embedded Gain Flattening Filter
- Constant pump current mode (test mode)
- Constant output power mode

- Constant gain mode
- Nondistorting low-frequency transfer function
- ASE compensation in Constant Gain and Constant Output Power modes
- Fast transient suppression
- Programmable tilt
- Full monitoring and alarm handling capability
- Gain range with gain tilt control of 5–17 dB (for OPT-EDFA-17 card) , 12 to 24 dB and 20 to 35 dB (for OPT-EDFA-35 card), and 12–24 dB (for OPT-EDFA-24 card).
- Extended gain range (with uncontrolled tilt) of 17–20 dB (for OPT-EDFA-17 card) , (for OPT-EDFA-35 card) of upto 27dB (for Gain Range1) and 40dB (for Gain Range2), and 24–27 dB (for OPT-EDFA-24 card).
- Optical Safety Remote Interlock (OSRI)
- Automatic Laser Shutdown (ALS)

You can install the OPT-EDFA-17, OPT-EDFA-24, and OPT-EDFA-35 cards in the following slots:

- Slots 2–7 in NCS 2006
- Slots 2–16 in NCS 2015

For more information about the OPT-EDFA-17, OPT-EDFA-24, and OPT-EDFA-35 cards, see the data sheet.

Power Monitoring of OPT-EDFA-17, OPT-EDFA-24, and OPT-EDFA-35 Cards

Physical photodiodes PD1 through PD6 monitor the power for the OPT-EDFA-17 and OPT-EDFA-24 cards.

Table 80: Port Calibration of OPT-EDFA-17 and OPT-EDFA-24 Cards

Photodiode	Calibrated to Port
PD1	COM-RX
PD2	LINE-TX
PD3	LINE-TX
PD4	OSC-RX
PD5	LINE-RX
PD6	LINE-RX

Physical photodiodes PD1 through PD8 monitor the power for the OPT-EDFA-35 card.

Table 81: Port Calibration of OPT-EDFA-35 Card

Photodiode	Calibrated to Port
PD1	LINE-2-RX
PD2	LINE-1-TX
PD3	LINE-1-RX
PD4	LINE-2-TX
PD5	OSC-2-RX
PD6	OSC-2-TX
PD7	OSC-1-TX
PD8	OSC-1-RX

Installing the Amplifier Card

Use this task to install the amplifier cards on the chassis.

Procedure

Step 1 Remove a DWDM card from its packaging, then remove the protective caps from the backplane connectors. (Safety caps are typically yellow.)

Step 2 Align the amplifier card so the markings on the card and the chassis are on the same side.

Step 3 Open the latches or ejectors of the first card that you will install.

Step 4 Use the latches or ejectors to firmly slide the card horizontally along the guide rails until the card plugs into the receptacle at the back of the slot. (slot 2 to 7 in the NCS 2006 shelf or slot 2 to 16 in the NCS 2015 shelf.)

Note The card slides vertically in NCS 2015 shelf.

The card slides horizontally in NCS 2006.

Step 5 Verify that the card is inserted correctly, and close the latches or ejectors on the card.

RAMAN-CTP and RAMAN-COP Cards

In this chapter, "RAMAN-CTP" refers to the 15454-M-RAMAN-CTP card and "RAMAN-COP" refers to the 15454-M-RAMAN-COP card.

The single-slot RAMAN-CTP and RAMAN-COP cards support counter and co-propagating Raman amplification on long unregenerated spans.

The cards manage up to 96 ITU-T 50 GHz spaced channels over the C-band of the optical spectrum (wavelengths from 1528.77 to 1566.72 nm). The counter-propagating RAMAN-CTP card is the primary unit.

The co-propagating RAMAN-COP card is the secondary unit and can be used only when the counter-propagating unit is present. The OSC pluggable used with the cards is ONS-SC-OSC-18.0=.

The RAMAN-CTP card can be calibrated either manually or automatically from the **Maintenance** tab in the SVO web interface. When the RAMAN-COP card is used, the RAMAN-CTP card can be calibrated only using the manual option.

The features of the RAMAN-CTP and RAMAN-COP cards include:

- Raman section: 1000-mW total pump power for four pumps and two wavelengths.
- Embedded distributed feedback (DFB) laser at 1568.77 nm to be used for optical safety and link continuity (in RAMAN-CTP card only).
- Photodiodes to enable monitoring of Raman pump power.
- Photodiodes to enable monitoring of the DFB laser and signal power (in RAMAN-CTP card only).
- Automatic laser shutdown (ALS) for optical laser safety.
- Hardware output signals for loss of signal (LOS) monitoring at input photodiodes.
- Raman pump back reflection detector to check for excessive back reflection.

When the node has either RAMAN-CTP or RAMAN-COP card, you can install the card in the following slots.

- Slots 2–7 in NCS 2006
- Slots 2–16 in NCS 2015

When the node has both RAMAN-CTP or RAMAN-COP cards, you can install the cards in the following slots.

- If the RAMAN-CTP card is installed in an even slot, the RAMAN-COP card must be installed in the next odd slot.
- If the RAMAN-COP is installed in an even slot, the RAMAN-CTP card must be installed in the next odd slot.

RAMAN-CTP and RAMAN-COP Cards Power Monitoring

Physical photodiodes P1 through P10 monitor the power for the RAMAN-CTP card.

Table 82: RAMAN-CTP Port Calibration

Photodiode	Type Name	Calibrated to Port
P1	DFB in-fiber Output Power	LINE-TX
P2	DWDM RX Input Power	LINE-RX
P3	Pump 1 in-fiber Output Power	LINE-RX
P4	Pump 2 in-fiber Output Power	LINE-RX
P5	Total Pump in-fiber Output Power	LINE-RX

Photodiode	Type Name	Calibrated to Port
P6	Back-Reflected Pump Power	LINE-RX
P7	DWDM TX Input Power	COM-RX
P8	Total Co-Pump in-fiber Output Power	LINE-TX
P9	DFB Input Power	LINE-RX
P10	ASE Input Power	LINE-RX

Physical photodiodes P3 through P6 monitor the power for the RAMAN-COP card.

Table 83: RAMAN-CTP Port Calibration

Photodiode	Type Name	Calibrated to Port
P3	Pump 1 in-fiber Output Power	RAMAN-TX
P4	Pump 2 in-fiber Output Power	RAMAN-TX
P5	Total Pump in-fiber Output Power	RAMAN-TX
P6	Back-Reflected Pump Power	RAMAN-TX

For more information about the RAMAN-CTP and RAMAN-COP cards, see the data sheet.

RMN-CTP-CL Card

Table 84: Feature History

Feature Name	Release Information	Feature Description
RMN-CTP-CL Card	Cisco NCS 2000 Release 12.3	The RMN-CTP-CL card is a RAMAN amplifier card that provides optical amplification of the wavelengths by counter-propagating Raman pumping. The card operates for both C and L bands of the optical spectrum. The card occupies one slot in NCS 2006 and NCS 2015 chassis.

In this chapter, "RMN-CTP-CL" refers to the NCS2K-RMN-CTP-CL card.

The RMN-CTP-CL card provides optical amplification of the wavelengths by counter-propagating Raman pumping. The card operates for both C and L bands of the optical spectrum.

The RMN-CTP-CL card can be installed in any service slot in the Cisco NCS 2006 and NCS 2015 chassis. The RMN-CTP-CL card works on a node that is installed with the flex package.

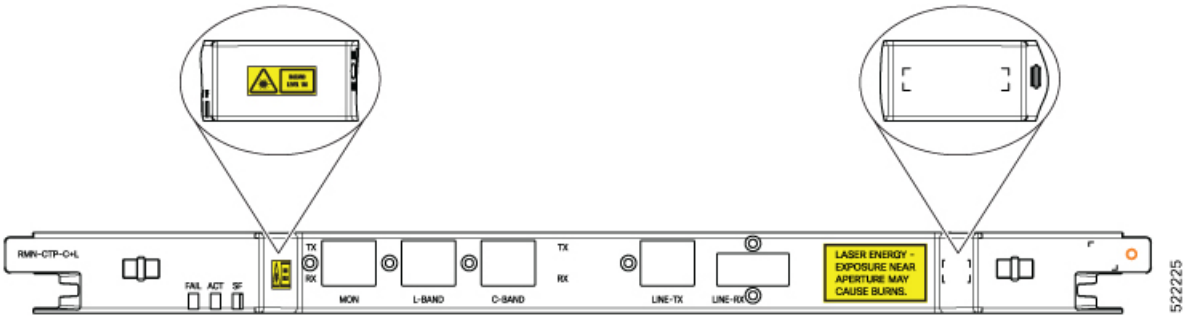
Key Features

The RMN-CTP-CL card provides the following key features:

- 1.2W total power with five Raman pump wavelengths to support Raman amplification over the C-band and L-band wavelength range.
- Multiplexer and demultiplexer section to combine and split the C-band and L-band wavelength range.
- Embedded laser at 1568.77 nm used for optical safety and link continuity.
- Photodiodes to enable monitoring of Raman pump power, embedded laser, and signal power.
- Raman pump back reflection detector to check for excessive back reflection.
- Automatic laser shutdown (ALS) for optical laser safety.
- Automated turn up of the card with automatic tuning of the pump wavelengths to ensure optimal amplification performance.

Faceplate Diagram

Figure 20: Faceplate Diagram of RMN-CTP-CL Card



Connector Assignment

The RMN-CTP-CL card uses LC connectors for all the ports except the LINE-RX port.

Table 85: Connector Assignment

Optical Connector Label	Optical Connector Type	Port Name
LINE	LC - UPC	LINE-TX
	E2000 – PS - PC	LINE-RX
C-BAND	LC - UPC	C-BAND-TX
	LC - UPC	C-BAND-RX
L-BAND	LC - UPC	L-BAND-TX
	LC - UPC	L-BAND-RX

Optical Connector Label	Optical Connector Type	Port Name
MON	LC - UPC	MON-TX
	LC - UPC	MON-RX

For more information about the RMN-CTP-CL card, such as the block diagram and card specifications, see the data sheet.

EDRA-1-xx and EDRA-2-xx Cards

In this chapter, "EDRA-1-xx" refers to the NCS2K-EDRA1-26C and NCS2K-EDRA1-35C cards.

"EDRA-2-xx" refers to the NCS2K-EDRA2-26C and NCS2K-EDRA2-35C cards.

The double-slot EDRA-1-xx and EDRA-2-xx cards combine standard erbium-doped fiber amplifiers and a Raman amplifier to enable amplification on long unregenerated spans.

The cards manage up to 96 ITU-T 50 GHz spaced channels over the C-band of the optical spectrum (wavelengths from 1528.77 to 1566.72 nm). You can install the EDRA-1-xx and EDRA-2-xx cards in the lowest slots to allow high output power. The power output is limited to 21 dBm when the cards are inserted in any other slot. The OSC pluggable used with the cards is ONS-SC-OSC-18.0=.

The cards can be used in point-to-point, ring, multi-ring, or mesh topologies and are supported on flexible nodes in line amplifier node configurations.

Apart from these node configurations having only EDRA cards as amplifiers, the system also supports hybrid configurations with OPT-EDFA-17, OPT-EDFA-24, RAMAN-CTP, and RAMAN-COP cards. These cards support span loss and gain values that are not supported in EDRA cards.

- For gain less than 15 dB, OPT-EDFA-17 or OPT-EDFA-24 must be used.
- For gain greater than 35 dB, RAMAN-CTP, RAMAN-COP, OPT-EDFA-17 or OPT-EDFA-24 must be used.

You can install the EDRA-1-xx and EDRA-2-xx cards in the following slots.

- Slots 2–6 in NCS 2006
- Slots 2–15 in NCS 2015

EDRA-1-xx and EDRA-2-xx Cards Power Monitoring

The following table lists the physical photodiodes that monitor the power for the EDRA-1-xx and EDRA-2-xx cards.

Table 86: EDRA-1-xx and EDRA-2-xx Port Calibration

Photodiode	CTC Type Name	Calibrated to Port
PD1	Remnant Pump Input power	LINE-TX
PD2	OSC Add Input Power	OSC-RX

Photodiode	CTC Type Name	Calibrated to Port
PD3	EDFA1 Input Power	LINE-RX
PD4	EDFA1 Output Power	COM-TX
PD5	EDFA2 Input Power	COM-RX
PD6	EDFA2/LINE-TX Output Power	LINE-TX
PD7	OSC Drop Output Power	LINE-TX
PD11	Pump λ1 in-fibre Output Power	LINE-RX
PD12	Pump λ2 in-fibre Output Power	LINE-RX
PD13	Pump λ3 in-fibre Output Power	LINE-RX
PD14	Pump λ4 in-fibre Output Power	LINE-RX
PD15	Total Pump in-fibre Output Power	LINE-RX
PD16	Back-Reflected Pump Power	LINE-RX
PD17	OTDR2-L Input Power	OTDR2-L-RX

Provision Amplifier Parameters

Use this task to provision the optical amplifier parameters for OPT-AMP-C, OPT-AMP-17-C, OPT-PRE, OPT-BST, OPT-BST-E, OPT-EDFA-17, OPT-EDFA-24, OPT-EDFA-35, EDRA1-xx, and EDRA2-xx cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Amplifier** tabs.

Step 2 Modify any of the settings described in the following table.

Table 87: Amplifier Parameters for Amplifier Cards

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (TX or RX).	—

Parameter	Description	Options
Total Output Power (dBm)	(Display only) Shows the current power level for each port.	—
Output Power Setpoint (dBm)	Shows the output power setpoint.	—
Working Mode	Shows the working mode.	• Channel Power • Total Power • Optimized • Fixed Gain • Start and Hold
Role	Role of the amplifier.	• Preamplifier • Booster
Actual Gain (dB)	Actual gain setpoint.	—
Target Gain (dB)	Target gain setpoint.	—
Tilt Setpoint (dB)	Target output tilt requested by the user.	—
PSD Setpoint (dBm/GHz)	Power Spectral Density. Target output power requested by the user for each circuit.	—
PSD Optimized (dBm/GHz)	Optimized PSD	—
Gain Setpoint (dB)	Target amplifier gain requested by the user.	—
Gain Range	Sets the gain range of the amplifier.	• Gain Range 1 • Gain Range 2 • No Gain Range
Power Degrade Threshold (High) (dBm/GHz)	Shows the current value of the optical power degrade high threshold.	—
Power Degrade Threshold (Low) (dBm/GHz)	Shows the current value of the optical power degrade low threshold.	—
Status	Shows the current status of the amplifier.	—

Parameter	Description	Options
Gain Degrade High (dB)	(Display only) Shows the current value of the gain degrade high threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode. Gain Degrade High refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up.	—
Gain Degrade Low (dB)	(Display only) Shows the current value of the gain degrade low threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode. Gain Degrade Low refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up.	—

Step 3 Click **Apply** to save the changes.

Provision Raman Amplifier Parameters

Use this task to provision the optical Raman amplifier parameters for the RAMAN-CTP, RAMAN-COP, RMN-CTP-CL, EDRA1-xx, and EDRA2-xx cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Raman Amplifier** tabs.

Step 2 Modify any of the settings described in the following table.

Table 88: Raman Amplifier Parameters for Amplifier Cards

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (TX or RX).	—
Name		
Gain Setpoint (dB)	Target amplifier gain requested by the user.	—
Tilt Setpoint (dB)	Target output tilt requested by the user.	—
Actual Gain (dB)	(Display only) Displays the actual amplifier gain.	—
Actual Tilt (dB)	(Display only) Displays the actual amplifier tilt	—
Pumping Scheme	(Display only) Displays the pumping scheme that the card uses.	• Counter-Propagating for the RAMAN-CTP, RMN-CTP-CL, EDRA-1-xx, and EDRA-2-xx cards. • Co-Propagating for the RAMAN-COP card.
Calibration Type	Calibration type that the card uses. The RAMAN-COP card supports only manual calibration. The RAMAN-CTP card supports both automatic and manual calibration. The RMN-CTP-CL card supports only automatic calibration. If a node has both RAMAN-CTP and RAMAN-COP cards, the RAMAN-CTP card supports only manual calibration.	• Automatic • Manual • No-Calibration
Unsaturated Gain Setpoint (dBm)	Unsaturated target amplifier gain. This field is editable only for the RAMAN-COP card.	0–50

Step 3 Click **Apply** to save the changes.

Step 4 Expand the RAMAN port to view the pump power details.

Table 89: RAMAN Pump Power Parameters

Parameter	Description
Pump ID	(Display only) Identifier of the Raman Pump (2 pumps with RAMAN-CTP and 4 pumps with EDRA).
Pump Power Setpoint (mW)	(Only for RAMAN-CTP and RAMAN-COP cards) Provisioned value of pump power setpoint. This value is effective only for manual calibration of RAMAN-CTP and RAMAN-COP cards and if the calibration is not performed. The value of this parameter must also be provided for automatic calibration of the RAMAN-CTP card even if the value is not effective.
Pump Power Target (mW)	(Display only) Target power set by the internal control algorithm. The result of calibration can be both automatic and manual.
Pump Power (mW)	(Display only) Actual power value of the individual pump.

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

Provision Interface Parameters

Use this task to change the optical interface parameters of OPT-AMP-C, OPT-AMP-17-C, OPT-PRE, OPT-BST, OPT-BST-E, OPT-EDFA-17, OPT-EDFA-24, OPT-EDFA-35, RAMAN-CTP, RMN-CTP-CL, EDRA1-xx, and EDRA2-xx cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Interface** tabs.

Step 2 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 90: Interface Options

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (RX or TX)	All the RX and TX ports
Admin State	Sets the administrative state of the port.	From the drop-down list, choose one of the following: • Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ Locked-enabled,maintenance
Optical Power (dBm)	(Display only) Displays the optical power for each port.	—
OSC Power (dBm)	(Display only) Displays the service-channel power level for each port.	—
Optical PSD Setpoint (dBm/GHz)	Target output Power Spectral Density requested by the user.	-50 to 10
Attenuator Value (dB)	Sets the attenuator value.	—
Optical Power Threshold Low (dBm)	Fail low threshold used to detect the LOS alarm on the port.	—
OSC Power Threshold Low (dBm)	(Display only) Displays the OSC power level for each port.	—

Parameter	Description	Options
Current Power Degrade High (dBm)	(Display only) Shows the current value of the optical power degrade high threshold configured in the card. Power Degrade High refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Degrade Low (dBm)	(Display only) Shows the current value of the optical power degrade low threshold configured in the card. Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Failure Low (dBm)	(Display only) Shows the optical power failure low threshold for the port.	—

Step 3 Click **Apply** to save the changes.

Manage Raman Interface Parameters

Use this task to manage the Raman interface parameters of RAMAN-CTP, RAMAN-COP, RMN-CTP-CL, EDRA1-xx, and EDRA2-xx cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Raman Interface** tabs.

Step 2 View the settings described in the following table. Only the Admin State parameter can be modified.

Table 91: Interface Options

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (RX or TX)	All the RX and TX ports
Admin State	Sets the administrative state of the port.	From the drop-down list, choose one of the following: • Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ Locked-enabled,maintenance
Optical Power (mW)	(Display only) Displays the optical power for each port.	—
Current Optical Power Setpoint (mW)	(Display only) Shows the current value of the optical power setpoint that must be reached.	—
Current Power Degrade High (mW)	(Display only) Shows that the current value of the optical power degrade high threshold. Power Degrade High refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—

Parameter	Description	Options
Current Power Degrade Low (mW)	(Display only) Shows that the current value of the optical power degrade high threshold configured in the card. Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Failure Low (mW)	(Display only) Shows the optical power failure low threshold for the port.	—

Step 3 Click **Apply** to save the changes.

Provision Thresholds for TCA alarms

Use this task to change the thresholds for TCA alarms raised on cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Optics Thresholds** tabs.

Step 2 Choose the type of threshold that you want to change, 15 Min or 1 Day.

Step 3 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 92: Threshold Options

Parameter	Description	Options
Interface Name	(Display only) Displays the port number, port type, and direction (RX or TX)	All the TX and RX ports
PM Type	Type of interface	• oscPowerPMTh • opticalPowerPMTh

Parameter	Description	Options
Low	Sets the low power warning level.	Numeric. The default is -50 dBm. Double-click the parameter, enter a value, and press Enter.
High	Sets the high power warning level.	Numeric. The default is 30 dBm. Double-click the parameter, enter a value, and press Enter.

Step 4 Click **Apply** to save the changes.

Provision Optical Safety

Use this task to provision the optical safety parameters for cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Optical Safety** tabs.

Step 2 Modify required settings described in the following table:

Table 93: Optical Safety Parameters for Cards

Parameter	Description	Options
Interface	(Display only) Displays the port name, port type, and direction.	—
Supported Safety	(Display only) Displays the supported safety mechanism.	• ALS for line cards and control cards. • ALS-OSRI for amplifier cards.

Parameter	Description	Options
ALS Mode	Automatic laser shutdown mode. The ALS mode is disabled for RX ALS interfaces.	From the drop-down list, choose one of the following: • ALS-Disabled—Deactivates ALS. • Automatic Restart—(Default) ALS is active. The power is automatically shut down when needed, and it automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart
OSRI	Optical safety remote interlock. The default value is OSRI-OFF. When set to OSRI-ON, the TX output power is shut down. **Note** OSRI configuration is not supported on the transponder and muxponder cards.	From the drop-down list, choose one of the following: • OSRI-OFF • OSRI-ON
ALS Status	(Display only) ALS status of the device.	• Working • Shutdown
Recovery Pulse Interval	Displays the interval between two optical power pulses.	60 to 300 seconds.
Recovery Pulse Duration	Displays the duration of the optical power pulse that begins when an amplifier restarts.	2 to 100 seconds
Manual Restart	Triggers manual restart action for the ALS interface. However, manual restart does not happen if Mode is set to Automatic Restart or Disabled.	—

Step 3 Click **Apply** to save the changes.

Clear the Raman Laser Shutdown Condition

The Raman Laser Shutdown (RLS) condition is raised during the Raman link turn-up phase on the RAMAN-TX port of the RAMAN-CTP and RAMAN-COP cards when excessive back reflection is detected. When the RLS condition is raised, the Raman pump laser inside the card is automatically shut down and the optical link turn-up procedure is terminated. The RLS condition must be cleared before proceeding with further provisioning.

Use this task to clear the RLS condition for RAMAN-CTP and RAMAN-COP cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Safety** tabs.

Step 2 Click **Manual Safety Restart** to clear the RLS condition.

A confirmation dialog box appears and is service-affecting.

Step 3 Click **Yes** to proceed.

Provision FPD Upgrade

Whenever the firmware version on the card is earlier than the FPGA firmware version, an alarm "FPD-UPG-REQUIRED" is raised on the card in the **Alarms** tab.

You can view the running firmware version and the NCS 2000 FPGA firmware version under the **Maintenance** > **FPD upgrade** tabs.

Use this task to upgrade the RMN-CTP-CL card with the latest firmware released as part of the NCS 2000 software release.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **FPD Upgrade** tabs.

Step 2 Click **FPD upgrade** to perform firmware upgrade for the card.

After the firmware upgrade is completed successfully, the "FPD-UPG-REQUIRED" alarm gets cleared in **Alarms** tab and you can view the updated running firmware version in the **FPD Upgrade** table.

View Insertion Loss Parameters

Use this task to view the insertion loss parameters of cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Click the **Maintenance** > **Insertion Loss** tabs to view the insertion loss parameters.

The Insertion Loss tab displays the following information:

- **Insertion Loss Path**—Displays the insertion loss path.
- **IL Value (dB)**—Displays the insertion loss value.

Note When the card is removed, the last retrieved Insertion Loss values are displayed in the SVO web UI. When the card is replaced, the Insertion Loss values are updated in the SVO web UI.

Perform Manual Calibration

Use this task to perform manual calibration for the RAMAN-CTP and RAMAN-COP cards.

The RAMAN-COP card supports only manual calibration. The RAMAN-CTP card supports both automatic and manual calibration. However, if a node has both RAMAN-CTP and RAMAN-COP cards, the RAMAN-CTP card supports only manual calibration.

For complete information on the specific setup that is required for manual calibration, see DLP-G690 Configure the Raman Pump Using Manual Day-0 Installation.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Manual Calibration** tabs.

All the values in this pane are read-only and reflects the status of last manual calibration.

Table 94: Parameters of Manual Calibration

Parameter	Description
Port	Displays the port number, port type, and direction (TX or RX).
Time Stamp	Displays the date and time of calibration.
Pump 1 Low Power (dBm)	Displays the measured incoming power with only pump 1 on at low power level.
Pump 2 Low Power (dBm)	Displays the measured incoming power with only pump 2 on at low power level.
Pump 1 High Power (dBm)	Displays the measured incoming power with only pump 1 on at high power level.
Pump 2 High Power (dBm)	Displays the measured incoming power with only pump 2 on at high power level.
Target Gain (dB)	Displays the target spectrum gain.
Obtained Gain (dB)	Displays the obtained spectrum gain.
Target Tilt (dB)	Displays the target spectrum tilt.
Obtained Tilt (dB)	Displays the obtained spectrum tilt.
Result	Displays the result of manual Raman calibration. The possible values of Result are as follows: • No Target Gain—Raman target gain is not configured. • Not Enough Gain—Raman gain obtained from calibration is too low. • Lower Than Target Gain—Raman gain obtained from calibration is below the target but is acceptable. • Target Gain Reached—Raman target gain is reached. • User Override—User has overridden the calibration result and uses the configured setpoint of Raman pumps manually.

Parameter	Description
Status	Displays the status of manual Raman calibration. The possible values of Status are as follows: • Not Calibrated—Raman calibration was not run. • In Progress—Raman calibration is being run by the user. • Completed—Raman calibration is completed. • Using pumps-power-setpoint—Raman pumps are regulated according to the user configuration.

Step 2 Click **Run Calibration**.

A confirmation message appears.

Step 3 Click **Yes**.

Step 4 Click **Run Pump Test** for each individual pump.

The pump test cannot be run if active circuits are present in the node. When you run the pump test, the Status column in the Manual Calibration tab changes to "In Progress."

Step 5 Enter the optimum power value of individual pump in the Power Value (dBm) field.

Step 6 Click **Calibrate Pump** to start the manual calibration.

The calibration progress appears in the **Calibration Result** area. The calibration result can be a success, failure, or lower than target gain.

- If the calibration result is success, the obtained target gain value is applied to the node.
- If the calibration result is a failure, the old target gain value is restored.
- If the calibration result is lower than the target gain, it implies that the obtained gain is + or –2 dB from the target gain. The gain is degraded. However, the calibration is still accepted and the obtained target gain value is applied to the node.

Perform Automatic Calibration

Use this task to perform automatic calibration for the RAMAN-CTP, RMN-CTP-CL, EDRA1-xx, and EDRA2-xx cards.

The automatic calibration automatically runs on the cards upon fiber restoration, power cycle, and so on.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Automatic Calibration** tabs.

All the values in this pane are read-only and reflects the status of last automatic calibration.

Note Only the Port, Timestamp, Result, Status, Max Gain, and Progress parameters are applicable for the RMN-CTP-CL card.

Table 95: Parameters of Automatic Calibration

Parameter	Description
Port	Displays the port number, port type, and direction (TX or RX).
Timestamp	Displays the date and time of calibration.
Calibration Gain (dB)	Displays the Raman gain that is obtained with calibration of total pump power.
Calibration Total Pumps (mW)	Displays the reference power level used throughout calibration. The default value is 700 mW. If Raman gain is too low, the power value is automatically increased to 850 mW.
Target Gain (dB)	Displays the target spectrum gain.
Obtained Gain (dB)	Displays the obtained spectrum gain.
Target Tilt (dB)	Displays the target spectrum tilt.
Obtained Tilt (dB)	Displays the obtained spectrum tilt.
Raman Noise Floor (dBm)	Displays the optical power measured at the LINE-RX port when Raman pumps are at calibration total pumps power level and incoming signal is not received from the neighboring node. It is noise generated by the Raman amplification process.
Incoming Power Pumps Off (dBm)	Displays the power level of probe signal with Raman pumps off.
Incoming Power Pumps On (dBm)	Displays the power level of probe signal with Raman pumps on (combined with Raman noise floor).

Parameter	Description
Power Source	Displays the type of power source that is used for calibration. The possible values of Power Source are as follows: • Broadband Optical Power—Raman automatic calibration used broadband optical power, typically, Amplified Spontaneous Emission (ASE) generated by an optical amplifier. • Active Optical Services—Raman automatic calibration used active services. • Active Optical Services (Unbalanced)—Raman automatic calibration used active services;however, they do not properly cover the whole C-Band spectrum.
Result	Displays the result of automatic Raman calibration. The possible values of Result are as follows: • No Target Gain—Raman target gain is not configured. • Not Enough Gain—Raman gain obtained from calibration is too low. • Lower Than Target Gain (Need Accept)—Raman gain obtained from calibration is below the target but might be acceptable. The user must accept the Raman gain. • Lower Than Target Gain (Accepted)—Raman gain obtained from calibration is below the target and the user has accepted the Raman gain. • Target Gain Reached—Raman target gain is reached. • User Override—User has overridden the calibration result and uses configured setpoint of Raman pumps manually.

Parameter	Description
Status	Displays the status of automatic Raman calibration. The possible values of Status are as follows: • Not Scheduled—Raman automatic calibration is not scheduled. • Invalid—Raman automatic calibration reports invalid data. • Pending—Raman automatic calibration is scheduled and pending. • Running On User Request—Raman automatic calibration is running on user request. • Running—Raman automatic calibration is automatically running. • Failed—Raman automatic calibration has failed. • Aborted—Raman automatic calibration has been terminated and will be re-scheduled soon. • Completed—Raman automatic calibration is completed.
Max Gain	(Only for RMN-CTP-CL card) Displays the maximum obtainable Raman gain value on the specific fibre span. The value is a result of the initial probing during the Raman Calibration procedure and indicates the quality of fibre for Raman amplification. The higher the max gain value, the better. The lower max gain value (10 dB or lower) indicates that the fibre is not suitable for Raman amplification.
Progress	(Only for RMN-CTP-CL card) Displays the current stage of the calibration. This parameter can have values such as "Probing Transmission Fibre", "Evaluating Max Gain", and "Calculating Pumps Power for Target Gain".

Step 2 Click **Run Calibration** to start the automatic calibration.

A confirmation message appears.

Step 3 Click **Yes**.

When you start the automatic calibration, the Status column in the Automatic Calibration tab changes to "Running on User Request."

The calibration result can be success, failure, or lower than target gain.

- If the calibration result is success, the obtained target gain value is applied to the node.
- If the calibration result is failure, the old target gain value is restored.

- If the calibration result is lower than target gain, it implies that the obtained gain is + or –2 dB from the target gain. The gain is degraded. The RAMAN-GAIN-NOT-REACHED alarm is raised on the node to inform the user of a lower target gain. The user can accept this lower target gain by clicking the **Accept Degraded Gain** button. This clears the RAMAN-GAIN-NOT-REACHED alarm and the lower target gain value is applied to the node.

Step 4 (Optional) (Not applicable for RMN-CTP-CL card) Click **Get All Calibration Reports** to display the last 10 calibration reports with the timestamp and result in a table.

Step 5 (Optional) Click **Get Last Calibration Error** to identify the reason for the last calibration failure.

The automatic calibration typically completes without user intervention. However, the automatic calibration fails upon certain conditions such as loss of communication between two nodes and OSC failure. You can identify the reason for the last calibration failure by clicking the **Get Last Calibration Error** button. The reason is displayed only when the Status column in the Automatic Calibration tab is Failure.

Collect Failure Logs

Use this task to collect the failure log information for the cards. This task can be used to debug the cards before RMA.

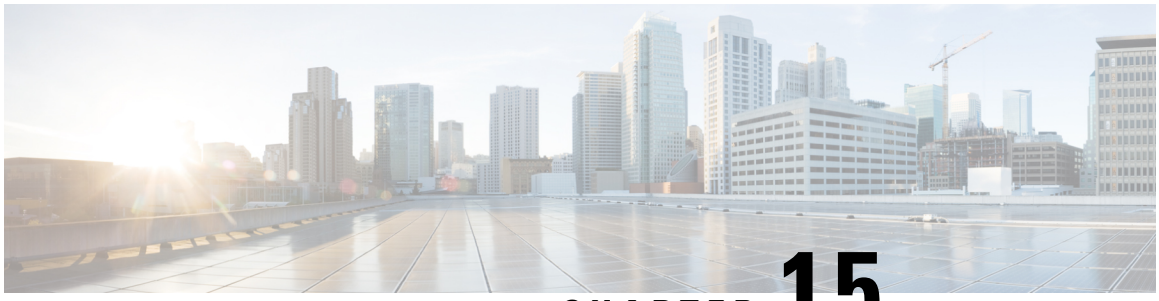
Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Right-click the card and choose **OBFL** to collect the On Board Failure Logs (OBFL).

The failure log information is displayed in the **Maintenance** > **OBFL Status** tabs.



CHAPTER 15

Provision Optical Add/Drop Cards

This chapter describes the Optical Add or Drop (ROADM) cards used in Cisco NCS 2000 SVO and its related tasks.

The following table lists the package support for the optical add/drop cards.

Card	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
16-AD-CCOFS	✓	
6AD-DD-CFS	✓	

16-AD-CCOFS Card

In this chapter, "16-AD-CCOFS" refers to the NCS2K-16-AD-CCOFS card.

The 16-AD-CCOFS card is a single slot add or drop card that provides colorless, contentionless, omnidirectional, and flex spectrum capability on 16 channels over 4 ROADM directions. The card receives the same wavelength from 16 transponder cards and forwards it to different ROADM nodes without collision. This capability is achieved using multicast switches. 2 or 3 16-AD-CCOFS cards can be connected using upgrade ports to provide the add/drop capability on 16 channels over 8 or 12 ROADM directions respectively.

Each add/drop port pair in the card is:

- Colorless - forwards any wavelength on a specific port
- Contentionless - adds/drops the same wavelength from the same add/drop section to different directions
- Omnidirectional - connects to both the add and drop directions

The 16-AD-CCOFS card can be installed in any service slots in the Cisco NCS 2006 and NCS 2015 chassis. The 16-AD-CCOFS card works only in the Cisco NCS Flex node.

Key Features

- Has a 16x4 multiplexer and a 4x16 demultiplexer.
- Monitors optical power on the input ports through optical photo diodes and raises alarms when the threshold is exceeded.
- Supports tone detection on the input ports in the add direction.
- Provides a multicast switch that does not block any wavelength and does not have any optical filtering element.
- Has fixed gain EDFA amplifiers in the add or drop directions to compensate for high optical insertion loss. The gain is -1 dB in the drop direction and -2 dB in the add direction.

For more information about the 16-AD-CCOFS card, such as the block diagram and card specifications, see the data sheet.

6AD-DD-CFS Card

Table 96: Feature History

Feature Name	Release Information	Feature Description
6AD-DD-CFS Card	Cisco NCS 2000 Release 12.3	The new NCS 2000 6-port add/drop card supports multiplexing and amplification of wavelengths from interfaces with ZR+ pluggables for colorless transmission over ROADM nodes in the network. The card can be installed in NCS 2006 and NCS 2015 chassis.

In this chapter, "6AD-DD-CFS" refers to the NCS2K-6AD-DD-CFS card.

The output power from the ZR and ZR+ pluggables is low and must be amplified before it enters the multiplexer on the ROADM node. The 6AD-DD-CFS card is a single slot add or drop card that supports C-band multiplexing of ZR and ZR+ wavelength outputs. The 6AD-DD-CFS card includes six add or drop port multiplexer with an amplifier working in fixed gain mode. This card provides colorless and flex spectrum capability on six channels over a single ROADM direction.

The 6AD-DD-CFS card can be installed in any service slots in the Cisco NCS 2006 and NCS 2015 chassis. The 6AD-DD-CFS card works only in the Cisco NCS node that is installed with the flex package.

Key Features

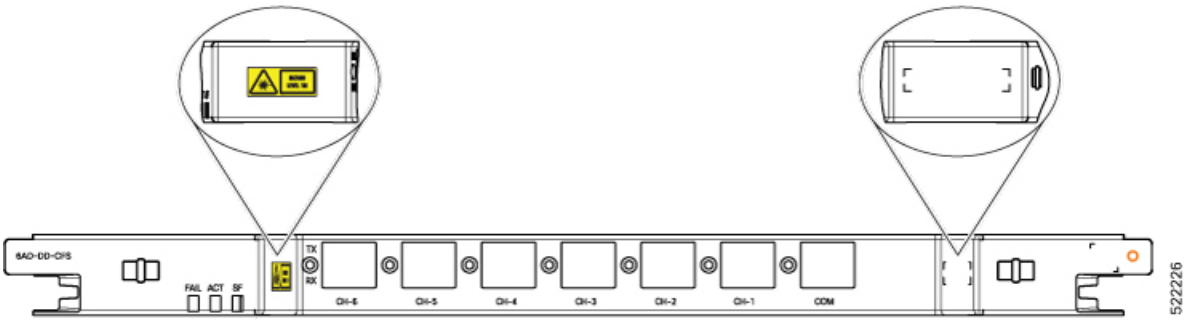
The 6AD-DD-CFS card provides the following key features:

- Provides aggregation and amplification of up to six wavelengths.

- Provides fixed gain EDFA amplifiers in the add and drop directions to compensate for high optical insertion loss.
- Supports ASE compensation in Constant Gain and in Constant Output Power mode.
- Supports fast transient suppression.
- Supports optical safety functionality through:
  - Signal loss detection, LOS signal generation, and alarm at any input port
  - Fast power down control
  - Reduced maximum output power in safe power mode
- Monitors optical power on the input ports through optical photodiodes and raises alarms when the threshold is exceeded.
- Supports tone detection on the input ports in the add direction.

Faceplate Diagram

Figure 21: Faceplate Diagram of 6AD-DD-CFS Card



LC Connector Assignment

The 6AD-DD-CFS card uses LC connectors for all the ports.

Table 97: LC Connector Assignment

Optical Connector Label	Optical Connector Type	Port Name
COM-TX	LC - UPC	COM-TX
COM-RX	LC - UPC	COM-RX
CH-1	LC - UPC	CH-1-TX/RX
CH-2	LC - UPC	CH-2-TX/RX
CH-3	LC - UPC	CH-3-TX/RX
CH-4	LC - UPC	CH-4-TX/RX
CH-5	LC - UPC	CH-5-TX/RX

Optical Connector Label	Optical Connector Type	Port Name
CH-6	LC - UPC	CH-6-TX/RX

For more information about the 6AD-DD-CFS card, such as the block diagram and card specifications, see the data sheet.

Provision Interface Parameters

Use this task to change the optical interface parameters of the 16-AD-CCOFS and 6AD-DD-CFS cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Interface** tabs.

Step 2 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 98: Interface Options

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (RX or TX)	All the RX and TX ports
Admin State	(Display only) Displays the administrative state of the port.	From the drop-down list, choose one of the following: • Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ Locked-enabled,maintenance
Optical Power (dBm)	Displays the optical power for each port.	—
Optical PSD Setpoint (dBm/GHz)	Target output PSD requested by the user.	—
Attenuator Value (dB)	Sets the attenuator value.	—
Optical Power Threshold Low (dBm)	Fail low threshold used to detect the LOS alarm on the port.	—
Current Power Failure Low (dBm)	(Display only) Shows the optical power failure low threshold for the port.	—
Current Power Degrade High (dBm)	(Only for 16-AD-CCOFS card) (Display only) Shows the current value of the optical power degrade high threshold configured in the card. Power Degrade High refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Degrade Low (dBm)	(Only for 16-AD-CCOFS card) (Display only) Shows the current value of the optical power degrade low threshold configured in the card. Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—

Parameter	Description	Options
VOA Attenuation Setpoint (dB)	(Only for 6AD-DD-CFS card) Sets the VOA attenuation value.	0 to 25
VOA Attenuation Offset (dB)	(Only for 6AD-DD-CFS card) Sets the offset with respect to the set setpoint.	0 to 25
VOA Current Attenuation (dB)	(Only for 6AD-DD-CFS card) (Display only) Shows the VOA current attenuation.	—

Step 3 Click **Apply** to save the changes.

Provision Thresholds for TCA alarms

Use this task to change the thresholds for TCA alarms raised on the 16-AD-CCOFS and 6AD-DD-CFS cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Optics Thresholds** tabs.

Step 2 Choose the type of threshold that you want to change, 15 Min or 1 Day.

Step 3 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 99: Threshold Options

Parameter	Description	Options
Interface Name	(Display only) Displays the port number, port type, and direction (RX or TX)	All the TX and RX ports
PM Type	Type of interface	opticalPowerPMTh
Low	Sets the low power warning level.	Numeric. The default is -50 dBm. Double-click the parameter, enter a value, and press Enter.

Parameter	Description	Options
High	Sets the high power warning level.	Numeric. The default is 30 dBm. Double-click the parameter, enter a value, and press Enter.

Step 4 Click **Apply** to save the changes.

Provision Optical Safety

Use this task to provision the optical safety parameters of the 16-AD-CCOFS card.

Note This task is not applicable for the 6AD-DD-CFS card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Optical Safety** tabs.

Step 2 Modify required settings described in the following table:

Table 100: Optical Safety Parameters for Cards

Parameter	Description	Options
Interface	(Display only) Displays the port name, port type, and direction.	—
Supported Safety	(Display only) Displays the supported safety mechanism.	• ALS for line cards and control cards. • ALS-OSRI for amplifier cards.

Parameter	Description	Options
ALS Mode	Automatic laser shutdown mode. The ALS mode is disabled for RX ALS interfaces.	From the drop-down list, choose one of the following: • ALS-Disabled—Deactivates ALS. • Automatic Restart—(Default) ALS is active. The power is automatically shut down when needed, and it automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart
OSRI	Optical safety remote interlock. The default value is OSRI-OFF. When set to OSRI-ON, the TX output power is shut down. **Note** OSRI configuration is not supported on the transponder and muxponder cards.	From the drop-down list, choose one of the following: • OSRI-OFF • OSRI-ON
ALS Status	(Display only) ALS status of the device.	• Working • Shutdown
Recovery Pulse Interval	Displays the interval between two optical power pulses.	60 to 300 seconds.
Recovery Pulse Duration	Displays the duration of the optical power pulse that begins when an amplifier restarts.	2 to 100 seconds
Manual Restart	Triggers manual restart action for the ALS interface. However, manual restart does not happen if Mode is set to Automatic Restart or Disabled.	—

Step 3 Click **Apply** to save the changes.

Provision FPD Upgrade

Whenever the firmware version on the card is earlier than the FPGA firmware version, an alarm "FPD-UPG-REQUIRED" is raised on the card in the **Alarms** tab.

You can view the running firmware version and the NCS 2000 FPGA firmware version under the **Maintenance** > **FPD upgrade** tabs.

Use this task to upgrade the 6AD-DD-CFS card with the latest firmware released as part of the NCS 2000 software release.

Note This task is not applicable for the 16-AD-CCOFS card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **FPD Upgrade** tabs.

Step 2 Click **FPD upgrade** to perform firmware upgrade for the card.

After the firmware upgrade is completed successfully, the "FPD-UPG-REQUIRED" alarm gets cleared in the **Alarms** tab and you can view the updated running firmware version in the **FPD Upgrade** table.

View Insertion Loss Parameters

Use this task to view the insertion loss parameters of the 16-AD-CCOFS and 6AD-DD-CFS cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Click the **Maintenance** > **Insertion Loss** tabs to view the insertion loss parameters.

The Insertion Loss tab displays the following information:

- **Insertion Loss Path**—Displays the insertion loss path.

- **IL Value (dB)**—Displays the insertion loss value.

Note When the card is removed, the last retrieved Insertion Loss values are displayed in the SVO web UI. When the card is replaced, the Insertion Loss values are updated in the SVO web UI.

Collect Failure Logs

Use this task to collect the failure log information for the 16-AD-CCOFS and 6AD-DD-CFS cards. This task can be used to debug the cards before RMA.

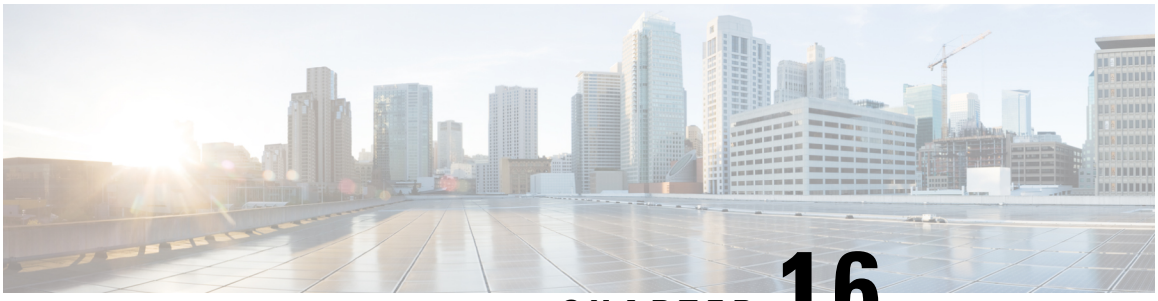
Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Right-click the card and choose **OBFL** to collect the On Board Failure Logs (OBFL).

The failure log information is displayed in the **Maintenance** > **OBFL Status** tabs.



CHAPTER 16

Provision Reconfigurable Optical Add/Drop Cards

This chapter describes the Reconfigurable Optical Add or Drop (ROADM) cards used in Cisco NCS 2000 SVO and its related tasks.

The following table lists the package support for the reconfigurable optical add/drop cards.

Card	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
9-SMR17FS	✓	
9-SMR24FS	✓	
9-SMR34FS	✓	
20-SMRFS	✓	
20-SMRFS-CV	✓	
80-WXC-C		✓
40-SMR1-C		✓
40-SMR2-C		✓

9-SMR17FS, 9-SMR24FS, 9-SMR34FS, 20-SMRFS, and 20-SMRFS-CV Cards

In this chapter, "9-SMRFS" refers to the 9-SMR17FS, 9-SMR24FS, and 9-SMR34FS cards. "20-SMRFS" refers to the NCS2K-20-SMRFS card. "20-SMRFS-CV" refers to the NCS2K-20-SMRFS-CV card.

The 9-SMR17FS, 9-SMR24FS, 9-SMR34FS, 20-SMRFS, and 20-SMRFS-CV cards are tunable over 96 channels in the C-band, at 50-GHz spacing on the ITU-T grid. The cards provide the flex spectrum capability, which gives the flexibility to allocate channel bandwidth, to increase the network scalability. With flex capability, the channel bandwidth is not fixed, but can be defined arbitrarily, with a specified granularity and within a given range. For each subrange, attenuation and power values are defined. The central frequency ranges from 191350 GHz (1566 .72 nm) to 196100 GHz (1528.77 nm).

The 9-SMR17FS, 9-SMR24FS, 9-SMR34FS, 20-SMRFS, and 20-SMRFS-CV cards are single-slot cards that integrate two cross-connect blocks (multiplexer and demultiplexer), a variable gain EDFA pre-amplifier, and a variable gain EDFA booster amplifier. The 9-SMR17FS, 9-SMR24FS, and 9-SMR34FS, cards support up to 9 directions for each ROADM node. The 20-SMRFS and 20-SMRFS-CV cards support up to 20 directions for each ROADM node. The cards can be installed in any service slot in the Cisco NCS 2000 Series chassis. The cards can be used in point-to-point, ring, multi-ring, or mesh topologies.

The 20-SMRFS-CV card has a dedicated laser source at the demultiplexer section, and a photodiode at the multiplexer section. The 20-SMRFS-CV card provides the connection verification capability using a connectivity check signal. The correctness and the quality of the interconnections determined by measuring the insertion loss of the external passive path can be validated with the connection verification feature. For more information about connection verification, see the Connection Verification, on page 110 and Verify Connections in Optical Cables, on page 112 sections.

Note When the user pre-provisions the 20-SMRFS-CV card in the SVO web interface and inserts the 20-SMRFS card physically and conversely, the system automatically updates with the card that is physically inserted.

The EDFA pre-amplifiers in 20-SMRFS and 20-SMRFS-CV cards have switchable gain ranges. The following table describes the gain ranges and extended gain ranges of an EDFA pre-amplifier in the 9-SMR17FS, 9-SMR24FS, 9-SMR34FS, 20-SMRFS, and 20-SMRFS-CV cards.

Table 101: Gain Ranges and Extended Gain Ranges of EDFA Pre-Amplifier

Card	Gain Range	Extended Gain Range
9-SMR17FS	0–17 dB with controlled tilt	20 dB with uncontrolled tilt
9-SMR24FS	12–24 dB with controlled tilt	27 dB with uncontrolled tilt
9-SMR34FS	20–34 dB with controlled tilt	40 dB with uncontrolled tilt
20-SMRFS and 20-SMRFS-CV	Gain Range 1: 0–17 dB with controlled tilt	20 dB with uncontrolled tilt
	Gain Range 2: 12–24 dB with controlled tilt	35 dB with uncontrolled tilt

For more information, such as the block diagrams and the card specifications of the 9-SMR17FS, 9-SMR24FS, 9-SMR34FS, 20-SMRFS, and 20-SMRFS-CV cards, see the data sheet.

20-SMRFS and 20-SMRFS-CV Ports

The 20-SMRFS and 20-SMRFS-CV cards have these ports:

- [EXP 1–8]-1...8-TX, [EXP 9–16]-1...8-TX and [EXP 17–20]-1...4-TX ports send the split-off optical signal that contains pass-through channels to the other side of the NE.
- [EXP 1–8]-1...8-RX, [EXP 9–16]-1...8-RX and [EXP 17–20]-1...4-RX port receive the optical signal from the pass-through channels.
- OSC-TX—The OSC-TX port transmits the Optical Service Channel signal that is received from the LINE-RX port signal to the controller card, separating it from the C-Band signals.
- OSC-RX—The OSC-RX port receives Optical Service Channel signal from the Controller Card and transmits it to the LINE-TX port.
- COM-TX—The COM TX port transmits the combined power from all directions or add or drop ports toward the booster amplifier.
- COM-RX—The COM RX port receives the optical signal from the pre-amplifier and sends it to the optical cross connect.

Note The COM-TX and COM-RX ports are not physical ports on the faceplate.

- LINE-TX—This port sends the optical signal from the local node to the far end node.
- LINE-RX—This port receives the optical signal from the far end node.

9-SMR-FS Ports

The 9-SMR-FS card has these ports:

- The nine EXP-TX ports send the optical signal to the other side of the NE based on the configuration of the internal WXC module.
- The nine EXP-RX ports receive the optical signal from the pass-through channels.
- OSC-TX—The OSC-TX port transmits the Service Channel signal that is received from the LINE-RX port signal, separating it from the C-Band signals.
- OSC-RX—The OSC-RX port receives signal from the Service Channel module and transmits it to the LINE-TX port.
- COM-TX—The COM TX port transmits the combined power from all the directions or add drop ports toward the amplifier.
- COM-RX—The COM RX port receives the optical signal from the pre-amplifier and sends it to the optical cross connect.

Note The COM-TX and COM-RX ports are not physical ports on the faceplate.

- LINE-TX—The booster amplifier amplifies the composite signal coming from WXC-MUX toward the LINE-TX port.
- LINE-RX—The pre-amplifier amplifies the composite signal coming from the LINE-RX port toward the WXC-DMX input.

Key Features

The multiplexer section of the 9-SMR17FS, 9-SMR24FS, 9-SMR34FS, 20-SMRFS, and 20-SMRFS-CV cards provide the following features:

- Selection of any arbitrary wavelength range from any EXP-RX*i* ports and routing to the MUX output port.
- Automatic VOA shutdown (AVS) blocking state on each wavelength on the MUX output port.
- Per-channel (closed loop) power regulation on the MUX output port based on OCM block feedback.
- Per-channel (open loop) attenuation regulation on the MUX output port, which is not based on the OCM feedback.
- Amplification of the aggregated C-Band signal toward the LINE-TX port by the variable gain booster EDFA amplifier.
- Combination of C-Band signals with 1510 nm by OSC MUX filter.
- Detection of the connectivity check signal, of wavelength 97 nm, by an embedded photodiode.

The demultiplexer section of the 9-SMR17FS, 9-SMR24FS, 9-SMR34FS, 20-SMRFS, and 20-SMRFS-CV cards provide the following features:

- Selection of any arbitrary wavelength range and routing to any EXP-TX*i* port.
- AVS blocking state on each wavelength, on any of the EXP-TX*i* ports.
- Per-channel (closed loop) power regulation on the EXP-TX*i* output port based on OCM block feedback.
- Per-channel (open loop) attenuation regulation on the EXP-TX*i* output port, which is not based on the OCM feedback.
- Amplification of the C-Band signals entering the LINE-RX port by the pre-amplifier.
- Separation of C-Band signals from 1510 nm by OSC De-MUX filter.
- Generation and transmission of the connectivity check signal into the DE-MUX input port.

80-WXC-C Card

Table 102: Feature History

Feature Name	Release Information	Description
80-WXC-C Card	Cisco NCS 2000 Release 12.2	The double-slot 80-channel Wavelength Cross-Connect C-band (80-WXC-C) card manages up to 80 ITU-T 50-GHz-spaced channels that are identified in the channel plan and sends them to dedicated output ports. Each channel can be selected from any input or output port. The card is an active ROADM module, and provides bidirectional capability. The 80-WXC-C card can be installed in NCS 2006 and NCS 2015 chassis.

The card is optimized for Degree-2 and Degree-N reconfigurable nodes.

The 80-WXC-C card provides the following functionalities:

- When used in the bidirectional mode, the 80-WXC-C card allows selection of a single wavelength or any combination of wavelengths from any of the nine input ports to the common output port.
- When used in the bidirectional mode, the output wavelength from the COM-RX port is split to manage the express and drop wavelengths.
- Automatic VOA shutdown (AVS) blocking state on each wavelength and port.
- Per-channel (closed loop) power regulation on the output port based on OCM block feedback.
- Per-channel (open loop) attenuation regulation on the output port which is not based on the OCM feedback.

For more information, such as the block diagrams and the card specifications, see 80-Channel Wavelength Cross-Connect Card and data sheet.

40-SMR1-C and 40-SMR2-C Cards

Table 103: Feature History

Feature Name	Release Information	Description
40-SMR1-C or 40-SMR2-C Cards	Cisco NCS 2000 Release 12.3	The 40-channel single-module ROADM with integrated optical pre-amplifier (40-SMR1-C) combines the OSC add/drop filter, a pre-amplifier, and a 2x1 wavelength selective switch (WSS)-based ROADM core into a single-slot unit. This unit is optimized for Degree-2 reconfigurable nodes. The 40-channel single-module ROADM with integrated optical pre-amplifier and boost amplifier (40-SMR2-C) includes the OSC add/drop filter, pre- and boost amplifiers, and a 4x1 WSS-based ROADM core. This unit provides an effective way to support multi-degree nodes up to Degree-4, allowing in-service upgrade from Degree-2 up to Degree-4 at a very competitive price point. Both cards optimize and increase the MSTP's throughput density.

"40-SMR1-C" refers to the _15454-40-SMR1-C card and "40-SMR2-C" refers to the _15454-40-SMR2-C card.

The 40-SMR1-C or 40-SMR2-C cards integrate the following functional blocks onto a single line card:

- Optical preamplifier
- Optical booster amplifier
- Optical service channel (OSC) filter
- 2x1 wavelength cross-connect (WXC) or a 4x1 WXC
- Optical channel monitor (OCM)

Key Features

The optical amplifier units in the cards provide the following features:

- Embedded gain flattening filter

- Mid-stage access for dispersion compensation unit (only applicable for preamplifier erbium-doped fiber amplifier [EDFA])
- Fixed output power mode
- Fixed gain mode
- Nondistorting low-frequency transfer function
- Amplified spontaneous emissions (ASE) compensation in fixed gain and fixed output power mode
- Fast transient suppression
- Programmable tilt (only applicable for preamplifier EDFA)
- Full monitoring and alarm handling capability
- Optical safety support through signal loss detection and alarm at any input port, fast power down control, and reduced maximum output power in safe power mode.
- EDFA section calculates the signal power, by taking into account the expected ASE power contribution to the total output power. The signal output power or the signal gain can be used as feedback signals for the EDFA pump power control loop.

The 40-SMR1-C card includes a 100GHz 1x2 WXC unit with integrated preamplifier unit (single EDFA). The card provides the following features:

- Selection of individual wavelength of the aggregated 100GHz signal from either the EXP-RX or ADD-RX ports
- Automatic VOA shutdown (AVS) blocking state on each wavelength and port
- Per-channel power regulation based on external OCM unit
- Open loop path attenuation control for each wavelength and port

The 40-SMR2-C card includes a 100GHz 1x4 WXC unit with integrated preamplifier and booster amplifier units (double EDFA). The card provides the following features:

- Selection of individual wavelength of the aggregated 100GHz signal from either the EXP*i*-RX (where *i* = 1, 2, 3) or ADD-RX ports
- Automatic VOA shutdown (AVS) blocking state on each wavelength and port
- Per-channel power regulation based on external OCM unit
- Open loop path attenuation control for each wavelength and port

The OCM unit provides per channel optical power monitoring at EXP-RX, ADD-RX, DROP-TX, and LINE-TX ports.

You can install the 40-SMR1-C or 40-SMR2-C card in any service slot in the Cisco NCS 2006 and NCS 2015 chassis.

For more information about the 40-SMR1-C or 40-SMR2-C card, see http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/data_sheet_c78-578552.html.

Change Optical Amplifier Settings

Use this task to change the optical amplifier settings of cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Amplifier** tabs.

Step 2 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 104: Amplifier Options

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (TX or RX).	—
Total Output Power (dBm)	(Display only) Shows the current power level per port.	—
Output Power Setpoint (dBm)	(Display only) Shows the current output power leaving the amplifier.	—
Working Mode	Sets the working mode.	The available options are: • Channel Power • Total Power • Optimized • Fixed Gain • Start and Hold
Role	Sets the role of the amplifier.	The available options are: • Preamplifier • Booster
Actual Gain (dB)	(Display only) The actual gain of the amplifiers.	—

Parameter	Description	Options
Target Gain (dB)	(Display only) The target gain of the amplifiers.	—
Tilt Setpoint (dB)	Target output tilt requested by the user.	-5 to 5
PSD Setpoint (dBm/GHz)	Power Spectral Density. Sets the PSD setpoint. Target output power requested by the user for each circuit.	-50 to 1
PSD Optimized (dBm/GHz)	Optimized PSD	—
Gain Setpoint (dB)	The value of the gain that the amplifier must achieve.	Display only or numeric depending on mode setting. When the system is configured as metro core, this field is display only. When the system is configured as metro access, this field can be changed by the user.
Gain Range	Sets the gain range of the amplifier.	• Gain Range 1 • Gain Range 2 • No Gain Range
Power Degrade Threshold High (dBm/GHz)	(Display only) Shows the current value of the optical power degrade high threshold configured in the card. This threshold applies only when the amplifier is active and in constant power mode. Power Degrade High refers to the port's Signal Output Power value and is automatically calculated by the control card when the amplifier is turned up.	—
Power Degrade Threshold Low (dBm/GHz)	(Display only) Shows the current value of the optical power degrade low threshold configured in the card. This threshold applies only when the amplifier is active and in constant power mode. Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card when the amplifier is turned up.	—

Parameter	Description	Options
Gain Degrade High (dB)	(Display only) Shows the current value of the gain degrade high threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode. Gain Degrade High refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up.	—
Gain Degrade Low (dB)	(Display only) Shows the current value of the gain degrade low threshold configured in the card. This threshold applies only when the amplifier is active and in constant gain mode. Gain Degrade Low refers to the Gain value of the port and is automatically calculated by the control card when the amplifier is turned up.	—

Step 3 Click **Apply** to save the changes.

Provision Interface Parameters

Use this task to change the optical interface parameters of cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Interface** tabs.

Step 2 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 105: Interface Options

Parameter	Description	Options
Port	(Display only) Displays the port number, port type, and direction (RX or TX)	All the RX and TX ports
Admin State	(Display only) Displays the administrative state of the port.	From the drop-down list, choose one of the following: • Unlocked (ETSI)/ IS (ANSI) • Locked, disabled (ETSI)/OOS, DSBLD (ANSI) • Locked, maintenance (ETSI)/OOS, MT (ANSI) • Unlocked, automaticInService (ETSI)/ IS, AINS (ANSI)
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR/ Unlocked-enabled • OOS-AU,AINS/ Unlocked-disabled, automaticInService • OOS-MA,DSBLD/ Locked-enabled,disabled • OOS-MA,MT/ Locked-enabled,maintenance
Optical Power (dBm)	Displays the optical power for each port.	—
OSC Power (dBm)	(Display only) Displays the service channel power level for each port.	—
Optical PSD Setpoint (dBm/GHz)	Target output PSD requested by the user.	-50 to 10
Attenuator Value (dB)	Sets the attenuator value.	—
Optical Power Threshold Low (dBm)	Fail low threshold used to detect the LOS alarm on the port.	—
OSC Power Threshold Low (dBm)	(Display only) Shows the OSC power level for each port.	— **Note** This is not supported on the 16-AD-CCOFS card.

Parameter	Description	Options
Current Power Degrade High (dBm)	(Display only) Shows the current value of the optical power degrade high threshold configured in the card. Power Degrade High refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Degrade Low (dBm)	(Display only) Shows the current value of the optical power degrade low threshold configured in the card. Power Degrade Low refers to the Signal Output Power value of the port and is automatically calculated by the control card.	—
Current Power Failure Low (dBm)	(Display only) Shows the optical power failure low threshold for the port.	—
VOA Attenuation Setpoint (dB)	(Only for 80-WXC-C, 40-SMR1-C, and 40-SMR2-C cards) Sets the VOA attenuation value	0 to 25
VOA Attenuation Offset (dB)	(Only for 80-WXC-C, 40-SMR1-C, and 40-SMR2-C cards) Sets the offset with respect to the set setpoint	—
VOA Current Attenuation (dB)	(Only for 80-WXC-C, 40-SMR1-C, and 40-SMR2-C cards) (Display only) Shows the VOA current attenuation	—

Step 3 Click **Apply** to save the changes.

Provision Thresholds for TCA alarms

Use this task to change the thresholds for TCA alarms raised on cards.

Before you begin

- Log into the SVO Web Interface, on page 67

- Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Optics Thresholds** tabs.

Step 2 Choose the type of threshold that you want to change, 15 Min or 1 Day.

Step 3 Modify the settings described in the following table. The provisionable parameters are listed in the Options column in the table.

Table 106: Threshold Options

Parameter	Description	Options
Interface Name	(Display only) Displays the port number, port type, and direction (RX or TX)	All the TX and RX ports
PM Type	Type of interface	opticalPowerPMTh
Low	Sets the low power warning level.	Numeric. The default is -50 dBm. Double-click the parameter, enter a value, and press Enter.
High	Sets the high power warning level.	Numeric. The default is 30 dBm. Double-click the parameter, enter a value, and press Enter.

Step 4 Click **Apply** to save the changes.

Provision Optical Safety

Use this task to provision the optical safety parameters for cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Optical Safety** tabs.

Step 2 Modify required settings described in the following table:

Table 107: Optical Safety Parameters for Cards

Parameter	Description	Options
Interface	(Display only) Displays the port name, port type, and direction.	—
Supported Safety	(Display only) Displays the supported safety mechanism.	• ALS for line cards and control cards. • ALS-OSRI for amplifier cards.
ALS Mode	Automatic laser shutdown mode. The ALS mode is disabled for RX ALS interfaces.	From the drop-down list, choose one of the following: • ALS-Disabled—Deactivates ALS. • Automatic Restart—(Default) ALS is active. The power is automatically shut down when needed, and it automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart
OSRI	Optical safety remote interlock. The default value is OSRI-OFF. When set to OSRI-ON, the TX output power is shut down. **Note** OSRI configuration is not supported on the transponder and muxponder cards.	From the drop-down list, choose one of the following: • OSRI-OFF • OSRI-ON
ALS Status	(Display only) ALS status of the device.	• Working • Shutdown
Recovery Pulse Interval	Displays the interval between two optical power pulses.	60 to 300 seconds.
Recovery Pulse Duration	Displays the duration of the optical power pulse that begins when an amplifier restarts.	2 to 100 seconds

Parameter	Description	Options
Manual Restart	Triggers manual restart action for the ALS interface. However, manual restart does not happen if Mode is set to Automatic Restart or Disabled.	—

Step 3 Click **Apply** to save the changes.

Configure Operating Mode

Use this task to change the operating mode of the 80-WXC-C Card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click **Provisioning** > **Card Mode**.

Step 2 Choose WXC-BIDI from the **Mode** drop-down list.

Note The 80-WXC-C Card supports only the WXC-BIDI mode. If you configure unsupported card modes (WXC-MUX or WXC-DEMUX), the system raises the PROV-MISMATCH alarm.

Step 3 Click **Apply** to save the changes.

View Insertion Loss Parameters

Use this task to view the insertion loss parameters of cards.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Click the **Maintenance** > **Insertion Loss** tabs to view the insertion loss parameters.

The Insertion Loss tab displays the following information:

- **Insertion Loss Path**—Displays the insertion loss path.
- **IL Value (dB)**—Displays the insertion loss value.

Note When the card is removed, the last retrieved Insertion Loss values are displayed in the SVO web UI. When the card is replaced, the Insertion Loss values are updated in the SVO web UI.

Collect Failure Logs

Use this task to collect the failure log information for the cards. This task can be used to debug the cards before RMA.

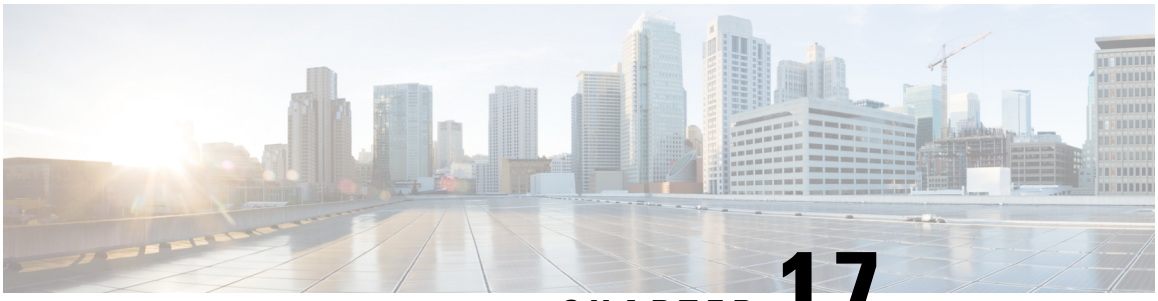
Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Right-click the card and choose **OBFL** to collect the On Board Failure Logs (OBFL).

The failure log information is displayed in the **Maintenance** > **OBFL Status** tabs.



CHAPTER 17

Manage Passive Devices

This chapter describes the passive devices used in Cisco NCS 2000 SVO and its related tasks.

Overview

Table 108: Feature History

Feature Name	Release Information	Description
Managing 15216-FLD-4 in SVO	Cisco NCS 2000 Release 12.3.1	You can now manage ten new Cisco ONS 15216 4 Channel Optical Add/Drop Multiplexers (OADMs), which are passive FLD units in a 100-GHz channel plan. These passive FLD units in SVO provide Multiservice Transport Platform (MSTP) to address the edge of the optical network in a cost-effective manner.
NCS2K-MF-8x10G-FO	Cisco NCS 2000 Release 12.3	The MPO-12 to 8-LC fan-out module is a double slot module with two MPO-12 connector (COM) and eight LC duplex connectors (Port-i-TX/RX). It contains 16 photodiodes to monitor the power of the channel input ports.

Feature Name	Release Information	Description
_15216-PP-4-SMR	Cisco NCS 2000 Release 12.3	The _15216-PP-4-SMR patch panel connects up to four 40-SMR2-C cards in a four-degree mesh node. The optical splitters inside the patch panel forward the output signal (EXP-TX port) of the 40-SMR2-C card on each side of the mesh node to the input port of the 40-SMR2-C cards on the other three sides of the mesh node.
NCS2K-MF-CL-SC	Cisco NCS 2000 Release 12.2	A new passive module, the C and L-band combiner and splitter, is introduced. The L-band addition for non-Raman assisted optical links requires a C and L optical combiner for expansion. The NCS2K-MF-CL-SC module allows Cisco to introduce any future L-band transmission system onto the existing NCS 2000 deployments.

Passive devices are used to build the optical network system. You can install them on:

- 19 inch (482.6 mm) or 23 inch (584.2 mm) EIA standard racks
- 19 inch (482.6 mm) IEC rack
- 600 mm x 600 mm or 600 mm x 300-mm ETSI rack

The following table lists the supported passive chassis and passive devices:

Passive Chassis and Passive Devices	Description	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
NCS2K-MF-6RU	You can install a combination of 14 single-slot passive devices in this chassis.	✓	
NCS2K-MF10-6RU	You can install a combination of 10 double-slot passive devices in this chassis.	✓	
NCS2K-MF-DEG-5	5-degree mesh module.	✓	
NCS2K-MF-UPG-4	4-degree upgrade module.	✓	

Passive Chassis and Passive Devices	Description	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
NCS2K-MF-MPO-16LC	MPO-16 to 16-LC fan-out module.	✓	
NCS2K-MF-2MPO-ADP	Double MPO-16 to two MPO-8 adapter module.	✓	
15216-MD-48-EVEN	Multiplexer/demultiplexer patch panels of 48-channels on the even ITU grid.	✓	✓ (only as inventory)
15216-MD-48-ODD	Multiplexer/demultiplexer patch panels of 48-channels on the odd ITU grid.	✓	✓ (only as inventory)
15216-MD-40-EVEN	Multiplexer/demultiplexer patch panels of 40-channels on the even ITU grid.		✓
15216-MD-40-ODD	Multiplexer/demultiplexer patch panels of 40-channels on the odd ITU grid.		✓
NCS1K-MD-64-C	Multiplexer/demultiplexer patch panels of 64-channels. **Note** Blink LED and status are not supported.	✓	
15216-MD-48-CM	Interleaver and deinterleaver pluggable that operates inside ONS 15216-MD-48 odd/even patch panels and 15216-MD-40 odd/even patch panels.	✓	✓ (only as inventory)
NCS2K-PPMESH8-5AD	8-degree mesh patch panel module with 16 MPO-16 connectors and 10 MPO-8 connectors.	✓	

Passive Chassis and Passive Devices	Description	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
NCS2K-MF-6AD-CFS	Six ports add/drop single slot module. It contains a 6x1 combiner and a 1x6 splitter.	✓	
NCS2K-MF-DEG-5-CV	5-degree mesh connection verification module with MPO-8 loopback caps.	✓	
NCS2K-MF-UPG-4-CV	4-degree upgrade connection verification module with MPO-8 loopback caps.	✓	
NCS2K-MF-MPO-8LC	MPO-APC to eight LC-PC fan-out module.	✓	
NCS2K-MF-M16LC-CV	MPO-16 to 16-LC fan-out connection verification double slot module based on the NCS2K-MF-MPO-16LC. It has eight LC loopback caps (NCS2K-LC-LBK=) on all LC dual ports.	✓	
NCS2K-MF-10AD-CFS	10 port add/drop double slot module. It contains a 10x1 combiner and a 1x10 splitter.	✓	
NCS2K-MF-16AD-CFS	16-channel colorless omnidirectional add/drop passive module.	✓	
NCS2K-MF-4X4-COFS	4-channel colorless omnidirectional add/drop passive module.	✓	
NCS2K-MF-CL-SC	The NCS2K-MF-CL-SC is a passive unit splitter that splits the C+L composite signal into individual C and L bands. The module can fit into a single slot (1/2 RU) of the NCS2K-MF-6RU shelf.	✓	

Passive Chassis and Passive Devices	Description	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
15216-MD-ID-50	The ONS 15216-MD-ID-50 is a C-band 50 GHz/100 GHz module that operates inside the patch panel. The ONS 15216-MD-ID-50 module interfaces between the 15216-MD-40-ODD and 15216-MD-40-EVEN patch panels, and 80 channels of wavelengths.		✓
15216-PP-MESH-4	Cisco 15454-PP-MESH-4 2RU 4-Degree mesh patch panel		✓
15216-PP-MESH-8	Cisco 15454-PP-MESH-8 2RU 8-Degree mesh patch panel		✓
NCS2K-MF-8x10G-FO	MPO-12 to 8-LC fan-out module. The MPO-12 to 8-LC fan-out module is a double slot module with two MPO-12 connector (COM) and eight LC duplex connectors (Port-i-TX/RX). Insertion loss, power monitoring, and attentuator settings are not supported.	✓	✓

Passive Chassis and Passive Devices	Description	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
15216-PP-4-SMR	15216-PP-4-SMR 4-degree mesh patch panel. The patch panel interconnects up to four 40-SMR2-C cards in a mesh node. The patch panel splits light coming from each direction into four and forwards it to the 40-SMR2-C cards in the other directions. The supported cables are: • 15454-MPO-MPO-2= is used for the PP-MESH interconnection • 15454-MPO-XMPO-2=is used for back-to-back 40-SMR2-C interconnections		✓

The following table lists the supported passive FLD units:

Passive FLD Units	Description	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
_15216-FLD4-30-3	Passive FLD Unit with 30 and 3 channels.	Not Supported	✓
_15216-FLD4-33-4	Passive FLD Unit with 33 and 4 channels.	Not Supported	✓
_15216-FLD4-36-6	Passive FLD Unit with 36 and 6 channels.	Not Supported	✓
_15216-FLD4-39-7	Passive FLD Unit with 39 and 7 channels.	Not Supported	✓
_15216-FLD4-42-9	Passive FLD Unit with 42 and 9 channels.	Not Supported	✓
_15216-FLD4-46-1	Passive FLD Unit with 46 and 1 channel.	Not Supported	✓
_15216-FLD4-49-3	Passive FLD Unit with 49 and 3 channels.	Not Supported	✓

Passive FLD Units	Description	SSON Package (12.xx-xxxx-xx.xx-S-SPA)	MSTP Package (12.xx-xxxx-xx.xx-L-SPA)
_15216-FLD4-52-5	Passive FLD Unit with 52 and 5 channels.	Not Supported	✓
_15216-FLD4-55-7	Passive FLD Unit with 55 and 7 channels.	Not Supported	✓
_15216-FLD4-58-9	Passive FLD Unit with 58 and 9 channels.	Not Supported	✓

The 15216-MD-48-ODD and 15216-MD-48-EVEN patch panels can be installed directly in the rack and require two Rack Units (RU). You can connect the patch panels to the NCS 2006 ECU or NCS 2015 ECU.

The NCS2K-MF passive devices can be installed in a one-Rack Unit (RU) high mechanical frame (NCS2K-MF-1RU) and can be directly connected to the NCS 2006 ECU or NCS 2015 ECU. You can also install the NCS2K-MF passive devices in the passive chassis. There are two types of passive chassis—NCS2K-MF-6RU and NCS2K-MF10-6RU. You can connect the passive chassis to the USB 3.0 port in the NCS 2006 ECU-S or NCS 2015 ECU.

Laser Radiation Emission Restrictions

The Class 1M Laser safety and warning label affixed to the passive optical modules indicate that the product should never be used or installed in an optical network with emissions higher than Class 1M.

Warning Class 1M laser radiation when open. Do not view directly with optical instruments. Statement 281

Laser Safety During Operation

Warning Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments. Statement 1051

Electrical Safety

The passive optical modules are optically and electrically passive and require no electrical connections. No electrostatic discharge (ESD) or other electrical safety considerations apply.

Manage Passive Devices

Use this task to add or delete a passive device.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Perform these tasks, as needed:

a) Add a Passive Device to a Rack, on page 362.
b) Add a Passive Device to a Passive Chassis, on page 363.
c) Delete a Passive Device, on page 364.

Add a Passive Device to a Rack

Use this task to add a passive device to a rack.

Note The NCS2K-MF-1RU chassis is a four -slot one rack unit mechanical frame that is auto-provisioned when a NCS2K-MF passive device is provisioned in the rack.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the Rack in the left panel.

The Rack view appears.

Step 3 Click an empty slot in the Rack.

Step 4 Click **Add Passive Device**.

Step 5 Select the node from the **Select Device** drop-down list.

Step 6 Select the passive device from the **Select Passive** drop-down list.

Step 7 Select the passive ID from **Enter Passive ID** drop-down list.

Note The 15216-MD-48-EVEN and 15216-MD-48-ODD devices are prefixed with a "_" in the SVO web interface.

Step 8 Select the slot number from **Select Slot** drop-down list.

Step 9 (Optional) Enter a device name in the **Display Name** field.

Step 10 Click **Provision**.

The passive device is provisioned and is listed in the Provisioning > Passives tab in the Rack view.

Add a Passive Device to a Passive Chassis

Use this task to add a passive device to a passive chassis. The following devices can be added to a passive chassis.

The following devices can be added to a NCS2K-MF-6RU chassis.

- NCS2K-MF-UPG-4
- NCS2K-MF-UPG-4-CV
- NCSK-MF-4x4-COFS
- NCS2K-MF-MPO-ADP
- NCS2K-MF-6AD-CFS
- NCS2K-MF-DEG-5
- NCS2K-MF-DEG-5-CV
- NCS2K-MF-MPO-8LC
- NCS2K-MF-CL-SC

The following device can be added to a NCS2K-MF10-6RU chassis.

- NCS2K-MF-MPO-16LC
- NCS2K-MF-M16LC-CV
- NCS2K-MF-10AD-CFS
- NCS2K-MF-16AD-CFS
- NCS2K-MF-8x10G-FO

Note To provision a CV passive device you must provision the respective non-CV passive device and associate it to a USB port. The PID of the CV passive device is then visible in the Provisioning > Passives tab in the chassis view.

Before you begin

- Log into the SVO Web Interface, on page 67
- Add a Chassis, on page 73

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click an empty slot in the passive chassis.

Step 4 Select the passive device from the **Select** drop-down list.

Step 5 Enter a passive ID in the **Passive ID** field.

Step 6 Click **Provision**.

The passive device is provisioned and is listed in the Provisioning > Passives tab in the chassis view.

Delete a Passive Device

Use this task to delete a passive device from a rack or a passive chassis.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the Rack in the left panel.

The Rack view appears.

Step 3 Left-click the passive device to be deleted in the rack or in the passive chassis, and select **Delete**.

Associate a Passive Chassis or a Passive Device to a USB Port

Use this task to associate a passive chassis or a passive device to a USB port.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the Rack in the left panel.

The Rack view appears.

Step 3 Perform these steps, as needed:

a) For a passive chassis or a passive device provisioned on the rack, perform these steps:

1. Click the **Provisioning** > **Passives** tabs.
2. Check the check box of the passive chassis or passive device you want to associate.

b) For a passive device provisioned in the passive chassis, perform these steps:

1. Left-click the passive chassis in the rack, and select **Open**.
2. Click the **Provisioning** > **Passives** tabs.
3. Check the check box of the passive device you want to associate.

Step 4 Click **Edit**.

The **Associate USB Port** dialog box appears.

Step 5 Select the **USB port** from the drop-down list.

Step 6 Click **Apply**.

Note When a passive chassis is associated to a USB port, all the passive devices that are provisioned on that passive chassis are automatically associated to the USB port.

View the Passive Device LED Status

Use this task to identify a specific passive device that is associated to a USB port by using the LED blink function.

Note This task does not apply to the 15216-MD-48-EVEN and 15216-MD-48-ODD devices.

Before you begin

- Log into the SVO Web Interface, on page 67
- Associate a Passive Chassis or a Passive Device to a USB Port, on page 364

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the Rack in the left panel.

The Rack view appears.

Step 3 Perform these steps, as needed:

a) For a passive device provisioned on the rack, perform these steps:

1. Click the **Provisioning** > **Passives** tabs.

b) For a passive device provisioned in the passive chassis, perform these steps:

1. Click the passive chassis in the rack, and select **Open**.
2. Click the **Provisioning** > **Passives** tabs.

Step 4 Check the checkbox of the passive device.

Step 5 Click **LED Status** to know the LED status of the associated device.

The message, **LED Status of the device connected to selected USB port is solid-green** is displayed.

Step 6 Click **LED Blink** to start blinking the LED of the passive device.

The message, **Blink-LED action succeed** is displayed. The LED blinks in blue color helping the operator to identify a specific passive device.

Step 7 Click **LED Status** again.

The message, **LED Status of device connected to selected USB port is blinking-blue** is displayed.

Step 8 Click **LED Blink** again to stop the blinking.

The message, **Blink LED action succeed** is displayed.

Step 9 Click **LED Status** again.

The message, **LED Status of device connected to selected USB port is solid-green** is displayed.

View Passive Device Port Settings

Use this task to view the details of the passive device ports. You can modify the attenuator value, if needed.

Note This task does not apply to NSC2K-MF-8x10G-FO modules.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the Rack in the left panel.

The Rack view appears.

a) For a passive device provisioned on the rack, perform these steps:

1. Left-click the passive device, and click **Open**.
2. Click the **Maintenance** >**OTS Passives** tab.

b) For a passive device provisioned in the passive chassis, perform these steps:

1. Left-click the passive device in the passive chassis, and select **Open**.
2. Click the **Maintenance** > **OTS Passives** tabs.

The following information is displayed:

Note You can specify an attenuator value if an attenuator is connected to the related port.

- **Port Label**—Displays the port name of the connector.
- **Port Type**—Displays the passive port type. Values can be OCH-PORT or OTS-PORT.
- **MPO ID**—Displays the MPO index as seen on the front panel if the port is related to an MPO connector, such as MPO-8 (8 fibers) or MPO-24 (24 fibers)
- **MPO Port Position**—Displays the position according to the pinout scheme of the MPO connectors if the port is related to an MPO connector, such as MPO-8 (8 fibers) or MPO-24 (24 fibers)
- **Attenuator Value (dB)**—Displays the attenuator value.
- **Optical Power (dBm)**—Displays measured power if the port has an associated photodiode and the passive device is associated to a USB port.
- **Optical Threshold Low (dBm)**—Displays the threshold for minimum optical power. When the Optical Power value is lower than the Optical Threshold Low value, the node raises an alarm.

Note If an attenuator is added on the related port, specify value in the **Attenuator Value** field, and click **Apply**.

View Insertion Loss

Use this task to view the insertion loss on the passive device.

Note This task does not apply to NSC2K-MF-8x10G-FO modules.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the Rack in the left panel.

The Rack view appears.

Step 3 Perform these steps, as needed:

a) For a passive device provisioned on the rack, perform these steps:

1. Left-click the passive device, and click **Open**.
2. Click the **Insertion Loss** tab.

b) For a passive device provisioned in the passive chassis, perform these steps:

1. Click the passive device in the passive chassis, and select **Open**.
2. Click the **Maintenance** > **Insertion Loss** tabs.

The following information is displayed:

- **Insertion Loss Path**—Displays the path between two passive ports.
- **IL Value (dB)**—Displays the insertion loss that is related to the path specified in the Insertion Loss Path field.

Note When the passive device is disassociated, the last retrieved Insertion Loss values are displayed in the SVO web UI. When the the passive device is replaced, the Insertion Loss values are updated in the SVO web UI.

Provision FPD Upgrade for Passive Chassis

Table 109: Feature History

Feature	Release Information	Description
FPD Upgrade for Passive Chassis	Cisco NCS 2000 Release 12.3.1	The SVO web interface allows you to make an FPD upgrade for the passive chassis NCS2K-MF-6RU and NCS2K-MF10-6RU to the latest version released as part of the NCS 2000 software release. You can selectively upgrade the versions of BOOTROM, OS_BOOT, and OS_KERNEL, one by one, directly from SVO.

Use this task to upgrade the passive chassis NCS2K-MF-6RU and NCS2K-MF10-6RU with the latest firmware released as part of the NCS 2000

software release.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the Rack in the left panel.

The Rack view appears.

Step 3 Click the NCS2K-MF-6RU and NCS2K-MF10-6RU chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Maintenance** > **FPD Upgrade** tabs.

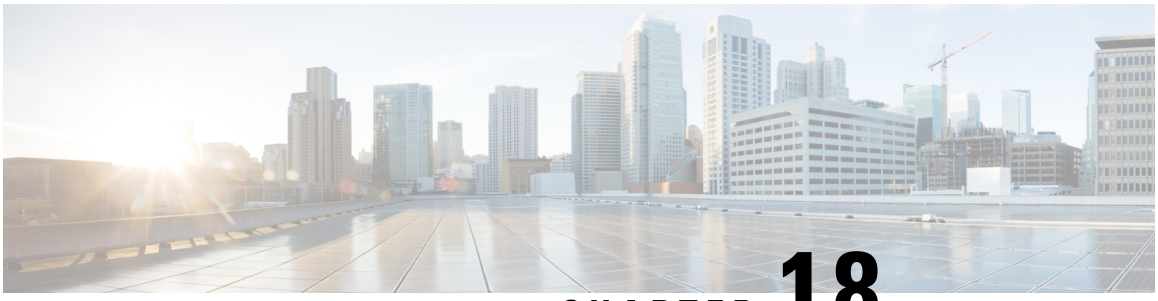
Step 5 Check the **BOOTROM**, **OS_BOOT**, and **OS_KERNEL** check boxes, and click **FPD Upgrade** to upgrade the versions of Boot ROM, operating system boot, and kernel versions necessary for the new software release.

Step 6 Click **Yes** to confirm.

After successful upgrade you can see the upgraded version of Boot ROM, OS_BOOT, and OS_Kernel in the FPD Upgrade table.

Note The **Running FW Version** is displayed as NA for OS_BOOT, if the Boot ROM is not upgraded to the latest version.

You can also perform the upgrade of Boot ROM, OS boot, and kernel one by one.



CHAPTER 18

Node Functional View

This chapter describes the Node Functional View (NFV) used in Cisco NCS 2000 SVO and its related tasks.

Table 110: Feature History

Feature Name	Release Information	Feature Description
Node Functional View (NFV) Enhancements	Cisco NCS 2000 Release 12.2	The following NFV enhancements are introduced to improve the user experience: • When you open a node or a side in the map view, the cards belonging to them are highlighted in the physical view. • Displays the last timestamp of NFV pane refresh using **Last graph update** icon. • In the **Display Neighbors** tab, clicking the IP address of the neighbor node opens the SVO Web User Interface of the neighbor node in a new browser tab. • In the **Card List** tab, the shelf number and slot number are displayed with the card name. The port number of the trunk port is also displayed for TXP cards. • You can set the width of the left shoulder.

Understanding Node Functional View

The NFV provides you with a display of the components and the association links between them in a graphical view. The graphical representation allows you to understand the connections and also guides you to troubleshoot.

The NFV can be accessed by clicking the hamburger icon at the top-left of the page in SVO web interface and selecting **Node Functional View**.

There are three views in the NFV representation:

View	Description
Physical view	Displays a physical representation of the node with the rack and all the cards inside.
Map view	Displays a map representation of the node in terms of components (sides, cards, and so on). The components are connected to each other using patch cords, according to the physical connections. You can have different context in the map view such as node view, side view, card view, circuit view, port view, and patch cord view. The appropriate details are displayed in the right shoulder based on the context in the map view. When you open a node or a side in the map view, the cards belonging to them are highlighted in the physical view. When you open a card in the map view, the card is zoomed and the corresponding rack is highlighted and zoomed in the physical view. You can view the circuits and patch cords at node view, side view, card view, and port views.
Detail view	Displays all the relevant information about the node, side, card, circuit, port, or patch cord depending on the context in the map view.

Alarm Status

The highest alarm severity is displayed as the overall status in the right shoulder. The possible alarm statuses, sorted by severity level, are:

- Normal - Displayed with White color
- Minor - Displayed with Yellow color
- Major - Displayed with Orange color
- Critical - Displayed with Red color

Action Icons in NFV

Icon	Description
Scroll View/Fit View	Scrolls or fits the rack view.
Zoom Reset	Resets the zoomed view to normal view.
Refresh	Refreshes the view with current information.
Last graph update	Displays the last timestamp of NFV pane refresh that is done using the **Refresh** button.
Open/Close Rack View	Opens or closes the rack view.
Status Filters	Displays only the alarms with specific severity. Click this button and check the **Critical**, **Major**, **Minor**, or **Normal** check boxes and click **Apply**.
User Settings	Sets the user preferences. See Set User Preferences, on page 380.
Zoom In	Zooms in the map view.
Zoom Out	Zooms out the map view.
Show/Hide Shoulder	Displays or hides the right shoulder.

View Details of Node

Use this task to view the details of the node in NFV.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Click **Show/Hide Shoulder** to open the right shoulder.

Step 3 View the **Name**, **Topology**, and **Status** fields in the right shoulder.

The **Status** field shows the most severe problem on the node.

Step 4 View the **Side List** pane that has two tabs - **Info on side** and **Display Neighbors**.

The **Info on side** tab displays the following information:

- Current status
- Span loss
- (Optional) OTDR, OSC, and PPC information is displayed when available

The **Display Neighbors** tab displays the list of optional neighbors of the components of the node. The following information is displayed for each side:

- Name of the side
- Icon corresponding to the alarm severity level
- (Optional) IP address of the node of its optional neighbor. To open the SVO web UI of the neighbor node in a new browser tab, click the IP address of the neighbor node.
- Degree of its optional neighbor

View Details of OLA Node

Use this task to view the details of the OLA node in NFV.

Note In OLA database, all the cards must be placed in the same degree and only one degree must be present in the node.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Click **Show/Hide Shoulder** to open the right shoulder.

Step 3 View the **Name**, **Topology**, and **Status** fields in the right shoulder.

The **Status** field shows the most severe problem on the node.

Step 4 View the **Side List** pane that has two tabs - **Info on side** and **Display Neighbors**.

The **Info on side** tab displays the following information:

- Current status
- Span loss for both the sides
- (Optional) OTDR, OSC, and PPC information is displayed when available

The **Display Neighbors** tab displays the list of optional neighbors of the components of the node. The following information is displayed for each side:

- Name of the side
- Neighbor node
- At Degree

Step 5 View the **Circuit List** tab that displays the list of all the circuits present in the side.

View Details of Side

Use this task to view the details of the side in NFV.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Right-click a side in the map view and choose **View Details** to view the details of the selected side along with the right shoulder.

Step 3 View the following information that is displayed in the right shoulder. Optional means that the information is displayed when available.

- Name of the side
- Overall alarm status as a colored label and an icon
- (Optional) Span loss

- (Optional) ORL of OTDR
- (Optional) Fiber End of OTDR
- (Optional) OSC power
- (Optional) IP address of the node of its optional neighbor. To open the SVO web UI of the neighbor node in a new browser tab, click the IP address of the neighbor node.
- Degree of its optional neighbor
- **Card List** tab - Displays the list of all the cards present in the side. The shelf number and slot number are displayed with the card name. The trunk port number is also displayed for TXP cards.

  To sort the list of cards, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.
- **Circuit List** tab - Displays the list of all the circuits present in the side.

  To sort the list of circuits, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.

View Details of Side for OLA Node

Use this task to view the details of the side for OLA node in NFV.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Right-click a side in the map view and choose **View Details** to view the details of the selected side along with the right shoulder.

Or

Click the arrow near the side name that is displayed inside the right shoulder.

Step 3 View Side 1 and Side 2 merged information that is displayed in the right shoulder. Optional means that the information is displayed when available.

- Overall alarm status as a colored label and an icon
- (Optional) Span loss
- (Optional) ORL of OTDR
- (Optional) Fiber End of OTDR

- (Optional) OSC power
- (Optional) IP address of the node of its optional neighbor. To open the SVO web UI of the neighbor node in a new browser tab, click the IP address of the neighbor node.
- Degree of its optional neighbor
- **Card List** tab - Displays the list of all the cards present in both sides. The shelf number and slot number are displayed with the card name. The trunk port number is also displayed for TXP cards.

  To sort the list of cards, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.
- **Circuit List** tab - Displays the list of all the circuits present in the side.

  To sort the list of circuits, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.

View Details of Card

Use this task to view the details of the card in NFV.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Right-click a side in the map view and choose **Open**.

Step 3 Right-click a card in the map view and choose **View Details**.

Step 4 View the following information that is displayed in the right shoulder:

- Name of the card
- Overall alarm status as a colored label and an icon
- **Port List** tab - Displays the list of all the ports with their aggregate power.

  To sort the list of ports, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.
- **Circuit List** tab: Displays the list of all the circuits present in the card.

  To sort the list of circuits, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.

View Details of Port

Use this task to view the details of the port in NFV.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Right-click a side in the map view and choose **Open**.

Step 3 Right-click a card in the map view and choose **Open**.

Step 4 Click the port name in the map view.

Step 5 View the following information that is displayed in the right shoulder:

- Name of the port
- Overall alarm status as a colored label and an icon
- **Agg. Powers** tab - Displays the list of all the links with their aggregate power.

  The aggregate power displays the current power in case of a single port. The aggregate power displays a list of all the different power levels in case of an MPO port or logical group.

  To sort the list of links, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Setpoint**, or **Low Setpoint**.
- **Circuit List** tab: Displays the list of all the circuits present in the port.

  To sort the list of circuits, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.

View Details of Patch Cord

Use this task to view the details of the patch cord in NFV.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Click the patch cord in the map view.

Step 3 View the following information that is displayed in the right shoulder:

- Type of the patch cord
- Status of the patch cord as a colored label and an icon
- **Connections** tab - Displays the ports that the patch cord connects with their cards and the aggregate power.

  To sort the list of patch cords, click the vertical ellipsis icon and choose **A-Z**, **Z-A**, **High Severity**, or **Low Severity**.

View Details of Circuit

Use this task to view the details of the circuit in NFV.

Circuits are created in EPNM and displayed as read-only in the **Optical Cross Connections** tab.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Click **Show/Hide Shoulder** to open the right shoulder.

Step 3 Click > against the circuit in the right shoulder to view the sides that are involved in the circuit in graphical view.

Step 4 View the following information that is displayed in the right shoulder:

- **Circuit Info** pane - Displays information on **Admin State**, **Frequency**, **From Degree**, and **To Degree**.
- **Path (Forward path)** pane - Click **:** next to the Path (Forward Path) pane and choose **Forward path**, **Backwards path**, or **Both paths** to specify the order of display of internal links. The pane name changes correspondingly.

Set User Preferences

Use this task to set the user preferences in NFV. The user preferences are stored in the local storage of the browser and are retained for that browser.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

The Node Functional View page appears.

Step 2 Click the **User Settings** icon.

The **Preferences** dialog box appears.

Step 3 From the **shoulder element order** drop-down list, choose **A-Z**, **Z-A**, **Low Severity**, or **High Severity** to sort the components in the right shoulder based on name and alarm severity.

Step 4 Enter a value in the **Layers spacing** field to set the horizontal distance between the components in the map view.

Refresh the browser to apply this value.

Step 5 Enter a value in the **Column spacing** field to set the vertical distance between the components in the map view.

Refresh the browser to apply this value.

Step 6 Enter the zoom scale value in the **Zoom scaling factor** field.

Step 7 From the **Circuit path sorting** drop-down list, choose **Forward path**, **Backward path**, or **Both paths** to set the link path between source and destination.

Step 8 Enter a value in the **Rack opacity factor** field to highlight the cards of interest in physical view. The other cards are covered by overlay with transparency depending on the value provided.

The range is from 0 to 1.

Step 9 Enter the value in the **Left shoulder width (px)** field to set the width of the left shoulder.

The range is from 400 to 600.

Step 10 Check the **Show only visible cards on the rack** check box to display only the visible cards in the rack view.

Step 11 Check the **Always display details** check box to automatically display the right shoulder upon opening NFV.

Step 12 Click **Apply** to apply the user settings.

Step 13 Click **Reset** to reset the user settings to default values.

Active Circuit Count

Table 111: Feature History

Feature Name	Release Information	Feature Description
Display the Number of Active Circuits	Cisco NCS 2000 Release 12.3.1	You can now view the total number of active circuits passing through a particular card on a degree. The active circuit count is visible on the **Node Functional View** window of the SVO Web User Interface.

Display Active Circuit List

Use this task to view the total number of circuits passing through a degree and a selected card.

Before you begin

- Log into the SVO Web Interface, on page 67

Procedure

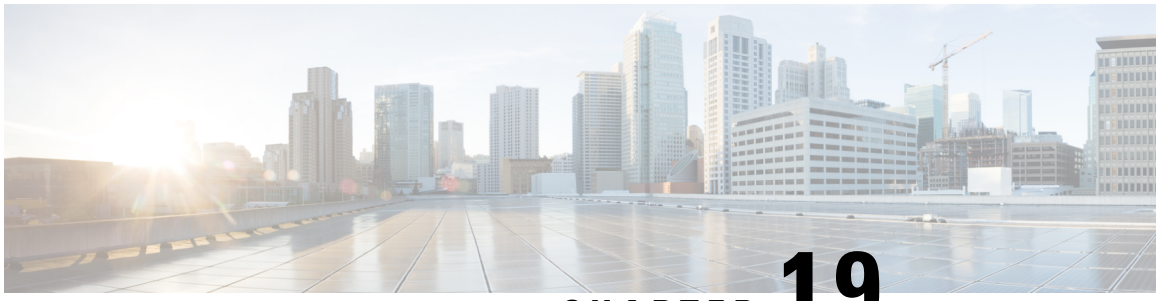
Step 1 Click the hamburger icon at the top-left of the page, and select **Node Functional View**.

Step 2 Select and right click **Degree**. Click Open.

In the right side pane, you can see the total number of circuits passing through the degree under **Circuit List**.

Step 3 Select and right click the card. Click Open.

In the right side pane, you can see the total number of circuits passing through the card under **Circuit List**.



CHAPTER 19

Monitor Performance

This chapter describes the Performance Monitoring (PM) parameters used in Cisco NCS 2000 SVO and its related tasks.

Note We recommend that you use either single EPNM session in standalone mode or EPNM with two servers in high availability mode. A single PM monitoring session is recommended either through EPNM, TL1, or SNMP.

Threshold Performance Monitoring

Thresholds are used to set error levels for each PM parameter.

During the accumulation cycle, if the current value of a PM parameter reaches or exceeds its corresponding threshold value, the PM details are highlighted with NA or with a change of color for the bucket. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If zero is entered as the threshold value, generation of TCAs is disabled but performance monitoring continues. PM parameters are used by service providers to gather, store, set thresholds, and report performance data for early detection of problems.

From 12.3.1 onwards, TCA is supported on the NCS 2002 chassis.

Performance Monitoring

The Performance tab displays the PM parameters.

Performance Monitoring Tab

The Performance Monitoring tab consists of:

- The **Refresh** icon manually refreshes the PM parameter values on the table.
- The **Auto-Refresh** drop-down list automatically refreshes the PM parameter values on the table based on the selected time interval. The auto-refresh can be set for several intervals ranging from 15 seconds to 5 minutes.
- The **Interval** drop-down list helps the user set a time interval at which the data would be split to be shown in the table. The two interval options that the user can choose to display the data are 15 minutes or one day.
- The **Interface Type** drop-down list helps the user choose the interface type of the card. The options available are based on the selected card.
- The **Interface** drop-down list helps the user choose the port of the card. The options available are based on the selected card.
- The **Direction** drop-down list helps the user choose the direction of path. The user can choose from one of two options: nearEnd and farEnd.
- The **Clear PM** button sets the PM parameter values on the card to zero. All counters on the card are cleared.

Interface Types

You have one of five options to choose from the interface type drop-down list: EthernetCsmacd, optical channel, OTNOdu, OTNOtu, and OpticalTransport.

Optical Channel PM

The Optical Channel PM lists parameters at the trunk and client side for all optical and control OPT-AMP-C, PSM, 400G-XP, MR-MXP, TNC, TNCE, TNCS, TNCS-O, TNCS-2, TNCS-2O cards.

The parameters for the Optical channel are as shown in the following table:

Table 112: Optical Channel PM Parameters

Trunk-Side/Client-Side Optical Channel PM Parameters	Definition
Laser Bias (Avg, %)	Average Laser Bias Current (Laser Bias Avg) is the average percentage of laser bias current during the PM time interval.
Laser Bias (Max,%)	Maximum Laser Bias Current (Laser Bias Max) is the maximum percentage of laser bias current during the PM time interval.
Laser Bias (Min,%)	Minimum Laser Bias Current (Laser Bias Min) is the minimum percentage of laser bias current during the PM time interval.

Link Status	Indicates if the Fibre Channel link is receiving a valid Fibre Channel signal (carrier) from the attached Fibre Channel device. Up indicates present, and down indicates not present.
Rx Optical Pwr (Min,dBm)	Minimum Receive Optical Power (Rx Optical Pwr Min, dBm) is the minimum received optical power during the PM time interval.
Rx Optical Pwr (Avg,dBm)	Average Receive Optical Power (Rx Optical Pwr Avg, dBm) is the average received optical power during the PM time interval.
Rx Optical Pwr (Max,dBm)	Maximum Receive Optical Power (Rx Optical Pwr Max, dBm) is the maximum received optical power during the PM time interval.
Tx Optical Pwr (Min,dBm)	Minimum Transmit Optical Power (Tx Optical Pwr Min, dBm) is the minimum optical power transmitted during the PM time interval.
Tx Optical Pwr (Avg,dBm)	Average Transmit Optical Power (Tx Optical Pwr Avg, dBm) is the average optical power transmitted during the PM time interval.
Tx Optical Pwr (Max,dBm)	Maximum Transmit Optical Power (Tx Optical Pwr Max, dBm) is the maximum optical power transmitted during the PM time interval.
CD (Min,ps/nm)	Minimum Chromatic Dispersion (CD Min, ps/nm) is the minimum chromatic dispersion during the PM time interval. Not supported on 10x10G-LC card.
CD (Avg,ps/nm)	Average Chromatic Dispersion (CD Avg, ps/nm) is the average chromatic dispersion during the PM time interval. Not supported on 10x10G-LC card.
CD (Max,ps/nm)	Maximum Chromatic Dispersion (CD Max, ps/nm) is the maximum chromatic dispersion during the PM time interval.
OSNR (Min,dB)	Minimum Optical Signal to Noise Ratio (OSNR Min, dB) is the minimum optical signal to noise ratio during the PM time interval.
OSNR (Avg,dB)	Average Optical Signal to Noise Ratio (OSNR Avg, dB) is the average optical signal to noise ratio during the PM time interval.
OSNR (Max,dB)	Maximum Optical Signal to Noise Ratio (OSNR Max, dB) is the maximum optical signal to noise ratio during the PM time interval.
PMD (Min,ps)	Minimum Polarization Mode Dispersion (PMD Min, ps) is the minimum polarization mode dispersion during the PM time interval. Not supported on 400G-XP and 10x10G-LC cards.
PMD (Avg,ps)	Average Polarization Mode Dispersion (PMD Avg, ps) is the average polarization mode dispersion during the PM time interval. Not supported on 400G-XP and 10x10G-LC cards.

PMD (Max,ps)	Maximum Polarization Mode Dispersion (PMD Max, ps) is the maximum polarization mode dispersion during the PM time interval. Not supported on 400G-XP and 10x10G-LC cards.
SOPMD (Min,ps^2)	Minimum Second-order Polarization Mode Dispersion (SOPMD Min,ps^2) is the minimum second-order polarization mode dispersion during the PM time interval. Not supported on 10x10G-LC card.
SOPMD (Avg,ps^2)	Average Second-order Polarization Mode Dispersion (SOPMD Avg,ps^2) is the average second-order polarization mode dispersion during the PM time interval. Not supported on 10x10G-LC card.
SOPMD (Max,ps^2)	Maximum Second-order Polarization Mode Dispersion (SOPMD Max,ps^2) is the maximum second-order polarization mode dispersion during the PM time interval. Not supported on 10x10G-LC card.
PCR (Min,10*rad/s)	Minimum Polarization Change Rate (PCR Min,10*rad/s) is the minimum polarization change rate during the PM time interval. Not supported on 400G-XP and 10x10G-LC cards.
PCR (Avg,10*rad/s)	Average Polarization Change Rate (PCR Avg,10*rad/s) is the average polarization change rate during the PM time interval. Not supported on 400G-XP and 10x10G-LC cards.
PCR (Max,10*rad/s)	Maximum Polarization Change Rate (PCR Max,10*rad/s) is the maximum polarization change rate during the PM time interval. Not supported on 400G-XP and 10x10G-LC cards.
PDL (Min,dB)	Minimum Polarization Dependent Loss (PDL Min,dB) is the minimum polarization dependent loss during the PM time interval. Not supported on 10x10G-LC card.
PDL (Avg,dB)	Average Polarization Dependent Loss (PDL Avg,dB) is the average polarization dependent loss during the PM time interval. Not supported on 10x10G-LC card.
PDL (Max,dB)	Maximum Polarization Dependent Loss (PDL Avg,dB) is the maximum polarization dependent loss during the PM time interval. Not supported on 10x10G-LC card.

SDH PM

The SDH PM pane lists parameters at the trunk and client side for all optical and control 40E-MXP, 400G-XP, and OTU2-XP cards.

The parameters for the SDH PM channel are as shown in the following table:

Table 113: SDH PM Parameters

Parameter	Definition
MS-BBE	Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an SES.
MS-BBER	Multiplex Section Background Block Error Ratio (MS-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
MS-EB	Multiplex Section Errored Block (MS-EB) indicates that one or more bits are in error within a block.
MS-ES	Multiplex Section Errored Second (MS-ES) is a one-second period with one or more errored blocks or at least one defect.
MS-ESR	Multiplex Section Errored Second Ratio (MS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
MS-SES	Multiplex Section Severely Errored Second (MS-SES) is a one-second period that contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES. For more information, refer to ITU-T G.829 Section 5.1.3.
MS-SESR	Multiplex Section Severely Errored Second ratio (MS-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
MS-UAS	Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as MS-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as MS-SESs. When the condition is entered, MS-SESs decrement and then count toward MS-UAS.
RS-BBE	Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of an SES.
RS-BBER	Regenerator Section Background Block Error Ratio (RS-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

RS-EB	Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within a block.
RS-ES	Regenerator Section Errored Second (RS-ES) is a one-second period with one or more errored blocks or at least one defect.
RS-ESR	Regenerator Section Errored Second Ratio (RS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
RS-SES	Regenerator Section Severely Errored Second (RS-SES) is a one-second period which contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES.
RS-SESR	Regenerator Section Severely Errored Second Ratio (RS-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
RS-UAS	Regenerator Section Unavailable Second (RS-UAS) is a count of the seconds when the regenerator section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as RS-UASs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as RS-UASs.

SONET PM

The SONET PM pane lists parameters at the trunk and client side for all optical and control 40E-MXP, 400G-XP, OTU2-XP, and 10x10G-LC cards.

The parameters for the SONET PM channel are as shown in the following table:

Table 114: SONET PM Parameters

Parameter	Definition
CV-L	Line Coding Violation (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
CV-S	Section Coding Violation (CV-S) is a count of bit interleaved parity (BIP) errors detected at the section layer (that is, using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register.

ES-L	Line Errored Seconds (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (that is, loss of signal) on the line.
S_ES-S	Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer BIP error was detected or an SEF or loss of signal (LOS) defect was present.
S_SEFS-S	Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when an SEF defect was present. An SEF defect is expected to be present during most seconds when an LOS or loss of frame (LOF) defect is present. However, there can be situations when the SEFS-S parameter is only incremented based on the presence of the SEF defect. **Note** The RTRV-PM-<MOD2> command does not retrieve SEFS counter for OC192/STM64 payloads on ADM-10G, 40G/40E (TXP/MXP), and OTU2-XP cards.
S_SES-S	Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see Telcordia GR-253 for value) or more section-layer BIP errors were detected or an SEF or LOS defect was present.
SES-L	Line Severely Errored Seconds (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ > 44) and/or defects on the line
UAS-L	Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable. A line becomes unavailable when ten consecutive seconds occur that qualify as SES-Ls, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ls.

OTNOdu/ OTNOtu PM

The OTNOdu and OTNOtu PM pane lists parameters at the trunk and client side for all optical and control 400G-XP, 200G-CK-C, 100G-CK-C, 100GS-CK-C, TNC, TNCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O cards.

The parameters for the OTNOdu/OTNOtu PM channel are as shown in the following table:

Table 115: OTBOdu/OTNOtu PM Parameters

Parameter	Definition

BBE-SM	Section Monitoring Background Block Errors (BBE-SM) shows the number of background block errors recorded in the OTN section during the PM time interval.
BBER-SM	Section Monitoring Background Block Errors Ratio (BBER-SM) shows the background block errors ratio recorded in the OTN path during the PM time interval.
ES-SM	Section Monitoring Errored Seconds (ES-SM) shows the errored seconds recorded in the OTN section during the PM time interval.
ESR-SM	Section Monitoring Errored Seconds Ratio (ESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval.
FC-SM	Section Monitoring Failure Counts (FC-SM) shows the failure counts recorded in the OTN section during the PM time interval.
SES-SM	Section Monitoring Severely Errored Seconds (SES-SM) shows the severely errored seconds recorded in the OTN section during the PM time interval.
SESR-SM	Section Monitoring Severely Errored Seconds Ratio (SESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval.
UAS-SM	Section Monitoring Unavailable Seconds (UAS-SM) shows the unavailable seconds recorded in the OTN section during the PM time interval.

Ethernet PM

The SVO provides Ethernet port performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics.

The parameters for the Ethernet PM channel are as shown in the following table:

Table 116: Ethernet Statistics Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the previous time statistics were reset.
ifInOctets	Number of bytes received since the last counter reset.
rxTotalPks	Number of received packets.

Parameter	Definition
ifInUcastPkts	Number of unicast packets received since the last counter reset.
ifInMulticastPkts	Number of multicast packets received since the last counter reset.
ifInDiscards	The number of inbound packets that are chosen to be discarded even though no errors are detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet is to free buffer space.
ifOutOctets	Number of bytes transmitted since the last counter reset.
txTotalPkts	Number of transmitted packets.
ifOutMulticastPkts	Number of multicast packets transmitted.
ifOutBroadcastPkts	Number of broadcast packets transmitted.
ifOutDiscards	Number of outbound packets that are chosen to be discarded even though no errors are detected to prevent their transmission. A possible reason for discarding such packets is to free up buffer space.
ifOurErrors	Number of outbound packets or transmission units that cannot be transmitted because of errors.
dot3StatsAlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsFrameTooLong	A count of frames received on a particular interface that exceed the maximum permitted frame size.
etherStatsUndersizePkts	The total number of packets received that are less than 64 octets long (excluding framing bits, but including FCS octets) and are otherwise well formed.
etherStatsFragments	The total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
etherStatsPkts64Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).

Parameter	Definition
etherStatsPkts65to127Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts128to255Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts256to511Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts512to1023Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518Octets	The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsBroadcastPkts	The total number of good packets received that are directed to the broadcast address. Note that this does not include multicast packets.
etherStatsMulticastPkts	The total number of good packets received that are directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
etherStatsOversizePkts	The total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets) and are otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.
etherStatsJabbers	The total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets), and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets.

Parameter	Definition
etherStatsCRCAlignErrors	The total number of packets received that has a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).

ITU G.709 Threshold PM

The ITU G.709 section monitoring trunk-side PM parameters are shown in the following table.

Table 117: ITU G.709 Section Monitoring PM Definitions

Paramaters	Definition
BBE-SM	Section Monitoring Background Block Errors (BBE-SM) shows the number of background block errors recorded in the OTN section during the PM time interval.
BBER-SM	Section Monitoring Background Block Errors Ratio (BBER-SM) shows the background block errors ratio recorded in the OTN path during the PM time interval.
ES-SM	Section Monitoring Errored Seconds (ES-SM) shows the errored seconds recorded in the OTN section during the PM time interval.
ESR-SM	Section Monitoring Errored Seconds Ratio (ESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval.
FC-SM	Section Monitoring Failure Counts (FC-SM) shows the failure counts recorded in the OTN section during the PM time interval.
SES-SM	Section Monitoring Severely Errored Seconds (SES-SM) shows the severely errored seconds recorded in the OTN section during the PM time interval.
SESR-SM	Section Monitoring Severely Errored Seconds Ratio (SESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval.
UAS-SM	Section Monitoring Unavailable Seconds (UAS-SM) shows the unavailable seconds recorded in the OTN section during the PM time interval.

The ITU G.709 path monitoring trunk-side PM parameters are shown in the following table.

Table 118: TU G.709 Path Monitoring PM Definitions

Parameter	Defintion
BBE-PM	Path Monitoring Background Block Errors (BBE-PM) shows the number of background block errors recorded in the OTN path during the PM time interval.
BBER-PM	Path Monitoring Background Block Errors Ratio (BBER-PM) shows the background block errors ratio recorded in the OTN path during the PM time interval.
ES-PM	Path Monitoring Errored Seconds (ES-PM) shows the errored seconds recorded in the OTN path during the PM time interval.
ESR-PM	Path Monitoring Errored Seconds Ratio (ESR-PM) shows the severely errored seconds ratio recorded in the OTN path during the PM time interval.
FC-PM	Path Monitoring Failure Counts (FC-PM) shows the failure counts recorded in the OTN path during the PM time interval.
SES-PM	Path Monitoring Severely Errored Seconds (SES-PM) shows the severely errored seconds recorded in the OTN path during the PM time interval.
SESR-PM	Path Monitoring Severely Errored Seconds Ratio (SESR-PM) shows the severely errored seconds ratio recorded in the OTN path during the PM time interval.
UAS-PM	Path Monitoring Unavailable Seconds (UAS-PM) shows the unavailable seconds recorded in the OTN path during the PM time interval.

FEC Threshold PM

The 100G-LC-C, 100GS-CK-LC , 200G-CK-LC, and 100G-CK-C card FEC PM parameters are shown in the following table.

Table 119:

Parameter	Definition
Bit Errors	Bit Errors are the number of bit errors corrected.
FEC (NE)	FEC enables correction and detection of errors along the optical links where OTN and FEC are provisioned. FEC uses Reed Solomon code RS (255,239) encoding. The FEC field is found in Rows 1 to 4 and Columns 3835 to 4080. It contains either the Reed-Solomon RS(255,239) codes, or if FEC is disabled, fixed stuff bytes (zeros).

Parameter	Definition
UNC-Words	Uncorrectable Words (UNC-Words) occur when FEC detects and corrects errors to deliver a 7 to 8 dB improvement in the signal-to-noise ratio (also called margin). For ITU G.709, the FEC code used is Reed-Solomon RS (255, 239).

RMON PM

The 100G-LC-C, 100G-CK-C, 100GS-CK-LC , 200G-CK-LC, and 10x10G-LC full RMON statistics PM parameters are shown in the following table.

Table 120: RMON PM Definitions

Parameter	Definition
dot3StatsFCSErrors	The number of frames with frame check errors.
dot3StatsFrameTooLong	The number of packets at least 64 octets long, without a bad Frame Check Sequence (FCS), where the 802.3 length or type field does not match the computed DATA field length.
etherStatsBroadcastPkts	The number of broadcast packets, excluding multicast packets, that are 64-16376 octets in length, and have a valid FCS.
etherStatsCRCAlignErrors	The number of packets that are 64-1518 octets in length without an integral number of octets, or with a bad FCS.
etherStatsFragments	The number of packets less than 64 octets long that do not have an integral number of octets or that have a bad FCS.
etherStatsJabbers	The number of octets of data, including bad packets, that are received on the network.
etherStatsMulticastPkts	The number of multicast packets, excluding broadcast packets, that are 64-16376 octets in length, and have a valid FCS.
etherStatsOctets	The number in bytes of received packets, including bad packets and excluding framing bits except for FCS bytes.
etherStatsOversizePkts	The number of packets more than 16376 octets long that have a valid FCS.
etherStatsPkts64Octets	The number of packet received, including error packets, that are 64 octets in length.
etherStatsPkts65to127Octets	The number of packets received, including error packets, that are 65-127 octets in length.

Parameter	Definition
etherStatsPkts128to255Octets	The number of packets received, including error packets, that are 128-255 octets in length.
etherStatsPkts256to511Octets	The number of packets received, including error packets, that are 256-511 octets in length.
etherStatsPkts512to1023Octets	The number of packets received, including error packets, that are 512-1023 octets in length.
etherStatsPkts1024to1518Octets	The number of packets received, including error packets, that are 1024-1518 octets in length.
etherStatsUndersizePkts	The number of packets less than 64 octets long that have a valid FCS.
fcStatsLinkRecoveries	The number of link recoveries.
fcStatsRxCredits	The number of current receive buffer to buffer credits.
fcStatsTxCredits	The number of current transmit buffer to buffer credits.
fcStatsZeroTxCredits	This is a count that increments when the FC/FICON Tx credits go from a nonzero value to zero.
gfpStatsLFDRaised	The number of loss of frame delineation (LFD) raised.
gfpStatsRoundTripLatencyUSe	Round trip delay for the end-to-end Fibre Channel transport in microseconds.
gfpStatsRxCRCErrors	The number of packets received with a payload FCS error.
gfpStatsRxCSFRaised	Received GFP loss of client character synchronization (LOCCS).
gfpStatsRxDistanceExtBuffers	The number of receive buffer credit for GFP-T (valid only if distance extension is enabled)
gfpStatsRxMBitErrors	The received multibit errored core header count (cHEC).
gfpStatsRxSBitErrors	The received single-bit errored cHEC.
gfpStatsRxSblkCRCErrors	The number of packets received with a payload FCS error. Sblk stands for super block in the GFP payload.
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when we expect Fibre Channel data.
gfpStatsTxDistanceExtBuffers	The number of transmit buffer credit for GFP-T (valid only if distance extension is enabled).
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which are not addressed to a multicast or broadcast address at this sub-layer.

Parameter	Definition
ifInMulticastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which are addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses.
ifInBroadcastPkts	The number of packets delivered to a higher sublayer and addressed to a broadcast address at this sublayer.
ifInDiscards	The number of inbound packets that are chosen to be discarded even though no errors are detected, to prevent them from being deliverable to a higher-layer protocol. One possible reason for discarding such a packet is to free buffer space.
ifInErrors	The number of inbound packets (or transmission units) that contain errors preventing them from being delivered to a higher-layer protocol.
ifInErrorBytePkts	The number of received packets with an error symbol detected.
ifInFramingErrorPkts	The number of received packets with a control symbol other than an error detected.
ifInJunkInterPkts	The number of interpacket gaps between valid start symbols during which a symbol other than idle is detected, including packets of length 1-8 octets.
ifInMulticastPkts	The total number of multicast frames received error-free.
ifInOctets	The number of bytes received since the last counter reset.
ifOutBroadcastPkts	The number of packets requested by higher-level protocols and addressed to a broadcast address at this sublayer, including those not transmitted.
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free buffer space.
ifOutMulticastPkts	The number of multicast frames transmitted error-free.
ifOutOctets	The number of bytes transmitted since the last counter reset.
InvalidCRCError	A count of invalid cyclic redundancy checks (CRCs).
mediaIndStatsRxFramesBadCRC	The number of received frames with a CRC error.
mediaIndStatsRxFramesTooLong	The number of received frames that are too long.

Parameter	Definition
Running Disparity Count	A count of errors that affect the disparity of the received data stream.
rxControlFrames	The number of MAC control packets that are type 0x8808 and contain at least 64 octets in length.
rxFrames	count of the number of frames received without errors.
rxLinkReset (Only for FC Mode)	A count of the received link resets.
rxPauseFrames	The number of received 802.x paused frames.
rxTotalPkts	The number of received packets.
rxUnknownOpcodeFrames	Number of packets of at least 64 octets in length ad type 0x8808, with opcode not equal to 1.
Time Last Cleared	A time stamp indicating the previous time statistics were reset.
txBytes	A count of the number of bytes transmitted from the frame since the last counter reset.
txFrames	A count of the number of transmitted frames.
txTotalPkts	The number of transmitted packets.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsFrameTooLong	A count of frames received on a particular interface that exceed the maximum permitted frame size.
dot3StatsInPauseFrames	A count of frames received on this interface with an opcode indicating the PAUSE operation.
dot3StatsOutPauseFrames	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.
etherStatsUndersizePkts	The total number of packets received that are less than 64 octets long (excluding framing bits, but including FCS octets and are otherwise well formed.
medialndStatsTxFramesTooLong	Total number of transmitted data frames that are less than 5 bytes. This value is a part of HDLC and GFP port statistics.
medialndStatsTxFramesTruncated	Number of transmitted data frames that exceed the MTU. This value is part of HDLC and GFP port statistics.
pcs49RxErrBer	Total number of 125uSec periods where BER is detected. BER is a condition where one or more errors are detected or counted on the PCS layer.

Parameter	Definition
pcs49RxErrDec	Total number of invalid blocks received. 64 bits of data are transmitted as 66-bit code blocks on the PHY layer with the 64-bit or 66-bit encoder or decoder. The 66-bit code block has an initial 2-bit Sync Header, that can assume only the values 01 (data only) or 10 (data or control). The block is counted as invalid if the Sync Header bits assume invalid values.
gfpStatsRxFrame	Total number of received data frames.
gfpStatsTxFrame	Total number of transmitted data frames.
gfpStatsRxOctets	Total number of GFP data octets received.
gfpStatsTxOctets	Total number of GFP data octets transmitted.
gfpRxCmfFrame	—
gfpTxCmfFrame	—

Performance Monitoring of SVO Card

This section lists the PM parameters that are supported by the SVO card.

Ethernet Counter PM

The Ethernet Counter PM tab lists the Ethernet counter parameters for the SVO card.

Table 121:

Parameter	Definition
goodOctetsRcv	Number of Ethernet frames received that are not bad Ethernet frames or MAC control packets.
pkts128to255Octets	Total number of received and transmitted undamaged and damaged frames that are 128 to 255 bytes in size. This does not include MAC control frames.
brdcPktsSent	Total number of good packets sent that have a broadcast destination MAC address. This does not include 802.3 flow control packets, packets dropped due to excessive collision, or packets with a Tx error.
jabberPkts	Number of jabber packets received.
badOctetsRcv	Sum of lengths of all the bad Ethernet frames received.

Parameter	Definition
pkts256to511Octets	Total number of received and transmitted undamaged and damaged frames that are 256 to 511 bytes in size. This does not include MAC control frames.
fcSent	Number of flow control frames sent.
macRcvError	Number of Rx error events seen by the receive side of the MAC address.
macTransmitErr	Number of frames not transmitted correctly or dropped due to internal MAC Tx error.
pkts512to1023Octets	Total number of received and transmitted undamaged and damaged frames which are 512 to 1023 bytes in size. This does not include MAC control frames.
goodFcRcv	Number of good flow control frames received.
badCrc	Number of CRC error events.
brdcPktsRcv	Total number of undamaged packets received that are directed to the broadcast address.
pkts1024toMaxOctets	Total number of received and transmitted undamaged and damaged frames that are more than 1024 bytes in size. This does not include MAC control frames.
dropEvents	Number of instances that the port are unable to receive packets due to insufficient bandwidth.
collisions	Total number of collisions seen by the MAC address.
mcPktsRcv	Total number of undamaged packets received that are directed to a multicast address.
goodOctetsSent	Sum of lengths of all the good Ethernet frames sent from this MAC address. This does not include 802.3 flow control packets, packets dropped due to excessive collision, or packets with a Tx error.
undersizePkts	Number of undersize packets received.
lateCollisions	Total number of late collisions seen by the MAC address.
pkts64Octets	Total number of received and transmitted undamaged and damaged frames that are 64 bytes in size. This does not include MAC control frames.
excessiveCollisions	Number of frames dropped in the transmit MAC address due to excessive collisions.
fragmentsPkts	Number of fragments received.

Parameter	Definition
ucPktsSent	Number of good frames sent that have a unicast destination MAC address.
pkts65to127Octets	Total number of received and transmitted undamaged and damaged frames that are 65 to 127 bytes in size. This does not include MAC control frames.
mcPktsSent	Total number of good packets sent that have a multicast destination MAC address. This does not include 802.3 flow control packets, packets dropped due to excessive collision, or packets with a Tx error.
oversizePkts	Number of oversize packets received.

Optics PM

The Optics PM tab lists the optics PM parameters for the SVO card.

Table 122: Optics PM Parameters

Optics PM Parameters	Definition
Laser Bias (%)	Laser Bias (Laser Bias) is the percentage of laser bias optical during the PM time interval.
Rx Power (dBm)	Receive Power (Rx Pwer dBm) is the received optical power during the PM time interval.
Tx Power (dBm)	Transmit Power (Tx Power dBm) is the transmitted optical power during the PM time interval.

Sensor Data PM

A temperature sensor helps the user manage the system and diagnoses malfunctions. The temperature is measured in degrees of Celsius, and it can be negative. There are several temperature sensors available in the device. The device raises an interrupt when the temperature exceeds a certain threshold.

View PM Parameters

Use this task to view the current and historical PM counts of a card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Performance** > **Performance Monitoring** tabs.

You can view the parameter names in the **Parameter** column and the corresponding PM values in the **Current Reading** and **Prev-n** (previous) columns.

Step 2 Select the **Interval**, **Interface Type**, **Interface**, and **Direction** from their respective drop-down lists.

Note The options available are based on the card that is selected.

Step 3 Click **Refresh**.

The values are displayed in the table. If a complete count for the specified interval is not possible, the value appears against a yellow background. An incomplete or incorrect count can be caused by monitoring for less than the specified interval after the counter starts, replacing a card, resetting a card, or changing port service states. When the problem is corrected, the subsequent specified interval appears against a white background.

Step 4 (Optional) If you want to set an auto-refresh interval, select a value from the **Auto Refresh** drop-down list.

Depending on the selected autorefresh interval, the displayed PM counts automatically update when each refresh interval completes. When the autorefresh interval is set, the **Refresh** button is automatically disabled. If the autorefresh interval is set to None, the PM counts that appear are not updated unless you click **Refresh**.

Step 5 (Optional) To clear the current reading values, click **Clear PM**.

A confirmation message is displayed. Click **Confirm** to proceed.

View Live Data

The **Live Data** tab displays the instantaneous PM parameters for a card. These details can be used for troubleshooting. Use this task to view the instantaneous PM counts of a card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Maintenance** > **Live Data** tabs.

You can view the parameter names in the **Parameter** column and the corresponding PM values in the **Current Reading** column.

Step 2 Select the **Interface Type** and **Interface** from their respective drop-down lists.

Note The options available are based on the card that is selected.

The values are displayed in the table.

Step 3 Click **Refresh** to see the latest PM counts.

Step 4 (Optional) If you want to set an autorefresh interval, select a value from the **Auto Refresh** drop-down list.

Depending on the selected autorefresh interval, the displayed PM counts automatically update when each refresh interval completes. When the autorefresh interval is set, the **Refresh** button is automatically disabled. If the autorefresh interval is set to None, the PM counts that appear are not updated unless you click **Refresh**.

View PM Parameters of SVO Card

Use this task to view the PM counts of the SVO card.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

Procedure

Step 1 Click the **Performance** tab.

Step 2 Perform these steps, as needed.

a) To view the ethernet counter PM parameters, perform these steps:

1. Click the **Ethernet Counter** tab.
2. From the drop-down list, choose a specific port or **ALL**.
3. Click **Refresh** to view the updated PM values.
4. (Optional) To clear the current reading values, click **Clear**.

   A confirmation message appears.
5. Click **Confirm** to proceed.

b) To view the sensor data PM parameters, perform these steps:

1. Click the **Sensor Data** tab.
2. Click **Refresh** to view the updated PM values.

c) To view the Optics PM parameters, perform these steps:

1. Click the **Optics PM** tab.
2. Click **Refresh** to view the updated PM values.

Export PM Data of SVO Card

Table 123: Feature History

Feature Name	Release Information	Feature Description
Export PM Data for SVO Card	Cisco NCS 2000 Release 12.3.1	From this release onwards, you can download the complete PM data for an SVO card through the SVO Web User Interface. This data can be used offline for device monitoring. The downloaded data is in an Excel format and is collated for the past 15 minutes and 1-day time duration. This feature eliminates the need for individually accessing data for each PM parameter separately.

Export PM Data of SVO Card

Use this task to export the complete PM data for the SVO card. The PM data will be downloaded as an Excel sheet in your system after performing the following steps.

Before you begin

- Log into the SVO Web Interface, on page 67
- Open the Card View, on page 70

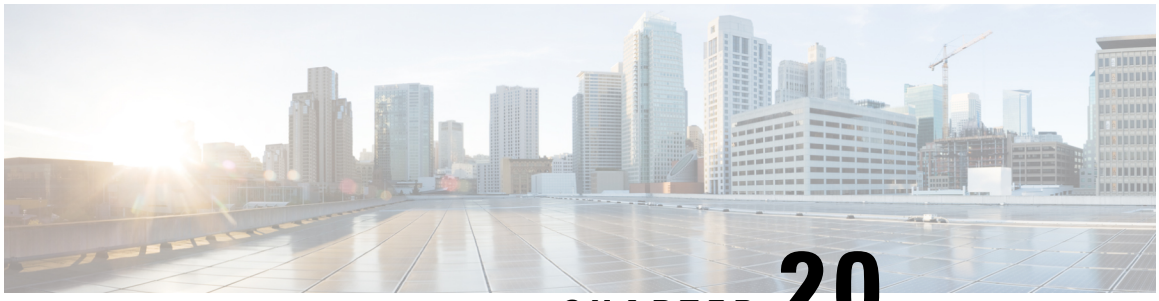
Procedure

Step 1 Click the **Performance** > **Performance Monitoring** tabs.

Step 2 Click **Export to Excel with nested data**.

The Excel sheet contains complete PM data for all the ports and interface type showing current and previous readings for the SVO card.

Note The downloaded Excel sheet contains PM data for 15 minutes and 1-day interval.



CHAPTER 20

Upgrade Software

Table 124: Feature History

Feature Name	Release Information	Feature Description
Card Controller Software Package	Cisco NCS 2000 Release 12.3	Card Controller software package includes all packages specific to the SVO card.

Feature Name	Release Information	Feature Description
Software Upgrade Enhancements	Cisco NCS 2000 Release 12.3.1	The following Software Upgrade enhancements are done: • The software repository capacity is increased to maintain up to eight Download Software Package. The **Software Packages** tab lists the packages and their contents. This feature improves the installation process by making more packages readily available for activation. • The operating system of the SVO device can be remotely upgraded from the **Device Software** tab. This eliminates the need to perform an on-site operating system upgrade of the SVO device. • An "Active session" label is displayed against the SVO card in the **Device Software** tab to indicate that it is running the active SVO session. This makes it simple to identify the active SVO card for operating system upgrades.

This chapter describes the software upgrade in Cisco NCS 2000 SVO and its related tasks. This chapter applies to the NCS 2000 node that is already migrated to SVO with release greater than R12.x

SVO Software Package

The software package is distributed as a single file that is downloaded to the local file system of SVO and it contains all the required packages for upgrading the system. The single file image is different depending on the SVO installation type: SVO line card (ISO image file) or SVO external server (TAR image file). The package can be downloaded by any active SVO ROADM instance running on the line card or external server.

External server TAR image consists of the following:

- NCS 2000 software packages
- SVO software package
- Admin plane package

ISO line card image consists of the following:

- NCS 2000 software packages
- SVO software package
- Admin plane package
- SVO line card operating system
- Additional packages for specific line card management
- Card controller software package

Note You must download the software only from the ROADM SVO instance and not from the OLA, DGE or TXP SVO instances.

Workflow for Software Upgrade

The **Software Manager** page has four tabs which are used for upgrading the device software.

Note The following sequence is mandatory for software upgrade.

1. Use the **Download** tab to download the necessary packages. The relevant procedure is discussed at Download Software Package, on page 408. The downloaded packages appear in the **Software Packages** tab.
2. Use the **Admin Plane Software** tab to activate the SVO package. It lists the active software versions. The relevant procedure is discussed at Activate Admin Plane Software , on page 409.
3. Use the **SVO Software** tab to activate the SVO package. It lists the active software versions. The relevant procedure is discussed at Activate SVO Software , on page 410.

4. Use the **Device Software** tab to download the NCS 2000 device software packages. The relevant procedure is discussed at Download Device Software , on page 411.
5. Use the **Device Software** tab to activate the NCS 2000 device software packages. The relevant procedure is discussed at Activate Device Software, on page 412.

Note After upgrading the SVO solution to R12.31, you should adjust the Reserved memory of the SVO container. For more information on how to adjust the reserved memory, see Edit Reserved Memory of an SVO Instance, on page 47.

Download Software Package

Use this task to download the software package on the SVO card.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Software Manager**.

Step 2 Click the **Download** tab.

Step 3 From the **Protocol** drop-down list, choose SFTP.

Step 4 Enter the remote file path of the software package in the **Remote File Path** field.

Step 5 Choose to enter the credentials either through **User-Password** or **Auth-Group**.

- If you choose **User-Password**, enter the **Username** and **Password** in the given fields.
- If you choose **Auth-Group**, choose the authentication group from the **Auth Group** drop-down list.

Step 6 Click **Download** to download the software package on the SVO card.

When the software package is successfully downloaded, the **Status** is updated to **Download of package completed on** <*time and date*>.

Step 7 After the download, click the **Refresh** icon on the **Software Packages** tab.

The **Software Packages** tab displays the list of software packages that are downloaded. The **Software Packages** tab lists the NCS2K, SVO, operating system, and Admin Plane packages.

From Release 12.3.1, the **Software Packages** tab displays the list of software packages in the increasing order of their release. Expand each package to see its software components.

The following details are displayed for the downloaded packages:

- **Software Package ID**—Displays the package ID of the ISO or TAR file.
- **Software Component**—Displays the name of the individual component that is part of the ISO or TAR file.

- **File Name**—Displays the filename of the software package.
- **Version**—Displays the version of the software package.
- **CRC Valid**—Cyclical Redundancy Check (CRC) to perform package integrity and ensure that the package content is valid.
- **Size (in bytes)**—Displays the size of the software package.

Note From Release 12.3.1, the **Software Packages** tab displays up to eight software packages. If the ninth software package is downloaded, it automatically overwrites the oldest package that is not in use.

Delete Software Package

Use this task to delete the software package on the SVO card or application.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Software Manager**.

Step 2 Click the **Software Packages** tab.

The package names and their corresponding software versions are displayed.

Step 3 Check the checkbox against the SW Package ID of the SVO package which you want to delete.

Step 4 Click **Delete**.

Note The SVO application checks to verify that no application (such as Admin Plane, SVO instance) or device (such as NCS2K, SVO controller) is running one of the images being removed. In case of NCS2K device, the standby package version is also checked. If any image in the selected package is currently running, then the deletion operation is stopped.

A dialog box for deleting the software package appears.

Step 5 Click **Delete**.

A confirmation message appears.

Step 6 Click **Yes**.

Activate Admin Plane Software

Use this task to activate the admin plane software package on the SVO card.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Software Manager**.

Step 2 Click the **Admin Plane Software** tab.

The following details of the admin plane software are displayed:

- **Name**—Displays the name of the admin plane software that is active.
- **SW Version**—Displays the admin plane software version that is active.

Step 3 Click **Activate**.

The **Software Image Activation** dialog box appears.

Step 4 From the drop-down list, choose the software image to activate.

Step 5 Click **Activate**.

A confirmation message appears.

Step 6 Click **Yes**.

When the admin plane software is successfully activated, **Activation of SW to version <*version-number*> has succeeded on <*time and date*>** message apears next to the **Activate** button.

The activated software version appears in the **SW Version** column.

Activate SVO Software

Use this task to activate the SVO software package on the SVO card.

Before you begin

Log into the SVO Web Interface, on page 67

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Software Manager**.

Step 2 Click the **SVO Software** tab.

The following details of the SVO software are displayed:

- **Name**—Displays the name of the SVO software that is active.
- **SW Version**—Displays the SVO software version that is active.

Step 3 Click **Activate**.

The **Software Image Activation** dialog box appears.

Step 4 From the drop-down list, choose the software image to activate.

Step 5 Click **Activate**.

A confirmation message appears.

Step 6 Click **Yes**.

The SVO software activation takes around 4 minutes to complete.

After the activation is complete, your session ends and the login page appears.

Step 7 Log in using your credentials and check for the updated version of the SVO software in the **SW version** column.

Download Device Software

Use this task to download the device software package from the SVO card to NCS 2000 device. In R12.x, you can download the device software package to only one NCS 2000 device for each SVO instance.

Before you begin

- Log into the SVO Web Interface, on page 67
- Activate SVO Software , on page 410

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Software Manager**.

Step 2 Click the **Device Software** tab.

The following details of the software packages are displayed:

- **Name**—Displays the name of the device where the software package is downloaded.
- **Component**—Displays the platform name.
- **Working SW Version**—Displays the package version that is active.
- **Protect SW Version**—Displays the backup package version.
- **Status**—Displays the progress of package download.

Step 3 Check the checkbox against the **Name** of the device for which you want to download the new software.

Note The **Device Software** tab lists the NCS2K, svo-primary, and svo-secondary devices. Only the NCS 2000 device software package can be downloaded in R12.x.

Step 4 Click **Download**.

The **Select Software Image** dialog box appears.

Step 5 From the **Software Image** drop-down list, select the software package.

Step 6 Click **Download**.

The **Status** field displays the progress (%) of package download. After the download, the downloaded package is indicated in the Protect SW Version column.

Note If you choose to download the TNC or TNCE card for the NCS 2000 device package, the **Status** column displays the download progress (%) of only the active card and not the standby card. The **Status** field changes to downloaded only after the standby card is downloaded.

After the device software is downloaded, the USB-sync alarm is raised. The USB-sync alarm clears after 6 minutes. Click the **Bell** icon to see the USB-sync alarm in the **Alarms** tab.

Use the **Terminate Download** option to terminate the software downloading on the selected device.

Note We recommend that you limit the number of simultaneous software downloads to eight nodes.

Activate Device Software

Use this task to activate the NCS 2000 device software package in R12.x.

Note After you have downloaded the device software, wait for the USB-sync alarm to clear. If the alarm is not cleared, the activation of the NCS 2000 device software package fails.

Before you begin

- Log into the SVO Web Interface, on page 67
- Activate SVO Software , on page 410
- Download Device Software , on page 411

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Software Manager**.

Step 2 Click the **Device Software** tab.

Step 3 Choose the NCS 2000 device, and click **Activate** to activate the device software package on NCS 2000 device.

The downloaded package that is available in the Protect SW Version is activated to the Working SW Version.

Note If you choose to activate the TNC or TNCE card for the NCS 2000 device package, the **Status** field displays the activation progress (%) of only the active card and not the standby card.

Note From Release 12.3, you can upgrade the CardController component of the SVO devices.

Note From Release 12.3.1, you can upgrade the OS component of the SVO devices. However, the **Activate** button is enabled only when you select the OS component for both the SVO devices or the device that is not running the Active SVO session. *Active session* label is added next to the SVO device that is running the Active SVO session. In case of Standalone configuration, the **Activate** button remains enabled.

During the activation of the new operating system, access is temporarily lost on the active session card and the SVO Web UI.

Caution Currently no automatic rollback procedure is supported for the OS component upgrade. If issues arise, the device can be only recovered on site.

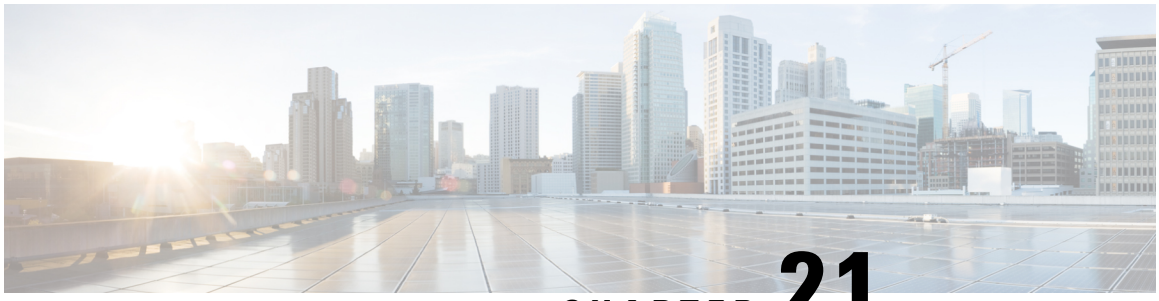
Workflow for Software Downgrade

The **Software Manager** page has four tabs which are used for downgrading the device software.

Note The following sequence is mandatory for software downgrade.

1. Use the **SVO Software** tab to activate the SVO package. It lists the active software versions. The relevant procedure is discussed at Activate SVO Software , on page 410.
2. Use the **Admin Plane Software** tab to activate the SVO package. It lists the active software versions. The relevant procedure is discussed at Activate Admin Plane Software , on page 409.
3. Use the **Device Software** tab to download the NCS 2000 device software packages. The relevant procedure is discussed at Download Device Software , on page 411.
4. Use the **Device Software** tab to activate or revert the NCS 2000 device software packages. The relevant procedure is discussed at Activate Device Software, on page 412.

Note When you downgrade the SVO solution to R12.3 from R12.31, the Reserved memory assigned for the SVO container increases by 2 GB in R12.3. After downgrading the SVO solution, you should adjust the Reserved memory of the SVO container. For more information on how to adjust the reserved memory, see Edit Reserved Memory of an SVO Instance, on page 47.



CHAPTER 21

Licensing Support for NCS 2000 Cards in SVO

This chapter describes the list of line cards that supports NCS 2000 SVO and the associated licensing operations.

Table 125: Feature History

Feature Name	Release Information	Feature Description
Licensing Support for NCS 2000 Cards in SVO	Cisco NCS 2000 Release 12.3	SVO web user interface supports licensing operations for the supported NCS 2000 line cards. You can install, save, prioritize, refresh, or rehost the licenses on the supported NCS 2000 line cards. You can also display the detailed information of the license installed.

Table 126: Feature History

Feature Name	Release Information	Feature Description
License Deployment from SVO for NCS 2000 cards	Cisco NCS 2000 Release 12.3.1	After procuring licenses from the Software Licensing Tool, the SVO web user interface now allows you to install, rehost, save these licenses, and save device credentials on the following line cards: • 9-SMR17FS • 9-SMR24FS • 9-SMR34FS Only three express (EXP) ports are active by default on these cards. This feature allows you to activate the remaining EXP ports using a license. You can use those ports to create the required ROADM services.

Overview of Licensing

A license is a permit for a software feature to be functional or enabled on a device. The "pay as you grow" model enables you to upgrade your hardware and software capacity by using a license key. As a result, the upfront deployment cost is reduced and additional capacity or features can be purchased on a need basis. You need not complete a return merchandise authorization (RMA) process to add a new hardware. Instead, you can purchase the license, have it electronically delivered, and use the license key to enable the licensed feature.

New devices are shipped with preinstalled licenses for specific functionalities based on your order. New licenses have to be added for enabling additional functionalities. New or upgraded Cisco devices must be registered in the Cisco Product License Registration portal and must have a product authorization key (PAK) to obtain licenses from Cisco.

Line Cards with SVO Licenses

SVO supports licensing for the following line cards:

• 40-SMR1-C and 40-SMR2-C Cards

- 20-SMRFS Card
- 200G-CK-LC Card
- 10x10G-LC Card
- 9-SMR17FS, 9-SMR24FS, and 9-SMR34FS Cards

40-SMR1-C and 40-SMR2-C Cards

The 40-SMR1-C and 40-SMR2-C cards use count-based licenses that represent the number of licensed wavelengths on the express (EXP) ports. The card has a base functionality for the first ten circuits provisioned using the EXP ports. License is required for provisioning any additional circuits on the EXP (Tx and Rx) ports. Permanent licenses can be purchased in 10-port increments. A maximum of three sets of permanent licenses, each supporting ten ports, can be installed.

The evaluation license on the 40-SMR1-C and 40-SMR2-C cards supports full capability and hence, all the ports can be provisioned.

The licensable PIDs for the 40-SMR1-C and 40-SMR2-C cards are:

- 15454-SMR1-LIC
- 15454-SMR2-LIC
- The non-licensable PIDs for the 40-SMR1-C and 40-SMR2-C cards are:
  - 15454-40-SMR1-C
  - 15454-40-SMR2-C

  The usage of the 40-SMR1-C and 40-SMR2-C card licensing impacts the circuit provisioning in the following ways:
  - If the card is used on a meshed node (of N degrees) or on a ROADM node, the licensing determines the number of OCH pass-through circuits that can be provisioned crossing the EXP (Tx) ports.
  - If the card is used on node where a side is defined on the EXP (Tx) port, the licensing will determine the number of OCH pass-through or add/drop circuits that can be provisioned on that side.

  If a circuit under base functionality is deleted, an existing circuit under temporary or evaluation license does not get transferred to the base functionality. However, if a new circuit is provisioned on the device, it will use the port available under base functionality.

  The 40-SMR1-C card goes to the LIC-Evaluation period without a traffic hit under the following conditions:
  - When the 40-SMR1-C card is upgraded to a release that requires a license.
  - When a permanent license is purchased for all the 40 channels.

20-SMRFS Card

The 20-SMRFS card uses count-based licenses that represent the number of licensed ports on the express (EXP) ports.

Card	Licensable PID	Non-Licensable PID
20-SMRFS	NCS2K-20-SMRFS-L=	NCS2K-20-SMRFS=

200G-CK-LC Card

The 200G-CK-LC card supports feature-based licensing.The 200G-CK-LC card supports feature-based licensing.

Table 127: Licensable and Non-Licensable PIDs

Card	Licensable PID	Non-Licensable PID
200G-CK-LC	NCS2K-200G-CK-LIC	NCS2K-200G-CK-LC

The base functionality is enabled in the licensed card version. Additional features are provided through specific feature licenses. The feature licenses can be permanent license or evaluation license.

10x10G-LC Card

The 10x10G-LC card supports count-based licenses.

Table 128: Licensable and Non-Licensable PIDs

Card	Licensable PID	Non-Licensable PID
10x10G-LC	15454-M-10x10-LIC	15454-M10x10G-LC

9-SMR17FS, 9-SMR24FS, and 9-SMR34FS Cards

The 9-SMR17FS, 9-SMR24FS, and 9-SMR34FS cards use count-based licenses that represent the number of licensed ports on the express (EXP) ports.

The licensable card versions for the 9-SMR17FS, 9-SMR24FS, and 9-SMR34FS cards have only three ports that are enabled, and by default, they do not have Flex Spectrum capability. Additional ports can be activated through specific licenses. The licenses can be permanent or evaluation licenses.

Table 129: Licensable and Non-Licensable PIDs

Card	Licensable PID	Non-Licensable PID
9-SMR17FS	NCS2K-9-SMR17FS-L=	NCS2K-9-SMR17FS=
9-SMR24FS	NCS2K-9-SMR24FS-L=	NCS2K-9-SMR24FS=
9-SMR34FS	NCS2K-9-SMR34FS-L=	NCS2K-9-SMR34FS=

Feature Licenses

The following table describes the feature licenses that can be purchased from the licensing portal.

License Feature PID	License Feature Name in SVO	Description
L-NCS2K-SMR-2P=	EXP Ports	Enables two EXP-TX/EXP-RX ports on the 9-SMR17FS, 9-SMR24FS, and 9-SMR34FS cards.
L-NCS2K-SMR-4P=	EXP Ports	Enables four EXP-TX/EXP-RX ports on the 20-SMRFS card.
L-NCS2K-CK-CL=	CPAK	Enables the CPAK client and allows to configure the TXP-100G operating mode.
L-NCS2K-SFEC-16Q=	200G	Enables 20% SD-FEC and 200G 16-QAM on the trunk port allowing the MXP_10x10G_100G, MXP_CK_100G and MXP_200G operating modes. This licence also enables CD range for the 200G application (+/- 20000 ps/nm). **Note** Two licenses, L-NCS2K-CK-CL=and L-NCS2K-SFEC-16Q, are required to configure the MXP_CK_100G operating mode.
L-NCS2K-FS=	FLEX_GRID	Enables Flex Spectrum tunability on the trunk port of the 200G-CK-LC card. NCS Flex package is required to use this license.
L-NCS2K-SD-FEC=	100G_SD_FEC_OR_CD_RANGE	Enables wide CD range (+/- 70000 ps/nm) on standard FEC or enables 20% SD-FEC and wide CD range (+/- 92000 ps/nm) for 100G operating modes on the 200G-CK-LC card.
15454-LIC-CH-10=	DWDM_Wavelength	Enables license for 10 Add/Drop or Express channels on the 40-SMR1-C and 40-SMR2-C cards.

Licensing Operations

You can choose one of the following licensing operations that best suits your requirement:

- Install License, on page 420

- Save License, on page 420
- Save Watchtower Device Certificate License
- Rehost License

Install License

Use this task to install the license on the card.

Note The license file would have been emailed to your registered e-mail address after the license registration on the licensing portal.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **License Operations** tabs.

Step 2 From the **Choose the Operation to Perform** drop-down list, choose **Install License**.

Step 3 Click **Select files**, browse and select the license file.

Step 4 Click **Apply**.

Save License

Use this task to save the license file on the card.

Note You can always save a license file that you have installed. If you have lost the license by accidental delete, you can reinstall the license using the saved license file. An evaluation license cannot be saved.

Note The saved license file used in SVO is not applicable in CTC and vice versa.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Choose the **Provisioning** > **Licensing** > **License Operations** tabs.
Step 2 From the **Choose the Operation to Perform** drop-down list, choose **Save Licenses**.
Step 3 Enter a name in the **File Name** field and click **Apply**.

Save Watchtower Device Certificate License

The Watchtower Device Certificate (WDC) is used to ascertain the physical authenticity of the device. The WDC is hard-coded on the device.

Use this task to save the credentials associated with the card.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **License Operations** tabs.
Step 2 From the **Choose the Operation to Perform** drop-down list, choose **Save Device Credentials (WDC)**.
Step 3 Enter a name in the **File Name** field and click **Apply**.

Rehost License

Rehosting enables you to transfer license between two cards, where you revoke the license from the source card and install it on a new card.

Use this task to upload a permission ticket onto the device from which the licenses are transferred (the source device) and rehost the licenses.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **License Operations** tabs.
Step 2 From the **Choose the Operation to Perform** drop-down list, choose **Rehost License**.

Step 3 Click **Select File** to choose a permission ticket, enter a name in the **File Name** field for the Rehost Ticket, and click **Upload**.

Step 4 Click **Apply**.

You will be notified with a **"Rehost License operation successful for the card"** message. You can download the Rehost file.

Step 5 Go to the Product License Registration application page: https://software.cisco.com/software/swift/lrp/#/pak.

Step 6 Click **Devices** > **Move Licenses** > **Complete Secure Rehost** tabs.

Step 7 Select the **Product Type**, enter the **Product ID**, and the **Serial Number** of the device that the licenses will be transferred to (the destination device).

Step 8 Paste the **Rehost Ticket** and click **Next**.

You will see the licenses that are available for transfer to the destination device.

Step 9 Click **Submit** to generate the licenses.

You will receive an email with the set of licenses. Install the licenses onto the destination device.

View License Information

You can perform the following operations to view the license information:

- Refresh License
- Display License

Refresh License

Use this task to refresh the license data. You can view the updated license information.

Note The license data cannot be automatically updated. The license card data can only be refreshed by using **Refresh License Data** operation.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **Counted License Features** > **License Features** tabs.

Step 2 Choose the license entry to refresh the license data.

Step 3 Click **Refresh License Data**.to refresh the following parameters:

- License Feature Name—Name of the licensed feature.
- Total Base Count— Total number of ports under built-in-base license.
- Available Base Count—Number of ports available to provision under base license.
- Total License Count—Total number of licensed ports that can be used under the current in-use license.
- Available License Count—Number of ports available to be provisioned under the current in-use license.
- Unlicensed Count—Number of unlicensed ports.
- Type Used—Type of the license.

Display License

Use this task to display the following information for the installed and evaluation licenses:

- License Index—In count-based licenses, the license index is based on the license type and the number of licensed ports. In feature-based licenses, the license index is based on the license type and is always license type-1.
- License State—License state such as Active, Inactive, In_use, or Not In use.
- License Type—License type such as Evaluation, Temporary, or Permanent.
- Expired—Shows whether the license is expired or not.
- Total License Count—The number of licensed ports.
- Priority—The priority of the license such as high, medium, or low.
- Expiry Date—Shows the license expiry date.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **Counted License Features** tabs.

Step 2 Choose the license entry.

Step 3 Click **Manage License Data**.

Manage Licensing Data

You can manage the license data by performing the following actions:

Annotate license

Use this task to annotate comments to a license line. The comments added are saved in the license file.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **Counted License Features** tabs.

Step 2 Choose the license entry and click **Manage License Data**.

Step 3 Choose the license entry that you want to annotate and click **Annotate License**.

Step 4 Enter the comment on the **Annotate License** dialog box and click **OK**.

Evaluation license cannot be annotated. License annotation allows you to add a maximum of 99 characters. This operation overwrites the existing user comments, if any.

Delete license

Use this task to delete a permanent or temporary license from the card. You can delete a license only when the license has expired or when it is in the **Inactive** or **Active, not in use** state.

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **Counted License Features** tabs.

Step 2 Choose the license entry and click **Manage License Data**.

Step 3 Choose the license entry that you want to delete and click **Delete License**.

Modify License Priority

Use this task to change the license priority of an evaluation or temporary license. You can change the priority of the license from high to low or vice versa.

Note License priority of a permanent license cannot be modified. Priority management does not support "Feature Based Licenses".

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **License Features** tabs.

Step 2 Choose the license entry and click **Manage License Data**.

Step 3 Choose the license entry that you want to modify and click **Modify License Priority**.

Step 4 From the **Select the Priority** drop-down list and click choose high or low priority.

Step 5 Click **OK**.

Display Detail License Usage

Use this task to display the list of ports and the corresponding license status for each of the ports in the **Detail License** page.

Note You can see the NETCONF client operations here: https://www.cisco.com/c/en/us/td/docs/optical/ncs2000/121/data-models-configuration/guide/b-data-models-config-guide-121.html

Before you begin

Log into the SVO Web Interface, on page 67

Open the Card View, on page 70

Procedure

Step 1 Click the **Provisioning** > **Licensing** > **Counted License Features** tabs.

Step 2 Click the **Get Detail License Usage** tab.

The list of ports and their license status are displayed. You can sort the ports based on created order or by port number.