Cisco Evolved Programmable Network Manager 7.1.1 RESTCONF API Guide

Abstract

The Cisco NBI OSS Integration Guide for RESTCONF gives information on OSS Integration using RESTCONF northbound interfaces.

Table of Contents

1.1 Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Preface

This guide provides information about the RESTCONF Northbound APIs supported by Cisco Evolved Programmable Network (EPN) Manager. OSS operators can use this document to integrate Cisco EPN Manager with their OSS system.

1.2   Conventions

This document uses the following conventions:

Convention	Indication
bold	Indicates commands, keywords, and user-entered text.
italic	Indicates document titles, new or emphasized terms, and arguments for which you supply values.
[]	Indicates elements that are optional.
{x|y|z}	Indicates required alternative keywords grouped within brackets and separated by vertical bars.
[x|y|z]	Indicates optional alternative keywords grouped in brackets and separated by vertical bars.
String	Indicates a nonsuited set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier font`	Indicates code snippets and XML.
<>	Indicates nonprinting characters such as passwords.
[ ]	Indicates default responses to system prompts.
!,#	Indicates a comment when used at the beginning of a line of code.
Note	Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

1.3   Additional User Documentation

The RESTCONF and YANG Specifications can be obtained from IETF.

Northbound RESTCONF Interface

Cisco EPN Manager implements the RESTCONF API as a standards-based Northbound Interface for integrating Cisco EPN Manager with a standards-compliant OSS. It is a set of RESTFul services confirmed to the RESTCONF/YANG specification.

The Cisco EPN Manager implementation of the RESTCONF/YANG interface supports the retrieval of device inventory, circuit inventory, circuit provisioning and notifications about respective resource changes and provisioning.

1.4   RESTCONF and Web Services Standards

RESTCONF NBI in Cisco EPN Manager is a RESTFul Web Services Interface that follows the IETF Draft specification of RESTCONF protocol for defining its interfaces and YANG specification for defining the data model. The following W3C and IETF standards are used:

- RESTCONF Protocol – RFC 8040 (January, 2017)
- YANG Specification – RFC 6020
- RESTful Web Services (JAX-RS)
- XML Schema version 1.0 (XSD)
- Hypertext Transfer Protocol HTTP 1.1 - RFCs 7230-7237

While no standard exists for information model exposed by this interface, the model is roughly based on TeleManagement Forum (TMF) standards governing the modeling of physical and service inventory.

1.5   Communication Patterns

RESTCONF interfaces supported by Cisco EPN Manager use REST (Representational State Transfer) techniques. REST is stateless and uses a client-server protocol (HTTP 1.1).

1.6   Batch Retrieval

Default Batch Size

The default max batch size for retrieval is set to 100.

Batch Size Properties

The operations in the API would return a single or multiple objects. In case of operations that return multiple objects, set of standard query parameters are defined to manage the number of objects retrieved per request. The following http query parameters can be used to control the batch retrieval.

Request Query Params

Query Param	Description
.startIndex	0 based index as a start index of the data to be retrieved. Note the dot (.) prefix in the parameter name. This is required to identify this as a special parameter.
.maxCount	Maximum number of objects to be retrieved. Note the dot (.) prefix in the parameter name. This is required to identify this as a special parameter.

The response for the data API always returns a list container with **startIndex** and **lastIndex** as first two elements of the container data to help with the batch sequence.

1.7   Fully Distinguished Name (FDN)

Inventory objects in this interface has attributes representing FDN (Fully Distinguished Name). These attributes are used as identifiers of the object or as a reference to the object in query parameters or in the returns data wherever a reference to the object is needed.

This FDN is a formatted string that consists of a set of type/value pairs with the following syntax:

- Sequence of <type>=<value> pairs separated by "!" where:
  - <type> is a constant value defined in the data model to represent the inventory object in the hierarchy, e.g. MD,ND,EQ,PTP,FTP, CTP, TL,VC,CFS, etc.
  - <value> is any text or sequence of <attrName>=<attrValue> pair separated by ";" that represents the attribute/value pairs of the inventory object constitutes a unique value within the local scope of the object represented by the type.

The following are some examples for the FDNs:

- Node FDN= "MD=CISCO_EPNM!ND=asr9k-cluster.cisco.com"
- Equipment FDN = "MD=CISCO_EPNM!ND=asr9k-cluster.cisco.com!EQ=name=subslot 0/3 transceiver 0;partnumber=ONS-SI-155-SR-MM"
- Termination Point FDN = "MD=CISCO_EPNM!ND=ME3800-Automation!CTP=name=GigabitEthernet0/2;lr=lr-ip;ADDRESS=192.168.100. 31"

Note: It is assumed that the devices in the network managed by Cisco EPN Manager have unique names and that this is continuously ensured by the network operator. If two or more devices have the same name, the API will not produce consistent results when using the Object Name as input to any of the APIs.

Supported FDNs (Fully Distinguished Name) for the Inventory Objects

The following table list all the supported FDNs for Inventory objects handled with in the APIs.

Inventory Object	FDN Format	Example
Node (Device)	MD=CISCO_EPNM!ND=<node.name>	MD=CISCO_EPNM!ND=asr9k-cluster.cisco.com
Equipment	MD=CISCO_EPNM!ND=<node name>!EQ=name=<equipment. name>;partnumber=<equipment.part number>	MD=CISCO_EPNM!ND=asr9k-cluster.cisco.com!EQ=name=subslot 0/3 transceiver 0;partnumber=ONS-SI-155-SR-MM
PhysicalConnector	MD=CISCO_EPNM!ND=<node name>!EQ=name=<equipment. name>;partnumber=<equipment.part number!PC=name>	MD=CISCO_EPNM!ND=example.cisco.com!EQ=name=APPM-3-1!PC=ACHAN-3-1-1
Termination Point – PTP	MD=CISCO_EPNM!ND==<node name>!PTP=name=<discovered-name>;lr=<layer-rate>	MD=CISCO_EPNM!ND=isc-asr903b.cisco.com!PTP=name=SONET 0/2/3;lr=lr-dsr-oc3-and-stm1
Termination Point – FTP	MD=CISCO_EPNM!ND==<node name>!FTP=name=<discovered-name>;lr=<layer-rate>	MD=CISCO_EPNM!ND=ME3800-Automation!FTP=name=TenGigabitEthernet0/2;lr=lr-ten-gigabit-ethernet
Termination Point – CTP	MD=CISCO_EPNM!ND==<node name>!CTP=name=<discovered-name>;lr=<layer-rate> Below are optional attribute=values in the type value: ADDRESS=<ip>;PWID=<pwid>;REMOTE_ADDRESS=<ip>	MD=CISCO_EPNM!ND=ME3800-Automation!CTP=name=GigabitEthernet0/2;lr=lr-ip;ADDRESS=192.168.100. 31 MD=CISCO_EPNM!ND=isc-cl-test-me3800x-1.cisco.com!CTP=name=PW_27_100.100.100.5;lr=lr-pseudowire;PWID=27;REMOTE_ADDRESS=100.100.100. 5
Topological Link	MD=CISCO_EPNM!TL=<tl.name>	MD=CISCO_EPNM!TL=LINK PW 100.100.100.5_145_192.169.105.65

Virtual Connection	MD=CISCO_EPNM!VC=<vc.name >	Discovered VC: MD=CISCO_EPNM!VC=EvcLink_EthPw Link#EPW_61.61.61.30_185_172.16.90.2 User Provisioned VC: MD=CISCO_EPNM!VC=MyService
Network Interface	MD=CISCO_EPNM!NI=<ni.name>	MD=CISCO_EPNM!NI=MyEplUni MD=CISCO_EPNM!NI=MyAccessEplEn ni
Customer Facing Service	MD=CISCO_EPNM!CFS=<cfs.name >	MD=CISCO_EPNM!CFS=MyEPLService 1
Customer	MD=CISCO_EPNM!CUSTOMER=< customer.name>	MD=CISCO_EPNM!CUSTOMER=MyGo ldCustomer
QOS Policy	MD=CISCO_EPNM!POLICY_QOS= <name>	MD=CISCO_EPNM!POLICY_QOS=My DeviceQoS
QOS Profile	MD=CISCO_EPNM!PROFILE_QOS =<name>	MD=CISCO_EPNM!PROFILE_QOS=My UserDefineQoS
Service Profile	MD=CISCO_EPNM!PROFILE_SER VICE=<name>	MD=CISCO_EPNM!PROFILE_SERVICE =GoldEplServiceProfile1
Path	MD=CISCO_EPNM!PATH=<name>	MD=CISCO_EPNM!PATH=123_exp_pat h
Controller Port	MD=CISCO_EPNM!ND=<node.nam e>!CTRLP=<name>	MD=CISCO_EPNM!ND=NCS4206-146.4!CTRLP=MediaType 0/4/0
SR Policy	MD=CISCO_EPNM!CFS=<srpolicy. name>	MD=CISCO_EPNM!CFS=MySrPolicyPol icy

Note: Generic API Get request with filters containing special characters should be encoded as per RFC 7230 and RFC 3986 standard.

For example: "[" character in FDN can be encoded to "%5B" using UTF-8 encoding.

1.8   HTTP Security Protocol

Any OSS Client accessing the Cisco EPN Manager RESTCONF NBI should use the HTTPS with TLS 1.2.

As of Cisco EPN Manager 2.1, Transport Layer Security (TLS) 1.2 is only supported for HTTPS and TLS related secured communication, for example, RADIUS EAP-TLS. Support for TLS 1.0, TLS 1.1 and all versions of SSL has been disabled due to security vulnerabilities.

This means that all peer systems and clients (such as OSS Clients using the NBI) that transact with Cisco EPN Manager using HTTPS/TLS must support TLS 1.2. If they do not support TLS 1.2, they must be upgraded. Where possible, the Cisco EPN Manager documentation highlights the potentially affected systems. Please contact your Cisco representative for support in this regard, if necessary.

1.9   Authentication

The RESTCONF resource paths in Cisco EPN Manager are secured. To access these resource paths, HTTP basic authentication is required. e.g. to access customer RESTCONF api

```
curl --cookie-jar cookie.txt --include --header "accept: application/json" --request
GET  https://<EPNM-HOST>/restconf/data/v1/cisco-customer:customer  --basic --user
<username>:<password>
```

After authenticating request to a RESTCONF resource path, web server returns a session cookie to the RESTCONF client in the response. This session cookie is valid for session time configuration for server (default being 60 minutes) and RESTCONF client can save this cookie. In subsequent requests for RESTCONF resource paths, RESTCONF client can include un-expired session cookie. The session cookie will be used in lieu of HTTP basic authentication by server in these subsequent requests. For making several call in a sessions using session cookie is recommended approach, not only response will be faster but such approach prevents the EPN Manager from making authentication requests to the local database or AAA server (Tacacs+, LDAP etc.) for each RESTCONF resource

request. These authentication calls from EPN Manager can stress AAA server and using session cookie eliminates redundant EPN Manager to AAA server requests.

Recommended flow for authentication of RESTCONF session is as follows
- Initialize a REST session using HTTP basic authentication to get and save a session cookie from spring security with http POST request to https://<epnmhost>/restconf/j_spring_security_check e.g.

```
curl --cookie-jar cookie.txt --include --header "Content-type: application/x-www-form-
urlencoded" --request POST  https://<epnmhost>/restconf/j_spring_security_check  -d
"j_username=<username>&j_password=<password>"
```

- Include saved session cookie in subsequent call to RESTCONF resource paths during the session and do not include HTTP Authorization header for basic authentication e.g.

```
curl --cookie cookie.txt --include --header "accept: application/json" --request
GET https://<EPNM-HOST>/restconf/data/v1/cisco-customer:customer
```

In summary, HTTP basic authentication can always be performed for individual RESTCONF resources paths, however it is recommended to get the authentication session/cookies established through spring security before making subsequent requests in a session.

1.10 Authorization

User credentials passed for accessing the RESTCONF resource paths require authorization to use the API. This authorization can be configured using Cisco EPN Manager's security management interface. In Cisco EPN Manager, NBI read privileges are required to perform GET (retrieval) on the RESTCONF data interfaces, whereas to use the provisioning interfaces, you need NBI write privileges.

Note: NBI Credential user group is Deprecated.

Virtual Domain Support

RESTCONF controls access to data by the virtual domain of the NBI user, as configured through the Cisco EPN Manager's security management interface. This interface allows an administrator to create virtual domains and assign them to users. Among other things, virtual domains contain a list of Network Devices (Nodes) accessible to the user. Refer the *Cisco EPN Manager User and Administration Guide* for details.

In general, a user may access all the data associated with a network device (Node) within the user's virtual domain. In case of the physical inventory, this is straight forward; if the user has access to a Node, the user may access any Chassis, Equipment, Module, and Physical Connector on that Node.

For services (QoS policies, Termination Points, Topological Links, Virtual Connections and Routes, and Customer Facing Services), RESTCONF allows access to the service data if **any** of the associated endpoints or policies are on a node that the user may access. However, note that for APIs where RESTCONF returns information about the service's endpoints, it includes data for authorized end points only, and omits data for end points on devices that are not accessible to the user.

For provisioning interfaces (Optical, CEM, Flex LSP, L2VPN, L3VPN, MPLS-TE, Model-Based Configuration, and Set Termination Point), NETCONF checks all resources, as identified by their Fully Distinguished Name (FDN), against the authorizations configured in the user's virtual domain. If the object identified by the FDN is not associated with a device in the user's virtual domain, RESTCONF reports that the resource is not accessible or does not exist. (For security reasons, RESTCONF does not confirm that the resource exists in scenarios where access is denied.)

RESTCONF currently supports one virtual domain per NBI user. Add all network devices accessible to a user to this single domain. Multiple NBI users may share the same virtual domain, but each user must have only one virtual domain.

1.11 Rate Limiting

The API is rate limited to protect against overload situations.

Overview

Rate limiting on the API is designed to protect RESTCONF from excessive requests. When the number of requests received within a time window reaches a threshold number, then further requests are rejected until the rate falls back below that threshold. Also, the maximum number of concurrent requests (per user and across all users) that the servers will handle can be configured. Once this limit is reached, further requests will be rejected. There are five thresholds that can be set by the system administrator of the platform.

- The maximum number of requests for all users within the window period
- The maximum number of requests per user within the window period
- The maximum number of concurrent requests per user
- The maximum number of concurrent requests for all users
- The maximum size of pages request

If any of these thresholds is exceeded, the requests will be rejected with status code of 503 (service unavailable). The text of the response will contain information about the cause as appropriate:

- NBI Global Rate limit exceeded (More than xxx in yyy ms)
- NBI Rate limit for user <userId> exceeded (More than xxx in yyy ms)
- Per user concurrent query count exceed Currently xxx : Limit is yyy

In the case of the per user threshold being exceeded, other users will continue to have access to the NBI as normal.

Note that requests rejected by the rate limiter do not count in calculation of the threshold.

Configuration

Rate and size limiting is configured internally in NBI is shown in the table below. These properties can not be changed.

The properties can be edited in a file called *restconf-ratelimit.properties* located in the directory **/opt/CSCOlumos/conf/restconf/**

Property	Allowed Values	Default Value	Description
restconf.nbi.rateLimit.maxConcurrentQueries	A non-zero positive integer	60	This is the number of concurrent requests allowed for any given user
restconf.nbi.rateLimit.maxAllUserConcurrentQueries	A non-zero postitive integer. Use -1 to disable the limiting of all user concurrent requests	270	This is the number of concurrent requests allowed for all users.
restconf.nbi.rateLimit.perUserThreshold	An integer. Use -1 to disable the limiting of per user requests.	30	This is the number of requests for any given user that can be handled in windowsize ms.
restconf.nbi.rateLimit.totalRequestThreshold	An integer. Use -1 to disable the limiting	120	This is the number of total request

Property	Allowed Values	Default Value	Description
	for total requests.		that can be handled in windowsize ms.
restconf.nbi.rateLimit.wndowSegments	An integer value such that windowSize /windowSegments is a whole number	10	This property is used internally to divide the window into segments. The number of segments determine the rate at which the window decrements the request counter. For example, with 10 segments in a 1000ms window, the count will be reduced every 100 ms by the number of counts held in the oldest segment. The count is increased immediately after receiving a new request.
restconf.nbi.rateLimit.windowSize		1000	This property is the size of the sliding window used to count requests.

1.12 Provisioning rate configuration

Overview

RESTCONF handles various service provisioning requests and number of requests that RESTCONF can accommodated can be configured.

Configuration

Provisioning requests rate are configured with properties defined in the table below. These properties can only be changed by a systems administrator and require EPNM restart to take effect.

The properties can be edited in a file called *restconf-config.properties* located in the directory **/opt/CSCOlumos/conf/restconf/**

Property	Allowed Values	Default Value	Description
thread.corePoolSize	A non-zero positive integer	50	This is the number of threads spawned and ready

			for accepting provisioning requests.
thread.queueCapacity	A non-zero postitive integer.	100	This is the number of provisioning requests can be kept in the queue when all the corePoolSize threads are actively running.
thread.maxPoolSize	A non-zero positive integer	50	This is the number of threads that will be spawned when the queueCapacity is exhausted during service provisioning requests.

1.13 License

A Cisco EPN Manager NBI license is required to use RESTCONF NBI APIs. EPNM Advance License is required for following APIs

- /restconf/operations/v1/cisco-service-activation
- /restconf/data/v1/cisco-service-network:virtual-connection
- /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route
- /restconf/operations/v1/cisco-service-oam:service-oam-config
- /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
- /restconf/operations/v1/cisco-resource-activation:assign-shared-risk-resource-group
- /restconf/operations/v1/cisco-resource-activation:create-shared-risk-resource-group
- /restconf/operations/v1/cisco-resource-activation:delete-shared-risk-resource-group
- /restconf/operations/v1/cisco-resource-activation:unassign-shared-risk-resource-group
- /restconf/data/v1/cisco-service-network:customer-facing-service
- /restconf/data/v1/cisco-service-network:ipsla-profile
- /restconf/data/v1/cisco-service-network:network-interface
- /restconf/data/v1/cisco-service-profile:service-profile
- /restconf/operations/v1/cisco-service-action:restore-reroute
- /restconf/operations/v1/cisco-service-action:restore-revert
- /restconf/operations/v1/cisco-service-action:restore-upgrade
- /restconf/operations/v1/network-service:resync-service

Supported Use Cases and Interfaces

The table below lists the use cases supported in the Cisco EPN Manager RESTCONF NBI:

Table - Supported Cisco EPN Manager RESTCONF NBI Use cases

Use case	API Path with Params
Retrieve List of Supported YANG Modules	
List All YANG Modules	/restconf/data/ietf-yang-library:modules-state
Retrieve Physical Inventory	
Get/Create Groups	/restconf/data/v1/cisco-resource-physical:group
Get/Update/Delete Group given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-physical:group?fdn=<value>
Get All Nodes	/restconf/data/v1/cisco-resource-physical:node
Get Node given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-physical:node?fdn=<value>
Get All Chassis	/restconf/data/v1/cisco-resource-physical:chassis
Get Chassis given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-physical:chassis?fdn=<value>
Get All Equipment	/restconf/data/v1/cisco-resource-physical:equipment
Get Equipment given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-physical:equipment?fdn=<value>
Get All Modules	/restconf/data/v1/cisco-resource-physical:module
Get Module given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-physical:module?fdn=<value>
Get All Physical Connectors	/restconf/data/v1/cisco-resource-physical:physicalconnector
Get Physical Connector given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-physical:physicalconnector?fdn=<value>
Get All Optical Network Settings	/restconf/data/v1/cisco-resource-optical:optical-nesettings
Get All Optical Network Settings (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-optical:optical-nesettings?node-fdn=<value>
Retrieve TerminationPoint Resource	
Get All TerminationPoints	/restconf/data/v1/cisco-resource-ems:termination-point
Get TerminationPoint given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-resource-ems:termination-point?fdn=<value>
Get All Physical Termination Points	/restconf/data/v1/cisco-resource-ems:termination-point?type=PTP
Get All Physical Termination Points for Device	/restconf/data/v1/cisco-resource-ems:termination-point?type=PTP&ndFdn=<value>
Get All Floating Termination Points	/restconf/data/v1/cisco-resource-ems:termination-point?type=FTP
Get All Floating Termination Points for Device	/restconf/data/v1/cisco-resource-ems:termination-point?type=FTP&ndFdn=<value>
Get All Connection Termination Points	/restconf/data/v1/cisco-resource-ems:termination-point?type=CTP
Get All Connection Termination Points for Device	/restconf/data/v1/cisco-resource-ems:termination-point?type=CTP&ndFdn=<value>
Get Contained Connection Termination Points	/restconf/data/v1/cisco-resource-ems:termination-point?fdn=<value>&containedCTP=true
Get Contained In Use Connection Termination Points	/restconf/data/v1/cisco-resource-ems:termination-point?fdn=<value>& containedInUseCTP=true
Retrieve Topological Links	
Get All Topological links	/restconf/data/v1/cisco-resource-network:topological-link
Get a Topological Link given a FDN	/restconf/data/v1/cisco-resource-network:topological-link?fdn=<value>

Get a Topological Link given a topo-Layer	/restconf/data/v1/cisco-resource-network:topological-link?topo-layer=<value>
Retrieve Virtual Connection Resource	
Get All Virtual Connections	/restconf/data/v1/cisco-service-network:virtual-connection
Get All Virtual Connections for a specific type	/restconf/data/v1/cisco-service-network:virtual-connection?type=<value>
Get a Virtual Connection given its FDN (Fully Distinguished Name)	/restconf/data/v1/cisco-service-network:virtual-connection?fdn=<value>
Get All Virtual Connection referencing a given Termination point	/restconf/data/v1/cisco-service-network:virtual-connection?tpFdn=<value>
Multi Layer Trace	
Get Multi Layer Trace for a given vcFDN	/restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=<value>
MPLSTE Explicit Path	
Get All MPLS TE Explicit Paths	/restconf/data/v1/cisco-resource-ems:mpls-te-explicit-path
Get an MPLS TE Explicit Path	/restconf/data/v1/cisco-resource-ems:mpls-te-explicit-path?path-ref=<value>
Retrieve Customer Facing Service Resource	
Get All Customer Facing Services of a given type	/restconf/data/v1/cisco-service-network:customer-facing-service?type=<value>
Get All Customer Facing Services of a given type and sub-type	/restconf/data/v1/cisco-service-network:customer-facing-service?type=<type value>&subtype=<sub-type value>
Get Customer Facing Services given its FDN	/restconf/data/v1/cisco-service-network:customer-facing-service?fdn=<value>
Get Planned Customer Facing Services	/restconf/data/v1/cisco-service-network:customer-facing-service?plannedServices=<true/false>
QoS Policy Retrieval	
Get All QoS Policies in a batch	/restconf/data/v1/cisco-qos:qos-policy
Get QoS Policy for a given FDN	/restconf/data/v1/cisco-qos:qos-policy?fdn=<value>
Get All QoS Policies for a given device	/restconf/data/v1/cisco-qos:qos-policy?ndFdn=<value>
QoS Profile Retrieval	
Get All QoS Profiles in a batch	/restconf/data/v1/cisco-qos:qos-profile
Get QoS Profile for an given FDN	/restconf/data/v1/cisco-qos:qos-profile?fdn=<value>
CLI Template Retrieval	
Get All CLI Template in a batch	/restconf/data/v1/cisco-resource-activation:cli-template
Get CLI Template for a given template name	/restconf/data/v1/cisco-resource-activation:cli-template?name=<cli-template-name>
Audit Log Retrieval	
Get All Audit Log Entries in a batch	/restconf/data/v1/cisco-audit:audit-log
Get filtered Audit Log Entries	/restconf/data/v1/cisco-audit:audit-log?*attribute=filter-spec*
Get sorted Audit Log Entries (+ or -)	/restconf/data/v1/cisco-audit:audit-log?.sort(+*attribute*)
Set Termination Point	
Set attributes on a Termination Point	/restconf/operations/v1/cisco-resource-activation:set-termination-point
Service Activation	
Provision a Service	/restconf/operations/v1/cisco-service-activation:provision-service
Modify a Service	/restconf/operations/v1/cisco-service-activation:modify-service
Terminate a Service	/restconf/operations/v1/cisco-service-activation:terminate-service
Roll a Service	/restconf/operations/v1/cisco-service-activation:roll-service
Customer CRUD	/restconf/data/v1/cisco-customer:customer
Standalone OAM Performance Test	

Execute Performance Test	/restconf/operations/v1/cisco-service-oam:service-oam-config
Get Performance Test Result	/restconf/operations/v1/cisco-service-oam:service-oam-config/{request-id}
Resource Activation	
Run CLI Configuration Template – TBC (Template Based Configuration)	/restconf/operations/v1/cisco-resource-activation:run-cli-configuration
CLI Configuration Template Run Status	/restconf/operations/v1/cisco-resource-activation:get-cli-configuration-run-status/{job-name}
MPLS TE explicit path - Create	/restconf/operations/v1/cisco-resource-activation:create-explicit-path
MPLS TE explicit path - Modify	/restconf/operations/v1/cisco-resource-activation:modify-explicit-path
MPLS TE explicit path - Terminate	/restconf/operations/v1/cisco-resource-activation:terminate-explicit-path
Performance Metrics	
Optical Power And Span Loss for Links	/restconf/data/v1/cisco-resource-network:perf-metrics
Alarm Retrieval	
Get All Alarms in a batch	/restconf/data/v1/cisco-rtm:alarm
Get All Alarms by given Node reference	/restconf/data/v1/cisco-rtm:alarm?nd-ref=<value>
Get All Alarms by given Termination point reference	/restconf/data/v1/cisco-rtm:alarm?tp-ref=<value>
Get All Alarms by given Equipment reference	/restconf/data/v1/cisco-rtm:alarm?eq-ref=<value>
Get All Alarms by given perceived severity	/restconf/data/v1/cisco-rtm:alarm?perceived-severity=<value>
Get All Alarms by given System Update Time	/restconf/data/v1/cisco-rtm:alarm?system-update-time=<value>
Get All Alarms by given IteratorId	/restconf/data/v1/cisco-rtm:alarm?.iteratorId=<value>
Alarm Handling	
Alarm Ack/UnAck/Clear/Delete	/restconf/data/v1/cisco-alarm:handle-alarm
Alarm to Service association	
Get All Alarms by Service name	/restconf/datav1/cisco-rtm:impacting-alarms-by-service?cfs-ref=<value>
Patch cord	
Create Patchcord	/restconf/operations/v1/cisco-resource-activation:create-patch-cord
Delete Patchcord	/restconf/operations/v1/cisco-resource-activation:delete-patch-cord
SRRG	
Get All SRRGs present in EPNM	/restconf/data /v1/cisco-resource-network:shared-risk-resource-group
Get SRRG by FDN	/restconf/data/v1/cisco-resource-network:shared-risk-resource-group?fdn=<value>
GetAll SRRG Pool	/restconf/data/v1/cisco-resource-network:srrg-pool
Get SRRG Pool by fdn	/restconf/data/v1/cisco-resource-network:srrg-pool?fdn=<value>
Get SRRG Pool by pool type reference	/restconf/data/v1/cisco-resource-network:srrg-pool?pool-type-ref=<value>
Get All SRRG Pool Type	/restconf/data/v1/cisco-resource-network:srrg-pool-type
Get SRRG Pool type by fdn	/restconf/data/v1/cisco-resource-network:srrg-pool-type?fdn=<value>
Performance Metrics for Topological	

Link	
Get Performance metrics for a given Topological Link	/restconf/data/v1/cisco-resource-network:perf-metrics?tlFdn=<value>
MediaType Controller	
Get/Update MediaType Controller	/restconf/data/v1/cisco-nrf-controller:controller-port
LMP Link	
Create LMP Link	/restconf/operations/v1/cisco-resource-activation:lmp-link-resource
Delete LMP Link	/restconf/operations/v1/cisco-resource-activation:lmp-link-resource?fdn=<lmpFdn>
Retrieve LMP Link	/restconf/data/v1/cisco-resource-network:topological-link?fdn=< lmpFdn>
AINS – Automatic In-Service	
Equipment Reserve Operation/ AINS Equipment	/restconf/operations/v1/cisco-nrf-physical:reserve-equipment
Device Synchronization	
Device Synchronization	/restconf/operations/v1/cisco-nrf-physical:synchronize-node
Resync-service	
Resync-service	/restconf/operations/v1/network-service:resync-service
Service tests – OTDR, OAM, Ping and Trace	
OTDR	/restconf/operations/v1/cisco-network-resource-oam:network-resource-oam-config
LSP ping and traceroute	/restconf/operations/v1/cisco-service-oam:service-oam-config
CFM/PW/Tunnel OAM/Device OAM (Server to Device and NE-to-NE) ping and traceroute	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext

Optical TerminationPoint Layer Rates Name Change

Following is list of legacy and currently supported layer rates for optical TerminationPoint.
e.g.,
Legacy layer rate:
<ns9:fdn>MD=CISCO_EPNM!ND=cvg-frodo-
235.cisco.com!CTP=name=ODU00/1/0/13;lr=**LR_OCH_DATA_UNIT_0**</ns9:fdn>

Currently supported layer rate:
<ns9:fdn>MD=CISCO_EPNM!ND=cvg-frodo-235.cisco.com!CTP=name=ODU00/1/0/13;lr=**lr-och-data-unit-
0**</ns9:fdn>

For complete supported layer rate set, see cisco-layer-rates.yang and cisco-optical-circuit-
extensions.yang

Legacy Layer Rates (Until release 2.1)	Updated Layer Rates (Release 2.2 onwards)
LR_OCH_DATA_UNIT_0	lr-och-data-unit-0
LR_OCH_DATA_UNIT_1	lr-och-data-unit-1
LR_OCH_DATA_UNIT_1E	lr-och-data-unit-1e
LR_OCH_DATA_UNIT_1F	lr-och-data-unit-1f
LR_OCH_DATA_UNIT_2	lr-och-data-unit-2
LR_OCH_DATA_UNIT_2E	lr-och-data-unit-2e
LR_OCH_DATA_UNIT_2F	lr-och-data-unit-2f
LR_OCH_DATA_UNIT_3	lr-och-data-unit-3
LR_OCH_DATA_UNIT_3E1	lr-och-data-unit-3e1
LR_OCH_DATA_UNIT_3E2	lr-och-data-unit-3e2
LR_OCH_DATA_UNIT_4	lr-och-data-unit-4
LR_OCH_DATA_UNIT_C2	lr-och-data-unit-c2
LR_OCH_DATA_UNIT_FLEXIBLE	lr-och-data-unit-flex
LR_OCH_TRANSPORT_UNIT_0	lr-och-transport-unit-0
LR_OCH_TRANSPORT_UNIT_1	lr-och-transport-unit-1
LR_OCH_TRANSPORT_UNIT_1E	lr-och-transport-unit-1e
LR_OCH_TRANSPORT_UNIT_1F	lr-och-transport-unit-1f
LR_OCH_TRANSPORT_UNIT_2	lr-och-transport-unit-2
LR_OCH_TRANSPORT_UNIT_2E	lr-och-transport-unit-2e
LR_OCH_TRANSPORT_UNIT_2F	lr-och-transport-unit-2f
LR_OCH_TRANSPORT_UNIT_3	lr-och-transport-unit-3
LR_OCH_TRANSPORT_UNIT_3E1	lr-och-transport-unit-3e1
LR_OCH_TRANSPORT_UNIT_3E2	lr-och-transport-unit-3e2
LR_OCH_TRANSPORT_UNIT_4	lr-och-transport-unit-4
LR_OCH_TRANSPORT_UNIT_C2	lr-och-transport-unit-c2
LR_OPTICAL_CHANNEL	lr-optical-channel
LR_OPTICAL_MULTIPLEX_SECTION	lr-optical-multiplex-section
LR_OPTICAL_SECTION	lr-optical-section
LR_OPTICAL_TRANSMISSION_SECTION	lr-optical-transmission-section
LR_OPTICALPHYSICALSECTION	lr-optical-physical-section
LR_OPTICALPHYSICALSECTION_MULTILANE	lr-optical-physical-section-multilane
LR_PHYSICAL_OPTICAL	lr-optical-physical
LR_DSR_10GIGABIT_ETHERNET	lr-dsr-10gigabit-ethernet
LR_DSR_100GIGABIT_ETHERNET	lr-dsr-100gigabit-ethernet
LR_DSR_FAST_ETHERNET	lr-dsr-fast-gigabit-ethernet
LR_DSR_GIGABIT_ETHERNET	lr-dsr-gigabit-ethernet

TerminationPoint default attributes

Following attributes are legacy attributes and will not be useful henceforth.

is-edge-point
is-promiscuous
is-span-monitored
duplex-mode
alias-name
flow-control

Optical Ethernet termination point and equivalent layer-rate

Optical Ethernet TerminationPoint of DWDM devices (e.g. NCS2k), layer-rate are aligned with packet ethernet TerminationPoint layer-rate, following table have the mapping

Legacy Optical Ethernet Layer Rates (Until release 3.0)	Updated Optical Ethernet Layer Rates (Release 3.1 onwards)
lr-dsr-fast-gigabit-ethernet	lr-hundred-megabit-ethernet
lr-dsr-10gigabit-ethernet	lr-ten-gigabit-ethernet
lr-dsr-25gigabit-ethernet	lr-twentyfive-gigabit-ethernet
lr-dsr-40gigabit-ethernet	lr-forty-gigabit-ethernet
lr-dsr-100gigabit-ethernet	lr-hundred-gigabit-ethernet
lr-dsr-gigabit-ethernet	lr-gigabit-ethernet

Example of an optical Termination Point FDN:
e.g : **MD=CISCO_EPNM!ND=cvg-bosshogg-101.cisco.com!CTP=name=HundredGigECtrlr0/0/0/2;lr=lr-hundred-gigabit-ethernet**

Termination point response with Actual wavelength attribute

From 5.1 version of EPNM, Termination point response with actual wavelength attribute with default value will be "First Tunable Wavelength". Earlier version used to be 0.0

5.1 version sample
<actual-wave-length>First Tunable Wavelength</actual-wave-length>

Pre 5.1 version sample
<actual-wave-length>0.0</actual-wave-length>

RESTCONF Interface Details

This section provides details about the supported RESTCONF interfaces.

1.14 YANG Module List Retrieval

This interface, defined by the RESTCONF specification, retrieves a list of YANG modules supported by Cisco EPN Manager. A YANG module defines how a portion of the data store is structured on the server. Use this information to discover the RESTCONF interfaces implemented on the server. See RFC 7895, Yang Module Library for more information about this interface.

Note: YANG modules are not to be confused with the Module object defined by EPN-M to model a line card.

Resource	Description
modules-state	Retrieves list of interfaces exposing YANGs.
HTTP Method	**Resource Path**
GET	/restconf/data/ietf-yang-library:modules-state
Query Parameters	
None	
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more module descriptions of type model – see the RESTCONF Specification for details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.

Yang Module Data

Name	Type	Description
Module	Container element	Holds the data for YANG module description.

Request/Response

Request

GET /restconf/data/ietf-yang-library:modules-state HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

• samples/Get_All_Module_States/response.xml

1.15 RESTCONF Protocol Capabilities

As mandated in RESTCONF RFC 8040, Cisco EPN Manager supports an interface to retrieve the optional functions supported by the server. Cisco EPN Manager supports a limited form of the depth parameter (depth=1) to allow

efficient retrieval of entities without traversing collections. It also reports that the server returns all populated leaf values (default values are not suppressed). This is part of the RESTCONF Monitoring Module described in Section 9.3 of RFC 8040.

Resource	Description
restconf-state/capabilities	Retrieves list of optional features.
HTTP Method	**Resource Path**
GET	/restconf/data/ietf-restconf-monitoring:restconf-state/capabilities
Query Parameters	
None	
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more capability URIs– see the RESTCONF RFC 8040 Section 9.1 for details.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.

Yang Module Data

Name	Type	Description
List a capability URIs	List elements	Describes optional feature support proved by server

1.16 RESTCONF Stream Resources

As mandated in RESTCONF RFC 8040, Cisco EPN Manager supports an interface to retrieve the optional stream resources supported by the server. These resources are:
- Attribute Value Change (AVC) Notifications for create, update, and delete notifications of inventory data resources. See the section on notifications for details.
- Service Activation Notifications for results of service create, modify, and delete actions through the operations interface. See the section on notifications.
- Template-base Configuration Notifications for the results of configuration change request through the operation interface. See the section on notifications.
- All is a convenience interface to register for all notifications.

The notification received by the user are restricted by his/her permissions based on device access permitted by the user's virtual domain(s).

Resource	Description
restconf-state/capabilities	Retrieves list of supported streams.
HTTP Method	**Resource Path**
GET	/restconf/data/ietf-restconf-monitoring:restconf-state/streams
Query Parameters	
None	
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more capability URIs – see the RESTCONF RFC 8040 Section 9.1 for details.
HTTP Status Code	• 200 OK - Success with response message-body

	• 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.

Yang Module Data

Name	Type	Description
List a capability URIs	List elements	Describes optional feature support proved by server.

1.17 Group Retrieval

This interface provides the operations required to retrieve the details of groups of nodes. Each group object contains identifying information and a list of Fully Distinguished Names of the nodes in the group. Nodes may appear in more than one group. Groups are created through the graphical user interface (GUI) and through this API. The Group may contain information about the physical location of the group by street address and/or latitude and longitude. The RESTCONF API also supports creating, updating, and deleting Groups. See RFC 8040 Sections 4.4, 4.5, and 4.7 for information about POST, PUT, and DELETE processing in RESTCONF.

Resource	Description	
Group	Retrieves groups of the nodes in the system.	
HTTP Method	**Resource Path**	
GET, POST, PUT, DELETE	/restconf/data/v1/cisco-resource-physical:group	
Query Parameters		
Name	**Type**	**Description**
fdn	String	Fully Distinguished Name (FDN) of the group to retrieve.
name	String	Name of the group to retrieve (unique).
description	String	Description of the group to retrieve (not unique).
Message Body (POST, PUT)		
Group	Group	Data to create or update the Group.
Authorization Required	'Add Groups' for HTTP Methods GET, PUT, POST 'Modify Groups' for HTTP Methods GET, POST, PUT 'Delete Groups' for HTTP Methods GET, DELETE	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more groups of type group – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials	

	For complete list of error-app-tag and error message refer to [EPNM 7.1.1 NB API Error Codes Reference.xlsx](#)
Yang file name	cisco-physical-node.yang

Group Data

Name	Type	Description
Group	Container element	Holds the data for group.

Get All Groups Request/Response

Request

GET /restconf/data/v1/cisco-resource-physical:group HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

- [samples/Get_All_Groups/response.xml](#)

1.18 Node Retrieval

This interface provides the operations required to retrieve node details. Each node object contains its own attributes and contains a list of the equipment instances contained within it. A node may contain the latitude and longitude of its physical location. Nodes are created through discovery of devices whose credentials are entered into the system through the graphical user interface (GUI). The RESTCONF API for nodes is read-only.

Note: Nodes were previously known as Managed Elements. The name was changed to align with the IETF standards.

Resource	Description	
Node	Retrieves the Nodes in the system.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-physical:node	
Query Parameters		
Name	**Type**	**Description**
fdn	String	Fully Distinguished Name (FDN) of the Node to retrieve.
name	String	Name of the Node to retrieve (unique).
description	String	Description of the Node to retrieve (not unique).
<attribute>	Varies	Uses any non-collection attribute to retrieve Node object(s).
Authorization Required	One or more from following - Chassis View Read - Chassis View Read and Write - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting - Network Topology - Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more Nodes of type **node** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body	

	• 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-physical-node.yang

Node Data

Name	Type	Description
Node	Container element	Holds the data for a node.

Get All Nodes Request/Response

1.18.1.1 *Request*

GET /restconf/data/v1/cisco-resource-physical:node HTTP/1.1
Host: \<epnm-host\>
Accept: application/yang-data+xml
Authorization: Basic …

1.18.1.2 *Response*

HTTP/1.1 200 OK
Server: \<epnm-host\>
Content-Type: application/yang-data+xml

• samples/Get_All_Nodes/response.xml

1.19 Equipment Retrieval

This interface provides the operations required to retrieve equipment details. Each equipment object contains its own attributes and contains a list of FDN of the equipment instances contained within it. If it is contained within another equipment instance, the FDN of that instance is shown. Equipment may contain physical connectors (explained below). Equipment is created through discovery on devices whose credentials are entered into the system through the graphical user interface (GUI). The RESTCONF API for equipment is read-only.

Note: Equipment is a super class of Chassis and Module. This interface retrieves Chassis, Module, and Equipment objects.

Resource	Description	
Equipment	Retrieves the Equipment in the system.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-physical:equipment	
Query Parameters		
Name	**Type**	**Description**

fdn	String	Fully Distinguished Name (FDN) of the Equipment to retrieve.
name	String	Name of the Equipment to retrieve (not unique).
description	String	Description of the Equipment to retrieve (not unique).
<attribute>	Varies	Uses any non-collection attribute to retrieve Equipment object(s).
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more Equipment of type **equipment** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-physical-equipment.yang	

Equipment Data

Name	Type	Description
Equipment	Container element	Holds the data for an Equipment instance.

Get All Equipment Request/Response

Request

GET /restconf/data/v1/cisco-resource-physical:equipment HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

- samples/Get_All_Equipment/response.xml

1.20 Chassis Retrieval

This interface provides the operations required to retrieve Chassis details. Each Chassis object contains its own attributes and contains a list of FDN of the equipment instances contained within it. Typically, a chassis object is contained directly by a node and does not have a containing equipment FDN. Chassis are created through discovery on devices whose credentials are entered into the system through the graphical user interface (GUI). The RESTCONF API for chassis is read-only.

Note: Chassis is a subclass of Equipment. This interface retrieves only Chassis objects along with any additional attributes defined for Chassis.

Resource	Description	
Equipment	Retrieves the Chassis instances in the system	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-physical:chassis	
Query Parameters		
Name	**Type**	**Description**
fdn	String	Fully Distinguished Name (FDN) of the Chassis to retrieve.
name	String	Name of the Chassis to retrieve (not unique).
description	String	Description of the Chassis to retrieve (not unique)
<attribute>	Varies	Uses any non-collection attribute to retrieve Chassis object(s).
Authorization Required	One or more from following - Chassis View Read - Chassis View Read and Write - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting - Network Topology - Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more Chassis of type **chassis** – see yang model for the data details.	
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-physical-equipment.yang	

Chassis Data

Name	Type	Description

Chassis	Container element	Holds the data for a Chassis.

Get All Chassis Request/Response

Request

GET /restconf/data/v1/cisco-resource-physical:chassis HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

- samples/Get_All_Chassis/response.xml

1.21 Module Retrieval

This interface provides the operations required to retrieve module details. Each module object contains its own attributes and contains a list of FDN of the equipment instances contained within it. Typically, a module object is contained within an equipment object and has a Containing equipment FDN. Equipment containing physical connectors (explained below) are often but not always Modules. Modules are created through discovery on devices whose credentials are entered into the system through the graphical user interface (GUI). The RESTCONF API for module is read-only.

Note: Module is sub class of Equipment. This interface retrieves only Module objects along with any additional attributes defined for Module.

Resource	Description	
Module	Retrieves the Modules in the system.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-physical:module	
Query Parameters		
Name	**Type**	**Description**
fdn	String	Fully Distinguished Name (FDN) of the Module to retrieve.
name	String	Name of the Module to retrieve (not unique).
description	String	Description of the Module to retrieve (not unique).
<attribute>	Varies	Uses any non-collection attribute to retrieve Module object(s).
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more Modules of type **module** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	

Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.
	If error is from underlying framework/core modules error-app-tag format one of following
	• FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
	• CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
	For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-physical-equipment.yang

Module Data

Name	Type	Description
Module	Container element	Holds the data for a Module.

Get All Modules Request/Response

Request

GET /restconf/data/v1/cisco-resource-physical:module HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

- samples/Get_All_Module/response.xml

1.22 Physical Connector Retrieval

This interface provides the operations required to retrieve PhysicalConnector details. A physical connector represents a connector capable of transmitting signals or power. Each PhysicalConnector object contains its own attributes and the FDN of the equipment instance that contains it. Equipment containing PhysicalConnectors are often but not always Modules. PhysicalConnectors are created through discovery on devices whose credentials are entered into the system through the graphical user interface (GUI). The RESTCONF API for PhysicalConnectors is read-only.

Note: PhysicalConnector is not a subclass of Equipment.

Resource	Description	
PhysicalConnector	Retrieves the PhysicalConnectors in the system.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-physical:physicalconnector	
Query Parameters		
Name	**Type**	**Description**
fdn	String	Fully Distinguished Name (FDN) of the Module to retrieve.
name	String	Name of the PhysicalConnector to retrieve (not unique).
description	String	Description of the PhysicalConnector to retrieve (not unique).
<attribute>	varies	Uses any non-collection attribute to retrieve PhysicalConnector object(s).
Authorization	One or more from following	

Required	• Chassis View Read
	• Chassis View Read and Write
	• Circuit or VC Provisioning
	• Circuit or VC Monitoring and Troubleshooting
	• Network Topology
	• Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more PhysicalConnectors of type **physical-connector** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body
	• 401, 403 – Authentication and Authorization errors.
	• 400 Bad Request - Invalid request message.
	• 500 Internal Server Error - operation-failed.
	Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.
	If error is from underlying framework/core modules error-app-tag format one of following
	• FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
	• CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
	For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-physical-equipment.yang

PhysicalConnector Data

Name	Type	Description
physical-connector	Container element	Holds the data for a PhysicalConnector.

Get All Physical Connectors Request/Response

Request

GET /restconf/data/v1/cisco-resource-physical:physicalconnector HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

• samples/Get_All_Physical_Connectors/response.xml

1.23 Optical Network Element Settings

This interface provides the operations to retrieve the node type of optical devices. The node-fdn attribute identifies the associated node object. The node-type indicates the role of the device in an optical network. The node-type

attribute was not added to the node object to avoid adding optical-specific information to node objects that are not optical devices.

By default, this interface returns the node object as well as the above two attributes. If you are not interested in the node information, you can suppress it with the ?.depth=1 query string. (See example, below.)

Resource	Description
OpticalNESettings	Retrieves the settings information for optical nodes in the system.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-resource-optical:optical-nesettings
Query Parameters	

Name	Type	Description
node-fdn	String	Fully Distinguished Name (FDN) of the associated node.
node-type	String	Optical node type, e.g.: ROADM (not unique).
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices	

Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more OpticalNESetting objects of type **optical-nesettings** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-resource-optical.yang

Optical Network Element Settings Data

Name	Type	Description
optical-nesettings	Container element	Holds the data for optical network elements settings

Get All Optical Network Element Settings Request/Response

Request

GET /restconf/data/v1/cisco-resource-optical:optical-nesettings HTTP/1.1
Host: <epnm-host>

Accept: application/yang-data+xml
Authorization: Basic …

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

- samples/Get_All_Optical_Network_Element_Settings/response.xml

1.24 TerminationPoint Retrieval

This interface provides the operations required to retrieve TerminationPoint details.

Resource	Description	
TerminationPoint	Retrieves TerminationPoints in the system.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-ems:termination-point	
Query Parameters		
Name	**Type**	**Description**
fdn	String	Fully Distinguished Name (FDN) of the terminationPoint to retrieve a single terminationPoint. FDN = 'MD=<CISCO_EPNM>!ND=<nodename>!<type>=<tpname>
type	String (CTP, PTP, FTP)	Type of the termination points to retrieve.
ndFdn	String	Fully Distinguished Name (FDN) of the Node. FDN = 'MD=<CISCO_EPNM>!ND=<nodename>
layerRate	String	Layer rate of the termination point to retrieve. e.g. lr-ten-gigabit-ethernet
containedCTP	String(true/false)	Enables you to return Contained Connection Termination Points for a given Termination Point.
containedInUseCTP	String(true/false)	Enables you to return Contained In Use Connection Termination Points for a given Termination Point.
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more terminationPoints of type **termination-point** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TP.<number> are generated by this API. For example:	

	TP.0004 for 'Invalid TerminationPoint - FDN: %s - name is missing.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-termination-point.yang

TerminationPoint Data

Name	Type	Description
termination-point	Container element	Holds the data for physical and floating terminationPoint.
connection-termination-point	Container element	Holds the data for connection terminationPoint.

Get All Physical Termination Points Request/Response

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?type=PTP HTTP/1.1

Response

- samples/Get_All_Physical_Termination_Points/response.xml

Get All Physical Termination Points for Device Request/Response

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?type=PTP&ndFdn=\<Node FDN\> HTTP/1.1

Response

- samples/Get_All_Physical_Termination_Points_for_Device/response.xml

Get All Floating Termination Points Request/Response

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?type=FTP HTTP/1.1

Response

- samples/Get_All_Floating_Termination_Points/response.xml

Get All Floating Termination Points for Device Request/Response

Request

- GET /restconf/data/v1/cisco-resource-ems:termination-point?type=FTP&ndFdn=\<Node FDN\> HTTP/1.1

Response

- samples/Get_All_Floating_Termination_Points_for_Device/response.xml

Get All Connection Termination Points Request/Response

Request

- GET /restconf/data/v1/cisco-resource-ems:termination-point?type=CTP HTTP/1.1

Response

- samples/Get_All_Connection_Termination_Points/response.xml

Get All Connection Termination Points for Device Request/Response

Request

- GET /restconf/data/v1/cisco-resource-ems:termination-point?type=CTP&ndFdn=<Node FDN> HTTP/1.1

Response

- samples/Get_All_Connection_Termination_Points_for_Device/response.xml

Get Single Termination Point Request/Response

Request

- GET /restconf/data/v1/cisco-resource-ems:termination-point? fdn=<Termination Point FDN> HTTP/1.1
  e.g., Termination Point FDN = MD=CISCO_EPNM!ND=NCS4206-TEST-120.33!CTP=name=CEM-PG57:16002;lr=lr-cem-grp
- Host: <epnm-host>
- Accept: application/yang-data+xml

Response

- samples/Get_Single_Termination_Point/response.xml

Get Contained Connection Termination Point Request/Response

Request

- GET /restconf/data/v1/cisco-resource-ems:termination-point? fdn=<Termination Point FDN> &containedCTP=true HTTP/1.1
  Ex Termination Point FDN = > MD=CISCO_EPNM!ND=NCS4206-TEST-120.33!PTP=name=SONET 0/5/6;lr=lr-dsr-oc48-and-stm16

Host: <epnm-host>
Accept: application/yang-data+xml

Response

- samples/Get_Contained_Connection_Termination_Points/response.xml

Get Contained in use Connection Termination Point Request/Response

Request

- GET /restconf/data/v1/cisco-resource-ems:termination-point? fdn=<Termination Point FDN> &containedInUseCTP=true HTTP/1.1

  Ex Termination Point FDN = > MD=CISCO_EPNM!ND=NCS4206-TEST-120.33!PTP=name=SONET 0/5/6;lr=lr-dsr-oc48-and-stm16

Host: <epnm-host>
Accept: application/yang-data+xml

Response

- samples/Get_Contained_in_use_Connection_Termination_Points/response.xml

Get All Termination Point for a Layer-Rate Request/Response

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?layerRate=<layer rate value> HTTP/1.1
Ex: layerRate=lr-optical-section
Host: <epnm-host>
Accept: application/yang-data+xml

Response

- samples/Get_All_Terminatin_Points_for_a_Layer_Rate/response.xml

Get All Termination Point with MPLSTE attributes Response

TerminationPoint retrieval can expose MPLSTE attributes through getTerminationPoint API.

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml

Response

- samples/Get_Tp_With_MPLSTE_Attributes_ISIS/response.xml
- samples/Get_Tp_With_MPLSTE_Attributes_ISIS/response.json
- samples/Get_Tp_With_MPLSTE_Attributes_OSPF/response.xml
- samples/Get_Tp_With_MPLSTE_Attributes_OSPF/response.json

Get Termination Point for AINS

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?fdn=<TpFdn> HTTP/1.1
Ex: fdn=TpFdn
Host: <epnm-host>
Accept: application/yang-data+xml

Response

- samples/Get_Tp_With_Ains/response.xml
- samples/Get_Tp_With_Ains/response.json

Get Termination Point for GMPLS

In order to retrieve gmpls attribute using getTP API for CISCO NCS 1004 devices, use layer rate "lr-optical-section" and to retrieve attributes like "baud-rate" and "bits-per-symbol" use layer rate "lr-optical-channel" in TpFdn used in query param.

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?fdn=<TpFdn> HTTP/1.1
Ex: fdn=TpFdn
Host: <epnm-host>
Accept: application/yang-data+xml

Response

- samples/Get_Tp_Gmpls_BaudRate_BitsPerSymbol/getTp-gmpls-response.xml
- samples/Get_Tp_Gmpls_BaudRate_BitsPerSymbol/getTp-baudRate-bitsPerSymbol-response.xml

Get Termination Point for Optics Port on ZR/ZR+ pluggable for SVO

In order to retrieve OCH attributes using getTP API, use layer rate "lr-optical-section" in fdn used in query param.

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?fdn=<TpFdn> HTTP/1.1
Ex: fdn=<TpFdn>
Host: <epnm-host>
Accept: application/yang-data+xml

Response

- samples/Get_Tp_Optics_ZR_ZRPlus_Pluggable_SVO/response.xml

1.25 Set TerminationPoint

This interface provides the operations required to set attributes on a given TerminationPoint.

Resource	Description
TerminationPoint	Set TerminationPoint
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:set-termination-point
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	The modified **termination-point** – see yang model for the data details. And result of modification on the feature.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.

| | Error tag with format TP.<number> are generated by this API. For example: TP.0029 for 'Set TerminationPoint Data Operation Failed: %s.'

If error is from underlying framework/core modules error-app-tag format one of following
•   FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
•   CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
•   RA.<number> - any tag starting with "RA." prefix for any internal errors like RA.0001=Operation is not supported.

For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx |
| Yang file name | cisco-termination-point.yang |

Set TerminationPoint Input Data

The table below provides the parameters that can be set on the Interfaces using the set-termination-point operation.

The PortConfig attribute in the request determines the group to which the attributes belong. The Sample Request/Response provided will give the different scenarios.

Parameter Name	Type	Allowed Values	Description
Port Config: **SONET_PORT_CONFIG**			
adminStatus	String	UP DOWN	Used to specify the admin status for the given TP. Can be set separately.
operStatus	String	UP DOWN	Specifies the operational status of the TP. Can be set separately.
loopBack	String		Specifies the values to be set for the loopBack. Can be set separately.
portMode	ENUM	SONET ETHERNET OTN	Indicates the portMode for the TP. Can be set separately.
SONET Port Parameters **portConf:** **SONET_PORT_CONFIG**			
framing	String	AUTO_DETECT C_BIT M23 DSX1_ESF DSX1_SF M23 CRC CRC4 GFP GFP_F GFP_T HDLC NO_CRC NOT_APPLICABLE UNFRAMED	Specifies the Framing for the TP. Has to be set with the clockSource value. **Note:** Cannot be set individually.
clockSource	String	LINE	Specifies the clock source

		INTERNAL RECOVERED FREE_RUNNING ENHANCED	for the TP. Has to be set if framing is being set. **Note:** Cannot be set individually.
rate	String	OC3 OC12 OC48 OC192	Indicates the rate to be set. Has to be set if clockSource and framing are being set. **Note:** Cannot be set individually.
loopBack	String	NETWORK NETWORK_LINE LOCAL NETWORK_PAYLOAD REMOTE REMOTE_LINE REMOTE_PAYLOAD	Indicates the loop back value to be set for the TP. Can be set separately.
SONET APS Parameters **portConfig:** **SONET_PORT_CONFIG**			
protectionGroupNumber	Integer	Range(0..255)	Mandatory for APS setting.
protectionRole	String	PRIMARY SECONDARY	Mandatory for APS setting.
protectionLoopBackIP	String	IP Address	Optional for APS setting.
protectionRevertiveTime	Integer	Range(1..255)	Optional for APS setting.
SONET LOP / HOP Parameters **portConfig:** **SONET_LOP_CONFIG – for LOP** **SONET_HOP_CONFIG – for HOP**			
mode	ENUM	Unframed, VT1.5, CT3, T3	
loopBack	ENUM	LINE, NETWORK, REMOTE	
operStatus	ENUM	UP,DOWN	
adminStatus	ENUM	UP,DOWN	Changing "adminStatus" value is not supported for XE devices with software version 16.8 onward.
framing	ENUM	Auto-Detect, M23, C-Bit	
clockSource	ENUM	LINE, INTERNAL, RECOVERED, ENHANCED	
T1 / T3 Parameters **portConfig:** **T1_PORT_CONFIG – for T1** **T3_PORT_CONFIG – for T3**			
loopBack	ENUM	LINE, NETWORK, REMOTE	
operStatus	ENUM	UP,DOWN	
adminStatus	ENUM	UP,DOWN	
framing	ENUM	Auto-Detect, M23, C-Bit	
clockSource	ENUM	LINE, INTERNAL, RECOVERED,	

		ENHANCED	
Ethernet Parameters **portConfig** **ETHERNET_PORT_CONFIG**			
loopback	ENUM	NO_LOOPBACK, OTHER, INTERNAL, LINE, DROP	
adminStatus	ENUM	UP,DOWN	
speed	ENUM	AUTOSPEED	
duplexMode	ENUM	HALFDUPLEX,FULLDUPLEX	
ODU Port Config Parameters **portConfig** **ODU_PORT_CONFIG**			
gcc	String	True (DEFAULT), false (remove the controller). **NOTE**: This attribute is mandatory for setting ODU parameters.	
tsg	String	-	
ttiSent	String	-	
ttiSapiSent	String	-	
ttiDapiSent	String	-	
ttiOperatorSent	String	-	
ttiExpected	String	-	
ttiSapiExpected	String	-	
ttiDapiExpected	String	-	
ttiOperatorExpected	String	-	
ttiStringTypeSent	ENUM	ASCII, HEX	This attribute is mandatory for setting ODU parameters of NCS1004 to update TTI functionality on OTN-XP card.
ttiStringTypeExpected	ENUM	ASCII, HEX	**NOTE**: This attribute is mandatory for setting ODU parameters of NCS1004 to update TTI functionality on OTN-XP card.
isTimActionEnabled	String	False (Default), True	Enables the PM TIM CA. This attribute is mandatory for setting ODU parameters of NCS1004 to update TTI functionality on OTN-XP card, and it is applicable to ODU mappers for Ethernet controllers.
SONET SDH Parameters **portConfig** **SONET_SDH_PORT_CONFIG**			
clockSource	ENUM	LOOP_TIMING, LOCAL_TIMING, LINE_TIMING, INTERNAL_TIMING	

Packet Termination Parameters **portConfig** **ODU_PACKET_TERMINATION** **_PORT_CONFIG**			
terminationMode	ENUM	ETHERNET	
mapping	ENUM	GMP	
Ethernet FlowControl Parameters **portConfig** **ETHERNET_FLOWCONTROL_** **PORT_CONFIG**			
flowControl	ENUM	BIDIRECTIONAL, EGRESS, INGRESS	
WaveLength Parameters **portConfig** **WAVELENGTH_PORT_CONFIG**			
waveLength	Float		
TTi Parameters **portConfig** **TTI_PORT_CONFIG**			
trcLevel	String	Permitted values: • J0 • TTI-SM • TTI-PM **NOTE**: This attribute is mandatory for setting tti.	
trcMode	String	Permitted values: • AUTO • AUTO-NO-AIS • MAN • MAN-NO-AIS • OFF **NOTE**: This attribute is mandatory for setting tti.	
ttiExpected	String	Free format. **NOTE**: This attribute is mandatory for setting tti.	
ttiSent	String	Free format. **NOTE**: This attribute is mandatory for setting tti.	
TCM Control Parameters **portConfig** **TCMCONTROL_PORT_CONFIG**			Applicable only for NCS4K devices
tcmId	Integer	Indicates the tandem connection monitoring field of the ODUk OH on which non-intrusive monitoring is performed. Valid values are integers from 1 to 6.	
tcmName	String	Tcm name	
tcmState	String	DISABLED, ENABLED	

perfMon	String	DISABLED, ENABLED	
signalDegradeBert	String	Signal degrade BER threshold - E_3, E4, E_5, D_6, E_7, E_8, and E_9.	
signalFailureBert	String	Signal failure BER threshold - E_3, E4, E_5, D_6, E_7, E_8, and E_9.	
ttiSent	String	Free format string.	
ttiSapiSent	String	Free format string.	
ttiDapiSent	String	Free format string.	
ttiOperatorSent	String	Free format string.	
ttiExpected	String	Free format string.	
ttiSapiExpected	String	Free format string.	
ttiDapiExpected	String	Free format string.	
ttiOperatorExpected	String	Free format string.	
ALS Parameters portConfig ALS_PORT_CONFIG			
alsMode	ENUM	DISABLED, AUTO, MANUAL_RESTART, MANUAL_RESTART_FOR_TEST.	
alsRecoveryInterval	Float	Value Ranging from 60.0 to 300.0.	
alsRecoveryPulseWidth	Float	Value Ranging from 2.0 to 100.0.	
NNI Control Parameters portConfig NNI_CONTROLLER_PORT_CONFIG			
nniControl			
ttiMode	String	TTI Mode – one of the following values SM, PM, TCM_1, TCM_2, TCM_3, TCM_4, TCM_5, TCM_6.	
adminWeight	String	<0-65535> Admin weight value.	
Optical Payload Parameters portConfig OPTICAL_PAYLOAD_PORT_CONFIG			
portMode	ENUM	One of the following values: ETHERNET, ETHERNET_PACKET , FC, OTN,SDH, SONET, BREAKOUT and NONE (for removing breakout lane). **NOTE**: This attribute is mandatory along with laneNumber for	

		identifying the lanes and its portMode.	
framing	ENUM	One of the following values: OPU0, OPU1, OPU1E, OPU2, OPU3, OPU3E1, OPU3E2, OPU4, OPU4FLEX, OPUFlex, OPU1F, OPU2F, OPUC2, OPUC4,PACKET and NONE (for removing breakout lane).	
mapping	String	One of the following values: BMP, GMP, GFPF, GFPT, WIS. HDLC. HDLC_LEX, HDLC_X86, CBR, TRP, AMP and NONE (for removing breakout lane).	
rate	String	One of the following values: OC3, OC12, OC48, OC192, STM1, STM4, STM16, STM64, OC768 , STM256 , FC_1G, FC_2G, FC_4G, FC_8G, FC_10G, FICON_1G, FICON_2G , FICON_4G , ESCON , GIGE, GIGE_10 , GIGE_40 , GIGE_100 , HDTV , GIB_5 , IB, D1VIDEO , VIDEO_3G, DV6000, ETRCLO , ISCCOMPAT, ISC3PEER2R, ISC3PEER1G, ISC3PEER2G , ISC3STP1G , ISC3STP2G, PASSTHRU , DVBASI , ISC1 , OCH , OTU2 , OTU3 , OTU4, OTU4C2 , OTU1, ILK , SDSDI , HDSDI , FSTE , FC_16G , and NONE (for removing breakout lane).	
ODU Channelization portConfig ODU_CHANNELIZE_PORT_CONFIG			
channelize_ODU	Boolean		Optional attribute should be set to 'True' for creating the channel and 'false' for removing ODU channel.
ODU_Channel	String		Channel values eg: /ODU/0/1/2.

oduLayer	ENUM		Possible values: ODU0, ODU1, ODU2, ODU-FLEX, ODU1E, ODU2E, ODU2F, ODU3, ODU3E1, ODU3E2.
tpn	NUMBER		Tributary Port Number, possible values: 1-80.
tps	String		Tributary Slots, Tributary slot string separated by (:) or (-) from 1 to no of Time Slots in Parent ODU controller. Eg: 3:4
Admin State portConfig **ADMIN_STATE_PORT_CONFIG**			
adminStatus	ENUM	UP, DOWN	Optical interfaceAdmin status can be either UP or DOWN.
Sonet SDH portConfig **SONET_SDH_PORT_CONFIG**			
clockSource	ENUM	LOCAL_TIMING, LINE_TIMING, INTERNAL_TIMING	
OTN portConfig **OTN_PORT_CONFIG**			
fec	ENUM	STANDARD,ENHANCED,ENHANCED_I_4,ENHANCED_I_7, STANDARD,ENHANCED,ENHANCED_I_4,ENHANCED_I_7 NONE	
payloadmap	ENUM	ASYNC,ODU, SYNC, NOTAPPLICABLE	
admssm	ENUM	SMC, DUS, PRS, RES, ST2, ST3E, STU, TNC, SETS, G811, G812L, G812T	
syncmsg	Boolean	True or false	
gG709	Boolean	True or false	
gcc0	Boolean	True or false	
sdber	ENUM	E_3,E_4,E_5,E_6, E_7,E_8, E_9	
trcMode	String	Permitted values: • AUTO • AUTO-NO-AIS • MAN • MAN-NO-AIS • OFF **NOTE**: This attribute is mandatory for setting tti.	

trcLevel	String	Permitted values: • J0 • TTI-SM • TTI-PM **NOTE**: This attribute is mandatory for setting tti.	
ttiSapiSent	String	Free format string.	
ttiDapiSent	String	Free format string.	
ttiOperatorSent	String	Free format string.	
ttiSapiExpected	String	Free format string.	
ttiDapiExpected	String	Free format string.	
ttiOperatorExpected	String	Free format string.	
ttiStringTypeSent	ENUM	ASCII, HEX	This attribute is mandatory for setting ODU parameters of NCS1004 to update TTI functionality on OTN-XP card.
ttiStringTypeExpected	ENUM	ASCII, HEX	This attribute is mandatory for setting ODU parameters of NCS1004 to update TTI functionality on OTN-XP card.
BreakOut portConfig **BREAKOUT_LANE_PORT_CONFIG**			
portMode	ENUM	One of the following values: ETHERNET, FC, OTN, SDH, SONET, and NONE (for removing breakout lane). **NOTE**: This attribute is mandatory along with laneNumber for identifying the lanes and its portMode.	
framing	ENUM	NONE,OPU0,OPU1,OPU1E, OPU1F	
rate	ENUM	OC3, OC12, OC48, OC192, STM1, STM4, STM16, STM64	
mapping	ENUM	BMP, GMP, GFPF, GFPT, WIS, HCLC, CBR, TRP, NONE	
laneNumber	Number		
LoopBack portConfig **LOOP_BACK_PORT_CONFIG**			
loopBack	ENUM	NO_LOOPBACK, OTHER, INTERNAL, LINE, DROP	
OPTICAL_PORT_CONFIG			
adminStatus	String	UP, DOWN	ADMIN STATUS for Optics

			controller of DWDM type on NCS1K
baudRate	String		Baud Rate value on selected controller (optional)
bitsPerSymbol	String		Bits Per Symbol value on selected controller (optional)
gmplsEnabled	String	true, false	Gmpls value on selected controller
rxLowThreshold	String		rxLowThreshold value on selected controller (optional)
rxHighThreshold	String		rxHighThreshold value on selected controller (optional)
txLowThreshold	String		txLowThreshold value on selected controller (optional)
txHighThreshold	String		txHighThreshold value on selected controller (optional)
OPTICS_PORT_CONFIG			
adminStatus	String	UP, DOWN	ADMIN STATUS for Optics controllers for ZR/ZR+ Pluggable card on SVO devices
fecMode	String	OFEC CFEC NONE	FEC Mode value on selected controller
breakout	String	1x100 2x100 3x100 4x100 NONE	Breakout mode value on selected controller
dacRate	String	1x1 1x1.25 1x1.50 1x1.75 1x2 NONE	DAC Rate value on selected controller
modulationType	String	QPSK 8QAM 16QAM NONE	Modulation type value applicable for selected optics controller.
OPTICS_DSP_PORT_CONFIG			
fec	String	Possible Values: • NONE • ENHANCED_SD_27 • ENHANCED_SD_15 • OFEC • CFEC	FEC Mode value on selected controller. The value-set varies based on card-types.

performanceMonitor	String	• ENABLED • DISABLED	Performance Monitor value on selected controller
preFecBerMax	String		Pre FEC Ber Max value on selected controller
preFecBerMin	String		Pre FEC Ber Min value on selected controller
postFecBerMax	String		Post FEC Ber Max value on selected controller
postFecBerMin	String		Post FEC Ber Min value on selected controller
flexoGroupId	String		Flexo Group Id
flexoInstanceId	String		Flexo Instance Id
FIBER_ATTRIBUTES_CONFIG			
fiberLengthUnit	String	KM, MILE	fiberLengthUnit value on selected controller
fiberType	String	G652-SMF, ELEAF, True-Wave-RS, Dispersion-Shifted, Metro-Core, True-Wave-Plus, True-Wave-Minus, True-Wave-Classic, Free-Light, LS, Tera-Light, True-Wave-Reach, G652-SMF-28E	fiberType value on selected controller
fiberLength	Float	Value Ranging from 0 to 998.	fiberLength value on selected controller

FIBRE_CHANNEL_PORT_CONFIG			
squelchMode	String	DISABLE, SQUELCH	you can configure different squelch modes on the interfaces of fibre channel
squelchHoldOffTimer	Integer	0 to 3000 (Time in ms)	you can configure different squelch hold off timer on the interfaces of fibre channel

Note: 1)The Set Termination Point is supported for Cisco NCS4xx, Cisco NCS2K, Cisco ASR903, Cisco ASR904, Cisco ASR907, and Cisco ASR920 family of devices.

2) Please find the attributes info below in SetTP Response :

tp.optical-transport-settings-attributes	This container will be there for NCS1K4,NCS2k,NCS4k as well.
tp.otn-odu-tcm-attributes	It is supported for NCS4k alone and no other device type would have this container.
tp.otn-attributes	This container will be there for NCS1K4,NCS2k,NCS4k as well.

3) Attributes : flexoGroupId, flexoInstanceId are not supported for LC mode: 4x100GE-MXP-DD ,Port Config : OPTICS_DSP_PORT_CONFIG

Set TerminationPoint-SONET LOP

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_SONET_LOP/request.xml
- samples/Set_Termination_Point_SONET_LOP/request.json

Response

- samples/Set_Termination_Point_SONET_LOP/response.xml

Set TerminationPoint-SONET PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_SONET_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_SONET_PORT_CONFIG/request.json

Response

- samples/Set_Termination_Point_SONET_PORT_CONFIG/response.xml

Set TerminationPoint-T1 PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_T1_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_T1_PORT_CONFIG/request.json

Response

- samples/Set_Termination_Point_T1_PORT_CONFIG/response.xml

Set TerminationPoint-ETHERNET PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_ETHERNET_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_ETHERNET_PORT_CONFIG/request.json

Response

- samples/Set_Termination_Point_ETHERNET_PORT_CONFIG/response.xml

Set TerminationPoint-NCS2K ETHERNET PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_NCS2K_ETHERNET_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_NCS2K_ETHERNET_PORT_CONFIG/request.json

Response

- samples/Set_Termination_Point_NCS2K_ETHERNET_PORT_CONFIG/response.xml

Set TerminationPoint-ODU PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_ODU_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_ODU_PORT_CONFIG/request.json
- samples/Set_Termination_Point_ODU_PORT_CONFIG/1.request.xml
- samples/Set_Termination_Point_ODU_PORT_CONFIG/1.request.json

Response

- samples/Set_Termination_Point_ODU_PORT_CONFIG/response.xml
- samples/Set_Termination_Point_ODU_PORT_CONFIG/1.response.xml
- samples/Set_Termination_Point_ODU_PORT_CONFIG/1.response.json

Set TerminationPoint-OPTICAL PAYLOAD PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_OPTICAL_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_OPTICAL_PORT_CONFIG/request.json

Response

- samples/Set_Termination_Point_OPTICAL_PORT_CONFIG/response.xml

Set TerminationPoint- FIBER ATTRIBUTES CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_for_Fiber_Attributes/request.xml

Response

- samples/Set_Termination_Point_for_Fiber_Attributes/response.xml

Set TerminationPoint-OTN PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_OTN_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_OTN_PORT_CONFIG/request.json
- samples/Set_Termination_Point_OTN_PORT_CONFIG/1.request.xml
- samples/Set_Termination_Point_OTN_PORT_CONFIG/1.request.json

Response

- samples/Set_Termination_Point_OTN_PORT_CONFIG/response.xml
- samples/Set_Termination_Point_OTN_PORT_CONFIG/1.response.xml
- samples/Set_Termination_Point_OTN_PORT_CONFIG/1.response.json

Set TerminationPoint-ADMIN STATUS PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_ADMIN_STATUS_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_ADMIN_STATUS_PORT_CONFIG/request.json

Response

- samples/Set_Termination_Point_ADMIN_STATUS_PORT_CONFIG/response.xml

Set TerminationPoint-WAVELENGTH PORT CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_WAVELENGTH_PORT_CONFIG/request.xml
- samples/Set_Termination_Point_WAVELENGTH_PORT_CONFIG/request.json

Response

- samples/Set_Termination_Point_WAVELENGTH_PORT_CONFIG/response.xml

Set TerminationPoint-Enabling MPLS LockOut for BDI

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_Enabling_MPLS_LockOut_for_BDI/request.xml
- samples/Set_Termination_Point_Enabling_MPLS_LockOut_for_BDI/request.json

Response

- samples/Set_Termination_Point_Enabling_MPLS_LockOut_for_BDI/response.xml

Set TerminationPoint-Enabling MPLS LockOut for BDI

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_Disabling_MPLS_LockOut_for_BDI/request.xml
- samples/Set_Termination_Point_Disabling_MPLS_LockOut_for_BDI/request.json

Response

- samples/Set_Termination_Point_Disabling_MPLS_LockOut_for_BDI/response.xml

Set TerminationPoint of VCOP

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_of_VCOP/request.xml

Response

- samples/Set_Termination_Point_of_VCOP/response.xml

Set TerminationPoint for Fiber Attributes

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_for_Fiber_Attributes/request.xml

Response

- samples/Set_Termination_Point_for_Fiber_Attributes/response.xml

Set TerminationPoint GMPLS

In order to perform set operation using setTP API , below examples can be referred.
 In NBI payload operator should use below

- portConfig= OPTICAL_PORT_CONFIG
- tpRef should be optics port of DWDM type from NCS1K device with layerRate as "lr-optical-channel"

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/set_Termination_Point_Gmpls_NCS1K/setTP-gmpls-request.xml

Response

- samples/set_Termination_Point_Gmpls_NCS1K/setTP-gmpls-response.xml

Set TerminationPoint – OPTICS_PORT_CONFIG ZR/ZR+ Pluggable SVO

In order to perform set operation on Optics port using setTP API , below examples can
 be referred. In NBI payload operator should use below

- portConfig= OPTICS_PORT_CONFIG
- tpRef should be optics port from SVO device (ZR/ZR+ pluggable) with layerRate as "lr-optical-channel"

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_OPTICS_PORT_CONFIG/request.xml

Response

- samples/Set_Termination_Point_OPTICS_PORT_CONFIG/response.xml

Set TerminationPoint – Breakout port lane NCS4k

In NBI payload operator should use below

- portConfig= BREAKOUT_LANE_PORT_CONFIG

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_BREAKOUT_LANE_PORT_CONFIG/request.xml

Response

- samples/Set_Termination_Point_BREAKOUT_LANE_PORT_CONFIG/response.xml

Set TerminationPoint – Breakout port lane delete NCS4k

In NBI payload operator should use below

- portConfig= BREAKOUT_LANE_PORT_CONFIG
- layerRate= LR_OpticalPhysicalSection_Multilane
- tpRef should have layerRate as "lr-optical-physical-section-multilane"

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
- samples/Set_Termination_Point_BREAKOUT_LANE_PORT_CONFIG_Delete/request.xml

Response

- samples/Set_Termination_Point_BREAKOUT_LANE_PORT_CONFIG_Delete/response.xml

Set TerminationPoint –Fibre channel port config

In NBI payload operator should use below

- portConfig= FIBRE_CHANNEL_PORT_CONFIG
- layer Rate : -> lr-fc-1600-14025 for FC16; lr-fc-3200-27200 for FC32

Request

- POST /restconf/operations/v1 cisco-resource-activation:set-termination-point
  /samples/Set_Termination_FIBRE_CHANNEL_PORT_CONFIG/request.xml

Response

- /samples/Set_Termination_FIBRE_CHANNEL_PORT_CONFIG/response.xml

1.26 Set AINS

Resource	Description
cisco-resource-ains	This resource is used to set AINS for port.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-ains:auto-in-service
Authorization	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices

Name	Type	Description
tp-ref	String	Fully Distinguished Name (FDN) of the port for which set AINS need to be performed.
generic-admin-state	ENUM	This attribute represents generic admin state of the port. Allowed values: • generic-admin-state-service • generic-admin-state-auto-service • generic-admin-state-maintenance • generic-admin-state-disable
soak-time	Int-32	Indicates soak time value to be set for a port. Allowed values: multiple of 15 e.g., 15, 30, 45, …
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TP.<number> are generated by this API. For example: TP.0050 for 'Invalid value for generic-admin-state, valid values are %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0039=TerminationPoint with FDN - %s and Layer Rate - %s does not exist or is not associated with a Node in the current user'€™s virtual domain. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials • RA.<number> - any tag starting with "RA." prefix for any internal errors like RA.0001=Operation is not supported. For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-nrf-physical-port.yang	

Request

- POST /restconf/operations/v1/cisco-resource-ains:auto-in-service
- samples/AINS/setAINS/request.xml
- samples/AINS/setAINS/request.json

Response

- samples/AINS/setAINS/response.xml
- samples/AINS/setAINS/response.json

1.27 Topological Link Retrieval

This interface provides the operations required to retrieve topological link details.

Resource	Description	
Topological Link	Retrieves the Topological Links in the system.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-network:topological-link	
Query Parameters		
Name	**Type**	**Description**
fdn	String	Fully Distinguished Name (FDN) of the topological to retrieve a single topological link.
topo-layer		Use this filter to display filtered links based on the link type provided. Supported link types are : otu-link-layer, och-link-layer, ots-link-layer, oms-link-layer, ops-link-layer, odu-link-layer, tdm-layer, manual-link-layer, physical-link-layer, mpls-te-tunnel-layer, mpls-tp-tunnel-layer, mpls-te-tunnel-p2p-layer, mpls-te-tunnel-p2mp-layer, mpls-lsp-layer, mpls-link-layer, gre-tunnel-layer, ethernet-link-layer, lacp-link-layer, iccp-link-layer, lag-link-layer, pw-layer, atm-layer, frame-relay-layer, bgp-layer, isis-layer, ospf-layer.
tpFdn	String	Use this filter to display links associated with given Termination Point.
.skipPerformanceMetrics	boolean	Use this filter to skip performance-metrics from the response. This filter skips a call to the device to get performance metrics data thus improving the API response time.
.skipFiberAttributes	boolean	Use this filter to skip fiber-attributes from the response. This improves the API response time.
Authorization Required	One or more from following • Chassis View Read • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more topological links of type **topological-link** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example:	

	TL.0053 – 'Invalid Query Param skipPerformanceMetrics: <value>' If error is from underlying framework/core modules error-app-tag format one of following: • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0068=Invalid Link Type was passed as filter: <value>. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	Cisco-topology.yang

Topological Link Data

Name	Type	Description
Topology	Container element	Holds the data for topological link.

1.27.1.1 *Topological Link Data details*

The Topological-link container contains the following attributes mentioned in the table below:

Parameter Name	Type	Description
fdn	String	Fully distinguished name of the topological Link. FDN = 'MD=<CISCO_EPNM>!TL=<tlname> Eg MD=CISCO_EPNM!TL=13.13.13.4-13.13.13.5 or Eg fdn=MD=CISCO_EPNM!TL=10.58.234.141:[WDMSIDE-A]--10.58.234.144:[WDMSIDE-A]
discovered-name	String	Name of the link alone without the complete FDN. Eg: 13.13.13.4-13.13.13.5
oper-stat	String	
direction	String	Indicates the direction of the link.
type	String	Indicates the type of the topological link. [deprecated]
topo-layer	String	Indicates the layer of the topological link with possible values pw-layer mpls-te-tunnel-layer mpls-te-tunnel-p2p-layer mpls-te-tunnel-p2mp-layer mpls-lsp-layer mpls-link-layer mpls-tp-tunnel-layer cem-layer ethernet-link-layer lacp-link-layer iccp-link-layer odu-link-layer otu-link-layer och-link-layer ots-link-layer oms-link-layer ops-link-layer tdm-layer physical-link-layer

		atm-layer frame-relay-layer bgp-layer isis-layer ospf-layer gre-tunnel-layer hdlc ip-sec-layer inter-chassis-control-layer bfd-layer manual-link-layer sr-te-layer unknown-layer Note: Refer to cisco-topology.yang model for complete and updated list.
link-type	String	This field will indicate if the topological links is either of the following: **-internal-patch-cord** **-cross-connect** **-open-ended.**
total-capacity		Total link capacity assigned.
used-capacity		Capacity utilized out of total link capacity.
member-of-ref	String	Applies to uni-directional links only. FDN of the container Bi-directional link, this Uni-directional link is part of. Not present if link is not part of any bi-directional link.
endpoint-list		Complex contained to hold the list of Endpoints.
end-point		Complex container to hold the endpoint information.
Endpoint-ref	String	FDN of the endpoint. Eg: MD=CISCO_EPNM!ND=SJ-NCS4206-21.cisco!CTP=name=BDI8-mpls layer;lr=lr-mpls
LOGO Attributes		Set of attributes to indicate the optical attributes that derive the feasibility of a path.
noise		Indicates the noise level of the link.
noise-sigma		Indicates noise level variance of the link.
pdl		Indicates polarization dependent loss of the link.
pmd		Indicates polarization mode dispersion of the link.
fgdr-filter		Indicates fgdr-Filter Group Delay Ripple of the link.
sf-filter		Indicates self-filtering.
chromatic-dispersion		Indicates chromatic dispersion of the link.
chromatic-dispersion-slope		Indicates the chromatic dispersion slope of the link.

Get All Topology

Request

- GET /restconf/data/v1/cisco-resource-network:topological-link HTTP/1.1

Response

- samples/Get_All_Topology/response.xml

Get a Topology

Request

- GET /restconf/data/v1/cisco-resource-network:topological-link?
  fdn=MD=CISCO_EPNM!TL=10.10.1.80:[WDMSIDE-A]--10.10.1.81:[WDMSIDE-A]

Response

- samples/Get_a_Topology/response.xml

Get Topology Filter on Layer

Request

- `https://<epnm-host>/restconf/data/v1/cisco-resource-network:topological-link?topo-layer=manual-link-layer`
  - Host: <epnm-host>
  - Accept: application/yang-data+xml

Response

- samples/Get_Topology_Filter_on_Layer/response.xml

Get Topology Filter on Termination Point

Request

- `https://<epnm-host>/restconf/data/v1/cisco-resource-network:topological-link? tpFdn=MD=CISCO_EPNM!ND=vm-svo-sim06b!CTP=name=4/PORT-6-RX%264/PORT-6-TX;lr=lr-optical-section`

Response

- samples/Get_Topology_Filter_on_TP/response.xml

1.28 Managed Link

Managed Link creation, modification and deletion are done via., POST and DELETE operations. LMP Links can be created between:

- NCS1K → NCS4K
- NCS2K → NCS2K with 400G-XP in OTN mode.
- NCS1010(OTS) —> NCS1010(OTS)
- NCS1010(OTS) —> External Device : ZR Pluggable or spitfire (Optics port) on external device and then och port on our simulated device.

➢ Managed Link creation requires the source and destination endpoints (Termination point FDN) fields to be specified.
➢ Managed Link deletion requires the Link FDN to be passed as a query parameter to the DELETE URL.
➢ Managed Link retrieval is like regular topological link retrieval. The Topological Link retrieval URL is provided with the Link FDN as query parameter.

Managed Link Create

Resource	Description
Managed Link Attributes	Creates a managed Link between the specified endpoints

HTTP Method	Resource Path	
POST	/restconf/operations/v1/cisco-resource-network:topological-link	
Input Parameters		
Name	**Type**	**Description**
tl-link-create-request		Managed Link Creation request container
src-endpoint-ref	String	FDN of the source endpoint of the Managed Link. Eg: **MD=CISCO_EPNM!ND=tcc30!CTP=name=LINE-1-2-1-TX;lr=lr-optical-section**
dst-endpoint-ref	String	FDN of the destination endpoint of the Managed Link. Eg: **MD=CISCO_EPNM!ND=tcc35!CTP=name=LINE-1-2-1-RX;lr=lr-optical-section**
Authorization Required	One or more from following • Network Topology • Network Topology Edit	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Result: Indicating the creation as SUCCESS / FAILED Message:	
	Type	**Description**
Result	String	SUCCESS / FAILED
message	String	**For success case**: Managed Topo Link is created successfully with name :tcc30:[LINE-1-2-1-TX]-tcc35:[LINE-1-2-1-RX] **For error condition** (Internal Error on Server): Preconditions not met **For API call error**: Managed Link creation failed
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL. TL.0072 - Invalid 'src-endpoint-ref' TP FDN '<value>'. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-topology.yang	

Request

- POST /restconf/operations/v1/cisco-resource-network:topological-link
  samples/Managed_Link_Create/request.xml

Response

- samples/Managed_Link_Create/response.xml

Managed Link Modify

Resource	Description	
Managed Link Attributes	Modify Managed Link name between the specified endpoints	
HTTP Method	**Resource Path**	
POST	/restconf/data/v1/cisco-resource-network:modify-topological-link	
Input Parameters		
Name	**Type**	**Description**
topo-link-modify-request		Managed Link Modify request container
tl-ref	Fdn	Topo Link Fdn of the Managed Link.
link-name	String	Link name of the managed Link.
Authorization Required	One or more from following • Network Topology • Network Topology Edit	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Result: Indicating the creation as SUCCESS / FAILED Message: Command pushed to CLI or Failure message when Result is Failed.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.\<number\> are generated by this API. For example: TL.0061- 'Invalid TL FDN \<TL Value\>' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-topology.yang	

Request

- POST /restconf/data/v1/cisco-resource-network:modify-topological-link
  samples/Managed_Link_Modify/request.xml

Response

- samples/Managed_Link_Modify/response.xml

Managed Link Delete

Resource	Description	
Managed Link Attributes	Deletes Managed Link specified as an URL parameter	
HTTP Method	**Resource Path**	
DELETE	/restconf/operations/v1/cisco-resource-network:topological-link?fdn=<TL FDN>	
Query Parameters		
Name	**Type**	**Description**
Fdn	String	FDN of the Managed link to be deleted. Link FDN
Authorization Required	One or more from following • Network Topology • Network Topology Edit	
Response Messae		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Result : Indicating the creation as CREATED / FAILED Message:	
	Type	**Description**
Result	String	DELETED / FAILED
Message	String	**For success case**: Managed Link is deleted Successfully **For error condition** (Internal Error on Server) : Preconditions not met **For API call error**: Managed Link deletion failed
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL.0061- 'Invalid TL FDN <value>' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-topology.yang	

- DELETE /restconf/operations/v1/cisco-resource-network:topological-link?fdn=MD=CISCO_EPNM!TL=tcc30%3A%5BLINE-1-2-1-TX%5D-tcc35%3A%5BLINE-1-2-1-RX%5D

Response

- samples/Managed_Link_Delete/response.xml

1.29 MPLS TE Explicit Path Retrieval

This interface provides the operations required to retrieve topological link details.

Resource	Description
MPLS TE Explicit Path	Retrieves the MPLS TE Explicit Paths in the system.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-resource-ems:mpls-te-explicit-path
Query Parameters	

Name	Type	Description
path-ref	String	Fully Distinguished Name (FDN) of the explicit path to retrieve a single MPLS TE Explicit Path Path-ref=MD=CISCO_EPNM!ND=cvg-scapa-223.cisco.com!PATH=223-225_OTU4 Path-ref= 'MD=<CISCO_EPNM>!ND=<nodename>!<PATH>=<pathname>
ignore-duplicate	String	ignore-duplicate=true (To remove duplicate entries)
Authorization Required	One or more from following - Chassis View Read - Chassis View Read and Write - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting - Network Topology - Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more MPLS TE Explicit Paths of type mpls-te-explicit-path. See the yang model for the data details.	
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format PATH.<number> are generated by this API. For example: PATH.0001 for 'FDN was passed without TE Path Name.' If error is from underlying framework/core modules error-app-tag format one of following: - TP.<number> - any tag starting with "TP." prefix for any internal errors like TP.0002 for 'Given LayerRate Value is Invalid'. - FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. - CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials	

	For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-mpls-te-extension.yang

MPLS TE Explicit Path Data

Name	Type	Description
mpls-te-explicit-path-type	Container element	Holds the data for mpls te explicit path.

Get All MPLS TE Explicit Paths

Request

- GET /restconf/data/v1/cisco-resource-ems:mpls-te-explicit-path

Response

- samples/Get_All_MPLS_TE_Explicit_Paths/response.xml

Get A MPLS TE Explicit Paths

Request

- GET /restconf/data/v1/cisco-resource-ems:mpls-te-explicit-path?path-ref=MD=CISCO_EPNM!ND=cvg-scapa-223.cisco.com!PATH=223-225_OTU4

Response

- samples/Get_a_MPLS_TE_Explicit_Paths/response.xml

1.30 Virtual Connection Retrieval

This interface provides the operations required to retrieve virtual connection details. For Yang schema definitions, see cisco-virtualconnection.yang

Resource	Description	
Virtual Connection	Retrieves all Virtual Connections in the system or retrieve a specific set based on the input parameters.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-service-network:virtual-connection	
Query Parameters		
Name	**Type**	**Description**
type	String	Type of the virtual connection to retrieve. If not specified all types will be returned. Possible values: carrier-ethernet-vpn, tdm-cem, mpls-te-tunnel, , mpls-l3-vpn and optical.
fdn	String	Fully Distinguished Name (FDN) of the virtual connection to retrieve a single virtual connection. FDN = 'MD=<CISCO_EPNM>!VC=<vcname>
ndFdn	String	Fully Distinguished Name (FDN) of the Node. FDN = 'MD=<CISCO_EPNM>!ND=<nodename>
tpFdn	String	Fully Distinguished Name (FDN) of the termination-point. When this parameter is provided, all virtual connections that reference this termination-points will be returned.
isProvisioned	String	To get provisioned data pass "true" as a value and will retrieve raw provision data.
Authorization Required	One or more from following	

	• Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more Virtual Connections of type virtual-connection. See the yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format VC.<number> are generated by this API. For example: VC.0001 for 'Currently subType filter is not supported.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-virtualconnection.yang

Virtual Connection Data

Name	Type	Description
virtual-connection	container	Container holds the virtual connection data.

Parameter Name	Type	Allowed Values	Description
Fdn	String		Fully distinguished name of the Virtual Connection. Eg: MD=CISCO_EPNM!VC=TRAIL-Do_NOT_DELETE_DEMO
discovered-name	String		Name of the link alone without the complete FDN. Eg: TRAIL-Do_NOT_DELETE_DEMO
admin-state	String	Up/Down	Indicates the admin state of the connection.
oper-state	String	Up Down Unavailable Partial Auto Up Up Not Protected	Indicates operational state of connection.
vc-id	String		Its id of the virtual connection.
discovery-state	String		Indicates the discovered state of the Connection/Service.

			Eg: discovery-resync, discovery-complete, discovery-missing, discovery-partial, discovery-unknown, discovery-not-applicable
Type	String		It represents multi-layer technology , i.e. mpls-te tunnel, Carrier-E, etc.
sub-type	String		Some Virtual Connections have different subtypes, i.e. Carrier-E EPL, Carrier-E EVPL, etc.
topology	String		Define the topology; Default is point-to-point.
direction	String	bi-directional uni-directional	Direction of a circuit.
protection-type	String	protection-type-one-plus-one protection-type-none protection-type-one-plus-one-plus-r protection-type-one-plus-r protection-type-splitter protection-type-upsr protection-type-ycable protection-type-unknown	Protection type can be of type Y-cable, splitter, one-plus-one -this applies to TE Tunnel and CEM too.
protection-role	String		working, protecting, restore
Termination point list	Container		Virtual Connection termination point list.
termination-point	Container		Container to show TP info in get VC
Fdn	String		Fully distinguished name of the Virtual Connection. Eg: MD=CISCO_EPNM!VC=TRAIL-Do_NOT_DELETE_DEMO
discovered-name	String		Name of the link alone without the complete FDN. Eg: TRAIL-Do_NOT_DELETE_DEMO
admin-state	String	Up/Down	Indicates the admin state of the connection.
oper-state	String	Up/Down	Indicates operational state of connection.
directionality	String	tp-source tp-sink tp-bidirectional unknown	Base identity for VC for direction. tp-bidirectional (for non-optical only) unknown (for optical services only)
is-edge-point	String		Indicates if the TP is an edge point of at least one virtual network, i.e. if it is an end point of a potential inter-network topological link.
ce-tp			
outer-vlan-tp-id	String		Outer virtual LAN termination point ID
untagged-default	String	true false	Default value for untagged services

sv-id-list	String			SV ids list
cv-id-list	String			VC ids list
vid-rewrite-oper	String	pop1, pop2, push1, push2 translate1-1, translate1-2, translate2-1 translate2-2 rewrite1-1 rewrite1-2 rewrite2-1 rewrite2-2		VLAN id rewrite operations
rewrite-is-symmetric	String	true false		rewrite-is-symmetric value of the circuit
mtu	String			MTU value for the service
Route name list	container			Virtual Connection route names including protecting/standby routes.
route-name	String			Indicates the route name used.
Te-tunnel				MPLS TE Tunnel specific attributes.
tunnel-id	String			Indicates the TE tunnel ID
tunnel-source	String			TE tunnel source IP
tunnel-destination	String			TE tunnel destination IP
association-id	String			TE tunnel association ID. Used for bi-directional TE tunnel association.
association-source-address	String			Source IP of the associated TE tunnel. Applicable to bi-direction TE tunnel.
global-id	String			global id (per Autonomous System) to enable MPLS TE tunnel source id unique globally.
co-routed-enabled	Boolean			A flag indicates whether the bi-directional tunnels share the same MPLS LSP route.
protection-type	String			This is obsolete. VC protection type is represented.
carried-by-vc-ref-list				Carried by Virtual Connection reference list
carried-by-vc-ref	String			The underlying Virtual Connection references. ex. SR-TE, TE-Tunnel of an ELINE VC, optical VC
carrying-vc-ref-list				Carrying Virtual Connection reference list
carrying-vc-ref	String			The top layer Virtual Connection references. ex. ELINE VC, top layer optical VC
sr-te-policy				SR TE Policy container
color	String			color represents a SLA treatment; i.e. low latency, high latency. color, head end and endpoint are the unique identifier of the SR

			policy color. Color can be used to indicate a certain treatment (SLA, policy) provided by an SR Policy. Only one SR Policy with a given color C can exist between a given node pair (head-end (H), end-point (E))
headend	Ip-address		TE router id/ip of head device
endpoint	Ip-address		TE router id/ip of destination device
binding-sid	Integer		In practice all paths associated with the Sr policy should have the same BSID
candidate-path-list			for each SR policy there up to 1 - n candidate-paths
candidate-path			candidate-paths
path-name	String		candidate path name
preference	Integer		Higher preference # indicate lower preference
type	String		dynamic, explicit or Dynamic with PCE(for inter domain path computation)
metric-type	String		segment routing metric type
sids-list			for each candidate path, there's a segment ids list 1 and 0-m (SIDs list)
sids			Segment IDs
name	String		segment IDs name
type	String		dynamic, explicit or Dynamic with PCE(for inter domain path computation)
state	String		Discovered state : active, inactive.
metric-type	String		segment routing metric type
weight	String		There's a weight for each SIDs list). weight is for load balancing between (SIDs List)
sid-list			segment id in the entry list
sid			segment id
index	Integer		index of the segment id in the entry list
sid	Integer		SID id
description	String		description of each SID id entry in the list
och-nc/och-cc/och-trail	Container		These containers to hold DWDM OCH circuit specific attributes.
media-channel-nc/media-channel-cc/media-channel-trail	Container		These containers hold DWDM MCH circuits specific attributes.
restoration-type	String	none restore revert	Restoration type of optical service
restoration-status	String	none	Restoration status of optical

		failed restored restoring revertible reverting	service
activation-state	String		activation state
regeneration-allowed	Boolean	true false	Is Circuit should allow regeneration
upstream-power-offset	String		offset of upstream channel
downstream-power-offset	String		offset of downstream channel
path-policy	String		path selection policy: ANY, LOGO
ignore-path-alarms	String	true/false	Optional parameter, when set the link port alarm status along the light path is ignored when creating a circuit.
circuit-diversity	String		Diversity of circuit diversity
revert-mode	String	manual automatic none notApplicable	Revert type of a circuit
soak-time	String		Period that the circuit on the restored path waits before switching to the original path after a failure is fixed
frequency	String		Bandwidth in frequency. -Deprecated
wavelength	float		wavelength in nm unit
width	String		Bandwidth of the service
priority	String	High low priority1 priority 2 priority 3 priority 4 priority 5 priority	Prioritize the restoration operation for the failed OCH circuit.
optical-path-settings	String		Optical path settings of a service
is-uni	Boolean	true false	flag indicating whether UNI should be configured
is-wson	Boolean	true false	Flag indicating whether it is a Wavelength Switched Optical Network circuit
is-mandatory-freq	Boolean	true false	Is frequency mandatory for this service -Deprecated
frequency-preference	String		Bandwidth in frequency-preference for protected services -Deprecated
frequency-protected	String		Bandwidth in frequency for protected services -Deprecated
frequency-protected-preference	String		Bandwidth in frequency for protected preference services -Deprecated
is-mandatory-frequency-	Boolean	true false	Is frequency mandatory for this service

protected			-Deprecated
grid-type	String	Fixed 50 GHz Fixed 50 Fixed 6 25 Flex 100	Grid-type attribute for the service
alien-card-id	String		Alien card id for the service
alien-trunk-mode	String		Alien trunk mode for the service
alien-fec-mode	String		Alien fec mode for the service
failure-reason			String
Och-Trail-Uni			DWDM OCH Trail UNI circuit specific attributes.
restoration-type	String		restoration type, none, restore, revert
restoration-status	String		restoration type, none, failed, restored, restoring, revertible, reverting
Tunnel-id	String		reference to the odu tunnel id
source-address	String		source ip address
signaled-name	String		Reference to the lsp signal
set-uni-cfg	String		OCH Trail UNI configuration indicator
och-nc-name	String		Reference to OCH NC that is automatically created as a result of this OCH Trail UNI creation
diverse-from-tunnel-id	String		Diverse from tunnel id
diverse-attribute-set-name	String		Diverse attribute et name
preferred-wave-length	String		This attribute is used to specify preferred wavelength.
manage-constraints	Boolean		Boolean flag to specify if constraints need to be considered or not. Default value: false **Note**: while provisioning optical service using existing service profile containing constraints information, <manage-constraints> tag needs to be set to true.
Is-unnumbered	Boolean		
failure-reason	String		Indicates the failure reason for DWDM OCH Trail UNI if any error exists during circuit provisioning
Odu-Uni			DWDM ODU UNI circuit specific attributs.
framing	String		ODU framing
bit-rate	String		Circuit-bitrate
tunnel-id	String		Associated tunnel-id

source-address	String		Reference to the protecting OCH Trail
diverse-from-tunnel-id	String		Diverse from tunnel
Odu-Tunnel			DWDM ODU Tunnel circuit specific attributes.
framing	String		ODU framing
bit-rate	String		Circuit-bitrate
tunnel-id			String
source-address	String		Reference to the protecting OCH Trail
diverse-from-tunnel-id	String		Diverse from tunnel
signaled-name	String		OTN tunnel signed name
record-route	String	true false	record-route specification
bandwidth	String	odu1,odu0, odu1e, odu1f, odu2,odu2e, odu2f, odu3, odu3e1, odu3e2, odu4, oduflex	ODU tunnel service bandwidth value
protection-profile	String		Name of the protection profile applied on circuit
diverse-attribute-name			String
failure-reason	String		Indicates the failure reason for DWDM OCH Trail UNI if any error exists during circuit provisioning
te-tunnel-path-option-list	String		Container hold te tunnel path related attributes
path-preference	String		Circuit path preference between source and sink
protection-role	String	working-path protected-path	It gives data about the protection role of circuit path
path-type	String	EXPLICIT DYNAMIC	Shows circuit path type
lock-down	String	true false	Lock down value of a circuit
protected-by	String		Circuit protected by value
explicit-path-name	String		Explicit path name applied on the service
ce-tp			
outer-vlan-tp-id	String		Outer virtual LAN termination point ID
untagged-default	String	true false	Default value for untagged services
sv-id-list	String		SV ids list
cv-id-list	String		VC ids list
vid-rewrite-oper	String		Base Identity for VLAN id rewrite operations
rewrite-is-symmetric	String	true false	Attribute to specify if rewrite is to be symmetric or not.
mtu	String		MTU value for the service
Route name list			Virtual Connection route names including protecting/standby

			routes.
route-name	String		Indicates the route name used.
Te-tunnel			MPLS TE Tunnel specific attributes.
tunnel-id			String
tunnel-source	String		TE tunnel source IP
tunnel-destination	String		TE tunnel destination IP
association-id	String		TE tunnel association ID. Used for bi-directional TE tunnel association.
association-source-address	String		Source IP of the associated TE tunnel. Applicable to bi-direction TE tunnel.
global-id	String		global id (per Autonomous System) to enable MPLS TE tunnel source id unique globally.
co-routed-enabled	Boolean		A flag indicates whether the bi-directional tunnels share the same MPLS LSP route.
protection-type	String		This is obsolete. VC protection type is represented.
carried-by-vc-ref-list			Carried by Virtual Connection reference list
carried-by-vc-ref	String		The underlying Virtual Connection references. ex. SR-TE, TE-Tunnel of an ELINE VC, optical VC
carrying-vc-ref-list			Carrying Virtual Connection reference list
carrying-vc-ref	String		The top layer Virtual Connection references. ex. ELINE VC, top layer optical VC
path-type	String		
lock-down	String		
protected-by	String		
explicit-path-name	String		
evpn	Container		Container to show EVPN related tags in get VC response.
bgp-attributes	Container		Container to show EVPN BGP specific attribute values.
bgp-signaling-protocol	Boolean	true , false	Flag to indicate if EVPN is enabled or not. For EVPN its value should be "true".
is-auto-route-distinguisher	Boolean	true, false	This tag indicates if auto RD was enabled for the service or not.
route-distinguisher	String	Allowed values IP:num or num:num	This tag indicates the value of RD.
is-auto-route-target	Boolean	true, false	This tag indicates if auto RT was enabled for the service or not.
import-route-target	String	Allowed values IP:num or num:num	This tag shows the value of import RT
export-route-target	String	Allowed values IP:num or num:num	This tag shows the value of export RT

vpws-attributes	Container		Container to show VPWS specific attribute values.
evpn-instance-id	Long		This tag shows the value of EVI for the service.
aend-attachment-circuit-id	Long		This tag shows the value of AEND AC id
zend-attachment-circuit-id	Long		This tag shows the value of ZEND AC id
enable-control-word	Boolean		Boolean flag to indicate of control word was enabled for the service or not.
L3VPN			L3vpn circuit related attributes.
address-family-list	Container		Container list to show addressfamily attribute values
address-family	Container		Container for address family details
address-family-type	Enum	IPV4_AF, IPV6_AF	Address family type supported for the service
max-routes	String		Maximum number of routes present
import-route-target	string		Import route target value if present
Export-route-target	String		Export route target value if present
Import-route-policy	String		import route policy map, can be sr-policy
export-route-policy	String		export route policy map, can be sr-policy
bgp-neighbor	Container		Bgp neighbor details container
ip-address	Ip-address	Ipv4/ipv6	BGP neighbor IP address
as-number	Number		assigned AS number
local-as-number	Number		local AS number
local-as-action	String		local AS placement -prepend, replace, etc.
bgp-address-family-list	Container		
bgp-address-family	Container		
address-family	Enum	IPV4_AF, IPV6_AF	Address family type supported for the service
ingress-route-policy	String		ingress route policy. Can be SR policy for XR
egress-route-policy	String		egress route policy. Can be SR policy for XR
local-as-number	Number		local AS number
local-as-action	String		local AS placement -prepend, replace, etc.

Get All Virtual Connection

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection HTTP/1.1

Response

- samples/Get_All_Virtual_Connections/response.xml

Get All Virtual Connection L3VPN

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?vcType=mpls-l3-vpn&.summary=*false*

Response

- samples/Get_All_Virtual_Connections_L3VPN/response.xml

Get a Single Virtual Connection

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?fdn=MD=CISCO_EPNM!VC=foo HTTP/1.1

Response

- samples/Get_a_Single_Virtual_Connection/response.xml

Get a Virtual Connection – L3VPN

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?
  fdn=MD=CISCO_EPNM!VC=L3VPN-Full-mesh-both900_nbi_ospfv3_1

Response

- samples/Get_a_Virtual_Connection_L3VPN/response.xml

Get a Virtual Connection – L3VPN with SR Policy

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?
  fdn=MD=CISCO_EPNM!VC=L3VPN-With-SR-Policy-25-A

Response

- samples/Get_a_Virtual_Connection_L3VPN_With_SR_Policy/response.xml

Get All Virtual Connections - CE service

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?type=carrier-ethernet-vpn&.maxCount=3

Response

- samples/Get_All_Virtual_Connections_CE/response.xml

Get a Virtual Connections - CE service

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?fdn=<VcFdn>

Response

- samples/Get_a_Virtual_Connection_CE/response.xml
- samples/Get_a_Virtual_Connection_CE_WithEVPN/response.xml

Get All Virtual Connections - CEM service

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?type= tdm-cem&.maxCount=3

Response

- samples/Get_All_Virtual_Connections_CEM/response.xml

Get a Virtual Connections - CEM Service

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?
  fdn=MD=CISCO_EPNM!VC=CemLink%23CemPwLink%23CEMPW_6.6.6.22_25_6.6.6.
  41

Response

- samples/Get_a_Virtual_Connection_CEM/response.xml

Get ALL Virtual Connections – OPTICAL services

For Yang schema definition, see cisco-virtualconnection.yang and cisco-optical-circuit-extensions.yang for more details.

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?type=optical

Response

- samples/Get_All_Virtual_Connections_OPTICAL/response.xml

Get All Virtual Connections – With ServiceInfo Resync State

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection?fdn=MD=CISCO_EPNM!VC=test-otu2-mr-mxp

Response

- samples/Get_All_Virtual_Connections_With_ServiceInfo_Resync_State/response.xml

Get all Virtual Connection – OCHCC service with Oper state UpNotProtected

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection? fdn=MD=CISCO_EPNM!VC=Y-CABLE-22-OTU2

Response

- samples/Get_All_Virtual_Connections_With_OperState_UpNotProtected/response. xml

Get all Virtual Connection – SR TE services for specific Node

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection?type=sr-te&ndFdn=<value>

Response

- samples/Get_All_Virtual_Connections_With_SR_TE_For_NodeFdn/response.xml
- samples/Get_All_Virtual_Connections_With_SR_TE_For_NodeFdn/response.json

Get a Virtual Connection – ODU service

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection? fdn=MD=CISCO_EPNM!VC=<oduServiceName>

Response

samples/Get_a_Virtual_Connection_Optical_ODU_Service/response.xml

Get a Virtual Connection – SR TE service

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection? fdn=MD=CISCO_EPNM!VC=<sRTeServiceName>

Response

samples/Get_a_Virtual_Connection_SRTE/response.xml

Get a Virtual Connection – ODU service with Filter IsProvisioned

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection?
  fdn=MD=CISCO_EPNM!VC=<ODU_ServiceName>&isProvisioned=true

Response

[samples/ Get_a_Virtual_Connection_Optical_ODU_Service_Filter_IsProvisioned/response.xml](samples/Get_a_Virtual_Connection_Optical_ODU_Service_Filter_IsProvisioned/response.xml)

Get a Virtual Connection – OCH Trail service with Filter IsProvisioned

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection?
  fdn=MD=CISCO_EPNM!VC=<OCH_Trail_ServiceName>&isProvisioned=true

Response

samples/Get_a_Virtual_Connection_Optical_OCHTrail_Service_Filter_IsProvisioned/response.xml

Get a Virtual Connection – ODU Tunnel service with Filter IsProvisioned

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection?
  fdn=MD=CISCO_EPNM!VC=<ODU_Tunnel_ServiceName>&isProvisioned=true

Response

samples/Get_a_Virtual_Connection_Optical_ODUTunnel_Service_Filter_IsProvisioned/response.xml

Get a Virtual Connection – ODU UNI service with Filter IsProvisioned

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection?
  fdn=MD=CISCO_EPNM!VC=<ODU_UNI_ServiceName>&isProvisioned=true

Response

[samples/ Get_a_Virtual_Connection_Optical_ODU_UNI_Service_Filter_IsProvisioned/response.xml](samples/Get_a_Virtual_Connection_Optical_ODU_UNI_Service_Filter_IsProvisioned/response.xml)

Get a Virtual Connection – MCHNC service with Filter IsProvisioned

Request

- GET /restconf/data/v1/cisco-service-network: virtual-connection?
  fdn=MD=CISCO_EPNM!VC=<MCHNC_ServiceName>&isProvisioned=true

Response

samples/Get_a_Virtual_Connection_Optical_MCHNC_Service_Filter_IsProvisioned
/response.xml

1.31 CEM Bulk Promotion

CEM Bulk Promotion is a RESTCONF operation which is used to promote one or more CEM services at a time.

Operation	Description
Bulk Promote	This operation can be used to bulk promote the CEM Services.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/network-service:bulk-promote-service
Request Message	
Request Content Type	application/xml
Request Data	List of CEM Service Names or Single Service Name.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns with the promotion status.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format VC.<number> are generated by this API. For example: VC.0025 for 'Maximum 100 CEM Services can be bulk promoted'. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-network-service.yang

Bulk Promote Data

Name of Tag	Data Type	Description

Service-names	List	It contains list of service-name or single service.
Service-name	String	Name of CEM service

1.31.1.1 *Request*

POST /restconf/operations/v1/network-service:bulk-promote-service HTTP/1.1

- samples/CEM_Bulk_Promotion/request.xml

1.31.1.2 *Response*

- samples/CEM_Bulk_Promotion/response.xml
- samples/CEM_Bulk_Promotion/response.json

1.31.1.3 *Criteria/Specification to Bulk Promote the Service*

- Service should be CEM
- Given service should be brownfield circuit and Discovery State should be full
- Bulk Promotion is a synchronous operation at a time user can promote up to 100 CEM services.

1.32 Multi-Layer Trace Retrieval

This interface provides the operations required to retrieve multi-Layer trace for a given virtual connection. The interface can be used to retrieve the multi-layered routes for CEM, MPLS-TE-Tunnel, Optical and all the other supported virtual connections. For Yang schema definitions, see cisco-topology.yang

Resource	Description	
Virtual Connection Route	Retrieves all Virtual Connections routes in the system or retrieve specific set based on the input parameters.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route	
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology	
Query Parameters		
Name	**Type**	**Description**
vcFdn	String	Fully Distinguished Name (FDN) of the virtual connection for which the MLT should be retrieved.
topo-layer	String	Topo-layer available part of MLT response, for possible topo-layer values, please refer cisco-topology.yang. Example : ?vcFdn=MD=CISCO_EPNM!VC={vcFdn}&topo-layer=pw-layer
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more connection (topological-link) of type **virtual-connection-multi-layer-route** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors.	

	• 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL.0002 – 'Invalid input. VirtualConnection missing in the Fdn' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	Cisco-topology.yang

Virtual Connection Multi-Layer Trace Data

Name	Type	Description
virtual-connection-multi-layer-route	Container element	Holds the data from multi-layer route. There will be one **virtual-connection-multi-layer-route** entry per layer.
topo-index	Integer	Indicates the index of the layer in the order.
topology-layer		Indicates the name of the layer. Eg: och-link-layer, ops-link-layer, ots-link-layer.
protection-role		Indicates the protection role of the path.
protection-state		Indicates the protection state of the path.
tl-list	Container element	List of links for the given layer (represented by virtual-connection-multi-layer-route).
topological-link	Container element	Contains n number of topological-link entities as there are connections for the given layer. Both internal and external links are represented as topological-link.
tl-index		Index of the topological link inside the given layer.
fdn		FDN of the given topological link. FDN = 'MD=<CISCO_EPNM>!TL=<tlname> Eg MD=CISCO_EPNM!TL=13.13.13.4-13.13.13.5
is-cc		Indicates if the link is a cross connect or not.
direction		Indicates if the link is uni-directional or bi-directional link.
endpoint-list	Container element	List of endpoints for the particular topological-link.
endpoint	Container element	Contains information about the endpoint of the topological-link.
endpoint-ref	String	FDN of the termination point. Eg: MD=CISCO_EPNM!ND=cvg-scapa-90.cisco.com!CTP=name=Optics0/1/0/3;lr=lr-optical-channel
directionality	String	Contains the direction of the TP. Eg: uni-

		direction, bi-direction.

Get MLT for OCHTRAIL UNI service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=TRAIL-smadama-OCHCC-00A

Response

- samples/Get_a_Virtual_Connection_Multi_Layer_Route_OCHTRAIL_UNI/response.xml

Get MLT for MCH Group service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC= MCHG-MCHNC_42_44

Response

- samples/Get_a_Virtual_Connection_Multi_Layer_Trace_MCHGroup/response.xml

Get MLT for OCHTrail UNI service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=OCHTrailUNI

Response

- samples/Multi_Layer_Trace_Retrieval_for_OCHTrail_UNI/response.xml

Get MLT for OPU over ODU service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=RestconfOPUOverODU

Response

- samples/Multi_Layer_Trace_Retrieval_for_OPU_over_ODU/response.xml

Get MLT for ODUUNI Hairpin service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=ODUUNI_HP

Response

- samples/Multi_Layer_Trace_Retrieval_for_ODUUNI_Hairpin/response.xml

Get MLT for OCHCC service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=ODUUNI_HP

Response

- samples\Multi_Layer_Trace_Retrieval_for_OCHCC\request.xml

Get MLT for OCHNC service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=OCHNC_21July2019_E3_Fi90A_preupgrade_DND

Response

- samples\Multi_Layer_Trace_Retrieval_for_OCHNC\request.xml

Get MLT for OCHTrail MP

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=OCHTrail_SVO_test

Response

- samples\Multi_Layer_Trace_Retrieval_for_OCHTrail_MP\request.xml

Get MLT for OCHCC MP

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=OCHCC_SVO_test

Response

samples\Multi_Layer_Trace_Retrieval_for_OCHCC_MP\request.xml

Get MLT for OCHNC MP

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=ochncsvo_circuit

Response

samples\Multi_Layer_Trace_Retrieval_for_OCHNC_MP\response.xml

Get MLT for ODU service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=Rac_ODU_2

Response

- samples\Multi_Layer_Trace_Retrieval_for_ODU\response.xml

Get MLT for CEM with MPLSTE service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=<cemServiceName>

Response

- samples/Multi_Layer_Trace_Retrieval_for_CEM_With_MPLSTE/response.xml

Get MLT for CE with MPLSTE service

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=<ceServiceName>

Response

- samples/Multi_Layer_Trace_Retrieval_for_CE_With_MPLSTE/response.xml

Get MLT by topo-layer

Request

- GET /restconf/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=MD=CISCO_EPNM!VC=<ServiceName>&topo-layer=<topo-layer>
- Possible values for topo-layer will be available in topology-layer attribute in the MLT response

Response

- samples/Multi_Layer_Trace_Retrieval_by_topo_layer/response.xml

1.33 Customer Facing Service Retrieval

This interface provides the operations required to retrieve Customer Facing Service (CFS) details which include the services provisioned for CE, CEM, MPLS-TE, L3VPN, Optical and all other supported virtual connections.

Resource	Description
Customer Facing Service	Retrieves all Customer Facing Services in the system or retrieve a specific set based on the input parameters.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-service-network:customer-facing-service
Query Parameters	

Name	Type	Description
type	String	Type of the CFS to retrieve. If not specified all types will be returned. Possible values: carrier-ethernet-vpn, tdm-cem, mpls-te-tunnel, and mpls-l3-vpn.
subType	String	Sub Type of the CFS to retrieve. If not specified all sub types will be returned. Should be used in conjunction with Type.
fdn	String	Fully Distinguished Name (FDN) of the CFS to retrieve a single virtual connection. FDN: MD=<CISCO_EPNM>!CFS=<cfsname> Eg:MD=CISCO_EPNM!CFS=TE Link _192.169.106.12_500_10.140.0.1
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more customer facing services of type **customer-facing-service** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format CFS.<number> are generated by this API. For example: CFS.0004 for 'Managed Element not found with FDN %s' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-customer-facing-service.yang	
Resource	**Description**	

Customer Facing Service Data

Name	Type	Description
customer-facing-service	container	Container holds the customer facing service data.

Parameter Name	Type	Allowed Values	Description
fdn	String		Fully distinguished name of the Customer Facing service. Eg: MD=CISCO_EPNM!CFS=Test_ODU
name	String		Provisioned name of the service. Eg: Test_ODU

discovered-name	String			Name of the discovered service.
service-type	String			It represents multi-layer technology, i.e. optical, mpls-te tunnel, Carrier-E, etc.
service-subtype	String			It represents sub category of the technology type, i.e. Och, Carrier-E EPL, Carrier-E EVPL, etc.
description	String			Indicates the Service description
deployment-schedule-time-iso8601	date-and-time			It shows deployment scheduled time in ISO 8601 format.
last-modified-iso8601	date-and-time			It shows last modified time in ISO 8601 format.
customer-name	String			Customer name For Eg. Infrastructure.
service-state	Enum		service-up, service-auto-up, service-down, service-admin-down, service-partial, service-unavailable, service-not-applicable, service-up-not-protected	It represents the state of the service.
provisioning-status			activate-failed, activate-in-progress, activate-succeeded, create-failed, create-in-progress, create-planned, create-succeeded, deactivate-failed, deactivate-in-progress, deactivate-succeeded, delete-failed, delete-in-progress, delete-planned, delete-succeeded, modify-failed, modify-in-progress, modify-planned, modify-succeeded, no-provisioning-status, promote-succeeded, revert-failed, revert-in-progress, revert-planned, revert-succeeded, cancelled-planned-create, cancelled-planned-modify, cancelled-planned-delete	Provisioning status in response to the provisioning action performed
service-	String			Service template reference

templateref			
profile-ref-list	Container		Service Profile List
fdn	String		Service profile FDN
type	Enum	protection-profile, qos-profile, unknown-profile	Types of user defined profile that can be associated with a customer service.
deployed-configuration	String		Deployed configuration in CLI or other device configuration interfaces
rfsref-list	Container		Resource Facing Service reference.
rfsref	String		FDN of the CFS reference

Note: In case of carrier and carried by services, **service-type** and **service-subtype** attributes supported only for Carrier Nc.

Get All Customer Facing Service

Request

- GET /restconf/data/v1/cisco-service-network: customer-facing-service? serviceSubtype=och-odu

Response

Get CFS for a service

Request

- GET /restconf/data/v1/cisco-service-network:customer-facing-service?fdn=MD=CISCO_EPNM!CFS=<service_name>

Response

- samples/Get_CFS/response.xml

Get CFS – ODU service

Request

- GET /restconf/data/v1/cisco-service-network: customer-facing-service? fdn=MD=CISCO_EPNM!CFS=<oduServiceName>

Response

samples/Get_CFS_Optical_ODU_Service/response.xml

1.34 Network Interface Retrieval

This interface provides operations that retrieve network interface (UNI/ENNI) details. It can be used to retrieve network interfaces available in the system to provide them with provisioning input.

Resource	Description
Network Interface	Retrieves all Network Interfaces (UNI/ENNI) in the system or retrieve specific set based on the input parameters.

HTTP Method	Resource Path
GET	/restconf/data/v1/cisco-service-network:network-interface
Query Parameters	

Name	Type	Description
Fdn	String	Fully Distinguished Name (FDN) of the NI to retrieve a single Network Interface.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more network interfaces of type **network-interface** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format CFS.\<number\> are generated by this API. For example: CFS.0004 for 'Managed Element not found with FDN %s' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-network-interface.yang	

Get Network Interface

Request

• GET /restconf/data/v1/cisco-service-network:network-interface?fdn={fdn}

Response

• samples/Get_Network_Interface/response.xml

1.35 QoS Policy Retrieval

This API retrieves QoS policies in all devices in Cisco EPN Manager. This API can be used to get the FDN of the QoS policy which can be passed in the ingress/egress QoS policies in the order of the service that is being provisioned.

Resource	Description
QoS Policy	Retrieves all QoS Policies in devices added to Cisco EPN Manager.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-qos:qos-policy

Query Parameters		
Name	**Type**	**Description**
Fdn	String (FDN Format)	Fully Distinguished Name (FDN) of the QoS Policy. Given this, a corresponding single QoS Policy will be returned. FDN = MD=<CISCO_EPNM>!ND=<nd_name>!POLICY_QOS=<policyname> Eg: MD=CISCO_EPNM!ND=ASR901-CSG-2-DOMAIN2.cisco.com!POLICY_QOS=money
nfFdn	String (FDN Format)	Fully Distinguished Name (FDN) of the device. Given this, all the QoS Policies for that device will be returned.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • QoS Profile Configuration Access	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more QoS Policies type **qos-policy** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format QOS.<number> are generated by this API. For example: QOS.0010 for 'No node with FDN %s in this user's virtual domain.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-qos.yang	

Request

- GET /restconf/data/v1/cisco-qos:qos-policy

Response

- samples/Get_All_QoS_Policy_Retrieval/response.xml

1.36 QoS Profile Retrieval

This API retrieves QoS profiles in Cisco EPN Manager. This API can be used to get the FDN of the QoS profile which can be passed as a user defined policy for the ingress/egress QoS policies in the order data of the provisioned service.

Resource	Description	
QoS Profile	Retrieves all QoS Profile in Cisco EPN Manager.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-qos:qos-profile	
Query Parameters		
Name	**Type**	**Description**
Fdn	String (FDN Format)	Fully Distinguished Name (FDN) of the QoS Profile. Given this, a corresponding QoS Profile will be returned FDN MD=<CISCO_EPNM>!PROFILE_QOS=<profilename>.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • QoS Profile Configuration Access	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more QoS Profiles of type **qos-profile** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format QOS.<number> are generated by this API. For example: QOS.0001 for 'QoS Profile RDN missing in FDN %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-qos.yang	

1.37 CLI Template Retrieval

This API retrieves CLI templates in Cisco EPN Manager. This API can be used to get the CLI template name and parameters which can be passed to run CLI configuration in resource activation.

Resource	Description	
CLI Template	Retrieves all CLI template in Cisco EPN Manager.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-activation:cli-template	
Query Parameters		
Name	**Type**	**Description**
Name	String	CLI Template name; a corresponding CLI template will be returned.
Authorization Required	One or more from following • Configure Templates	
Response Message		

Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more CLI template of type **cli-template** – see yang model for the data details.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format RA.<number> are generated by this API. For example: RA.0104 for 'Error getting CLITemplate list: %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-resource-activation.yang

Request

- GET /restconf/data/v1/cisco-resource-activation:cli-template?name=<template-name>

Response

- samples/Get_CLI_Template_by_name/response.xml
- samples/Get_CLI_Template_by_name/response.json

1.38 IPSLA Profile Retrieval

This API retrieves IPSLA profiles for L3VPN services in Cisco EPN Manager. This API can be used to get the FDN of the IPSLA profile which can be passed via L3VPN service provision.

Resource	Description
QoS Profile	Retrieves all ISPLA Profile in Cisco EPN Manager.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-service-network:ipsla-profile
Authorization Required	One or more from following - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting
Query Parameters	
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more IPSLA Profiles of type **ipsla-profile** – see yang model for the data details.

HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-ipsla-profile.yang

Get IPSLA Profile

Request

- /restconf/data/v1/cisco-service-network:ipsla-profile

Response

- samples/Get_IPSLA_Profile/response.xml

1.39 Audit Log Retrieval

This API retrieves audit information about login attempts, data retrieval, and data modification by RESTCONF users. The audit subsystem logs data from both the UI and RESTCONF API. The element category with value RESTCONF identifies audit entries generated by RESTCONF API accesses.

The audit log is filterable on all attributes and can be sorted on all attributes.

Resource	Description
Audit Log	Retrieves all Audit Log in Cisco EPN Manager.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-audit:audit-log
Authorization Required	Both • NB API Read • View Audit Log Access
Query Parameters	
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more **audit-logs** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.

	If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	audit-log.yang

Get Audit Log

Request

• GET /restconf/data/v1/cisco-audit:audit-log

Response

• samples/Get_Audit_Log/response.xml
• samples/Get_Audit_Log/response.json

1.40 Resync Service

This API is used to re-synchronize a Circuit / VC to resolve discovery issues such as discovery state is down, or the link between the participating devices is missing, etc.

1.40.1 Resync Service Operation

Operation	Description
resync-service	This operation is used to resync-service
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/network-service:resync-service
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
resync-service-request	Container element
vc-ref-list	Virtual connection fdn list container
vc-ref	Virtual connection fdn. Only one vc-ref is supported
• Authorization Required	One or more from following • Circuit or VC Provisioning • Provisioning Access
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
resync-service-response-list	Container element
resync-service-response	Resync service response
status	Status of the request submitted. Possible values • service-resync-started • service-already-in-resync • device-in-sync • device-not-accessible

	• service-not-exists • service-resync-status-unknown • service-resync-error • service-resync-not-supported • service-ref-not-unique
vc-ref	Virtual connection fdn
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message • 500 Internal Server Error - operation-failed Please refer to RESTCONF standard status codes and standard error response data for further detail.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format VC.<number> are generated by this API. For example: VC.0017 for 'Invalid input. resync-service-request, vc-ref-list and vc-ref elements are mandatory.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx

1.40.2 Resync Service Operation

Request

- POST /restconf/operations/v1/network-service:resync-service
- samples/Resync_Service/request.xml

Response

- samples/Resync_Service/response.xml

1.41 Service Activation

Operations

The following sub-sections provide the details of the operations that can be used for service activation.

1.41.1.1 *Provision Service*

Operation	Description
Provision a Service	This operation can be used to provision a service.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-activation:provision-service
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json

Request Data	Request data of type **provision-service-request** that contains the details of the service type and **order-data** and other related data – see yang model for the data details.
Authorization Required	One or more from following • Circuit or VC Provisioning • Provisioning Access
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return a provisioning response of type **provision-service-response** that contains the details of the execution which includes service reference details, device CLI details, etc. – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format PROV.\<number\> are generated by this API. For example: PROV.0024 for 'A service exist with same name.' If error is from underlying framework/core modules error-app-tag format one of following • TP.\<number\> - any tag starting with "TP." prefix for any internal errors like TP.0004 =Invalid TerminationPoint - FDN: %s - name is missing. • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	• cisco-service-activation.yang

1.41.1.1.1 Provision Service Request

Name	Type	Description
provision-service-request	Container element	Holds the data for provisioning a service.
service-order-data	service-order-data type	Container holding the service order data – see the order data sections for details on each service type data.

1.41.1.1.2 Provision Service Response

Name	Type	Description
provision-service-response	Container element	Holds the data for provision service response.
customer-ref	String (FDN)	FDN of the service to be created. e.g., MD=CISCO_EPNM!CUSTOMER=Infrastructure
ni-ref	String (FDN)	FDN of the Network Interface (UNI/ENNI) e.g., MD=CISCO_EPNM!NI=\<NI Name\>
request-id	uuid	Request id to track the provisioning request.
service-name	String	Service name.
service-type	String	Service type.

service-subtype	String	Service subtype.
Preview	Boolean	Is preview true/false. **Note**: This will be deprecated soon, start using deploy-action tag in payload to specify "Preview", "Deploy", "Later" or "Scheduled"
request-time	DateTime	Request time.
completion-time	DateTime	Completion time.
deploy-results	Container element	Holds the response for provision.
Result	Container element	Holds the response for provision.
node-ref	String (FDN)	FDN for the node.
State	String	Provisioning state. (SUCCESSFUL, FAILED, NOT_STARTED, NOT_APPLICABLE)
Info	String	Provision information.
Config	String	Device configuration.
Error	String	Error in provisioning.
rollback-config	String	Rollback Device configuration.
rollback-errors	String	Error in rollback provisioning.
work-flow-result	Container element	Holds the response for provision in case of Workflows.
cfs-ref	String (FDN)	FDN of the service to be created.
ni-ref	String (FDN)	FDN of the Network Interface (UNI/ENNI).
service-type	String	Service type.
work-flow-index	String	Workflow index.
work-flow-name	String	Workflow name.
Result	Container element in Workflow Results	Holds the response for provision in case of Workflows.
node-ref	String (FDN)	FDN for the node.
State	String	Provisioning state. (SUCCESSFUL, FAILED, NOT_STARTED, NOT_APPLICABLE)
Info	String	Provision information.
Config	String	Device configuration.
Error	String	Error in provisioning.
rollback-config	String	Rollback Device configuration.
rollback-errors	String	Error in rollback provisioning.
completion-status	String	Provisioning state. (SUCCESS, FAILED, PENDING, SUBMITTED).
Error	String	Error in provisioning.
validation-error	String	Validation Error in provisioning.
request-validation-error	String	Request Validation Error in provisioning.
test-ref	Container element	Holds the test id's for provision in case of service test included.
test-id	String	List of test id's invoked.

1.41.1.2   *Provision CEM Service Examples*

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service/request.xml
- samples/Provision_CEM_Service/request.json

Response
- samples/Provision_CEM_Service/response.json

Notification

- samples/Provision_CEM_Service/notification.xml

1.41.1.2.1 Provision CEM Service with uni-directional tunnel as preferred path Example

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service_with_uni_directional_tunnel_as_preferred_path/request.xml

Response

- samples/Provision_CEM_Service_with_uni_directional_tunnel_as_preferred_path/response.xml

1.41.1.2.2 Provision CEM Service Consolidated: CEM+MPLS TE+BERT

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service_Consolidated_CEM_MPLS_TE_BERT/request.xml
- samples/Provision_CEM_Service_Consolidated_CEM_MPLS_TE_BERT/request.json

Response

- samples/Provision_CEM_Service_Consolidated_CEM_MPLS_TE_BERT/response.json

Notification

- samples/Provision_CEM_Service_Consolidated_CEM_MPLS_TE_BERT/notification.json

1.41.1.2.3 Provision CEM Service with Service and Tunnel Profiles

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service_with_service_and_tunnel_profiles/request.xml

Response

- samples/Provision_CEM_Service_with_service_and_tunnel_profiles/response.xml

1.41.1.2.4 Provision CEM Service with MPLS TE and LSP

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service_with_MPLS_TE_and_LSP/request.xml

Response

- samples/Provision_CEM_Service_with_MPLS_TE_and_LSP/response.xml

1.41.1.2.5 Provision CEM Service with MPLS TE – RO to RO devices

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service_with_MPLS_TE_RO_to_RO_devices/request.xml

Response
- samples/Provision_CEM_Service_with_MPLS_TE_RO_to_RO_devices/response.xml

1.41.1.2.6 Provision CEM Service with MPLS TE – RO to CO devices

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service_with_MPLS_TE_RO_to_CO_devices/request.xml

Response
- samples/Provision_CEM_Service_with_MPLS_TE_RO_to_CO_devices/response.xml

1.41.1.2.7 Provision CEM Service with MPLS TE – CO to RO devices

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Modify_CEM_Service_with_MPLS_TE_CO_to_RO_devices/request.xml

Response
- samples/Modify_CEM_Service_with_MPLS_TE_CO_to_RO_devices/response.xml

1.41.1.2.8 Provision CEM VC4 Service over SDH Controller

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_VC4_Service_over_SDH_Controller/request.xml

Response
- samples/Provision_CEM_VC4_Service_over_SDH_Controller/response.xml

1.41.1.2.9 Provision CEM VC4-4c Service over SDH Controller

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_VC4-4c_Service_over_SDH_Controller/request.xml

Response
- samples/Provision_CEM_VC4-4c_Service_over_SDH_Controller/response.xml

1.41.1.2.10 Provision CEM VC4-16c Service over SDH Controller

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_VC4-16c_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_VC4-16c_Service_over_SDH_Controller/response.xml

1.41.1.2.11   Provision CEM STS-1 Service over SONET Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_STS1_over_SONET_Controller/request.xml

Response

- samples/Provision_CEM_STS1_over_SONET_Controller/response.xml

1.41.1.2.12   Provision CEM DS0 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_DS0_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_DS0_Service_over_SDH_Controller/response.xml

1.41.1.2.13   Provision CEM T1 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_T1_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_T1_Service_over_SDH_Controller/response.xml

1.41.1.2.14   Provision CEM T3 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_T3_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_T3_Service_over_SDH_Controller/response.xml

1.41.1.2.15   Provision CEM E1 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_E1_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_E3_Service_over_SDH_Controller/response.xml

1.41.1.2.16 Provision CEM E3 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_E3_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_E3_Service_over_SDH_Controller/response.xml

1.41.1.2.17 Provision CEM VC11 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_VC11_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_VC11_Service_over_SDH_Controller/response.xml

1.41.1.2.18 Provision CEM VC12 Service over SDH Controller

Request

POST /restconf/operations/v1/cisco-service-activation:provision-service

- samples/Provision_CEM_VC12_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_VC12_Service_over_SDH_Controller/response.xml

1.41.1.2.19 Provision CEM service with MSP 1+1 protection

Request

POST /restconf/operations/v1/cisco-service-activation:provision-service

- samples/Provision_CEM_SDH_MSP_VC12/request.xml
- samples/Provision_CEM_SDH_MSP_VC4/request.xml

Response

- samples/Provision_CEM_SDH_MSP_VC12/response.xml
- samples/Provision_CEM_SDH_MSP_VC4/response.xml

1.41.1.2.20 Provision CEM service with SNCP protection

Request

POST /restconf/operations/v1/cisco-service-activation:provision-service

- samples/Provision_CEM_SDH_SNCP/request.xml

Response

- samples/Provision_CEM_SDH_SNCP/response.xml

1.41.1.2.21　　Provision CEM e3 service over e3 controller

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_e3_service_over_e3_controller/request.xml

Response
- samples/Provision_CEM_e3_service_over_e3_controller/response.xml

1.41.1.2.22　　Provision CEM service over STS1e controller

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_Service_over_STS1e_Controller/Cem-e3-service-over-STS1E-controller-create-request.xml
- samples/Provision_CEM_Service_over_STS1e_Controller/Cem-STS-1-service-with-1-plus-1-card-protection-over-STS1E-controller-create-request.xml
- samples/Provision_CEM_Service_over_STS1e_Controller/Cem-vt1.5-service-over-STS1E-controller-create-request.xml

Response
- samples/Provision_CEM_Service_over_STS1e_Controller/Cem-e3-service-over-STS1E-controller-create-response.xml
- samples/Provision_CEM_Service_over_STS1e_Controller/Cem-STS-1-service-with-1-plus-1-card-protection-over-STS1E-controller-create-response.xml
- samples/Provision_CEM_Service_over_STS1e_Controller/Cem-vt1.5-service-over-STS1E-controller-create-response.xml

1.41.1.2.23　　Provision MPLS-TE Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_MPLS_TE_Service/request.xml
- samples/Provision_MPLS_TE_Service/request.json

Response
- samples/Provision_MPLS_TE_Service/response.xml

1.41.1.2.24　　Provision MPLS-TE Bidirectional Tunnel with LSP

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_MPLS_TE_Bidirectional_Tunnel_with_LSP/request.xml

Response
- samples/Provision_MPLS_TE_Bidirectional_Tunnel_with_LSP/response.json

1.41.1.2.25   Provision MPLS-TE Unidrectional Tunnel with Auto Bandwith

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_MPLS_TE_Unidirectional_Tunnel_with_Auto_Bandwidth/request.xml

Response
- samples/Provision_MPLS_TE_Unidirectional_Tunnel_with_Auto_Bandwidth/response.xml

1.41.1.2.26   Provision MPLS-TE with existing bfd template

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_MPLS_TE_Service_with_Existing_BFD/request.xml

Response
- samples/Provision_MPLS_TE_Service_with_Existing_BFD/response.xml

1.41.1.2.27   Provision MPLS-TE with new bfd template

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_MPLS_TE_Service_with_New_BFD/request.xml

Response
- samples/Provision_MPLS_TE_Service_with_New_BFD/response.xml

1.41.1.2.28   Provision MPLS-TE with Flex-Lsp

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_MPLS_TE_Bidirectional_Tunnel_with_FlexLsp/request.xml

Response
- samples/Provision_MPLS_TE_Bidirectional_Tunnel_with_FlexLsp/response.xml

1.41.1.2.29   Provision CE Service

Note : While provisioing ELINE/ACCESS (EPL/EVPL) service we can either create UNIs/ENNIs along with service create or we can make use of existing UNIs/ENNIs during service create/modify.
Below tag should be used when an NBI user want to create UNIs/ENNIs during service create

```
<p:termination-point-list> ➔ <p:termination-point-config> ➔ <p:network-
interface-name>

<p:network-interface-list> ➔ <p:network-interface> ➔ <p:name>
```

```
<p:operation>add</p:operation>
```
Below tag should be used when an NBI user want to re-use existing UNIs/ENNIs during service create/modify.
```
<p:termination-point-list> → <p:termination-point-config> → <p:network-
interface-ref>
```

```
<p:network-interface-list> → <p:network-interface> → <p:ref>
<p:operation>update</p:operation>
```

1.41.1.2.30   Provision EPL Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EPL_Service/request.xml
- samples/Provision_EPL_Service/request.json

Response
- samples/Provision_EPL_Service/response.xml

Notification
- samples/Provision_EPL_Service/notification.xml

1.41.1.2.31   Provision EPL Service – EPL over Bi-Directional Tunnel

Request
- POST /restconf/operations/v1/cisco-service-activation: provision-service
- samples/Provision_EPL_Service_EPL_Over_Bi_Directional_Tunnel/request.xml

Response
- samples/Provision_EPL_Service_EPL_Over_Bi_Directional_Tunnel/response.json

1.41.1.2.32   Provision EPL with Profile

Request
- POST /restconf/operations/v1/cisco-service-activation: provision-service
- samples/Provision_EPL_with_Profile/request.xml

Response
- samples/Provision_EPL_with_Profile/response.xml

1.41.1.2.33   Provision EVPL Service – EVPL over Uni-directional Tunnel

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_EVPL_over_Uni_Directional_Tunnel/request.xml

Response
- samples/Provision_EVPL_Service_EVPL_over_Uni_Directional_Tunnel/response.json

1.41.1.2.34   Provision EVPL Service – EVPL with Pref Path UNI

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_with_Pref_Path_UNI/request.xml

Response
- samples/Provision_EVPL_with_Pref_Path_UNI/response.json

1.41.1.2.35   Provision EVPL Service – EVPL Provide with Existing Tunnel

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_with_Existing_Tunnel/request.xml

Response
- samples/Provision_EVPL_Service_with_Existing_Tunnel/response.json

1.41.1.2.36   Provision EVPL with existing SR Policies

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision-SRPolicy-EVPL/EVPL-Request.xml

Response
- samples/Provision-SRPolicy-EVPL/EVPL-Response.xml

1.41.1.2.37   Provision EVPL – EVPL with Modular QoS

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service

  samples/Provision_EVPL_Service_EVPL_Modular_QoS/request.xml

Response

  samples/Provision_EVPL_Service_EVPL_Modular_QoS/response.xml

1.41.1.2.38   Provision ELINE service with EVPN

In order to provision an ELINE service with EVPN, NBI input payload should have value as "bgp" for the "signaling-protocol" tag, otherwise it will go to default case i.e. ELINE service provisioning with/without pseudo wire settings.

Note:

1. ELINE service provisioning with EVPN is currently applicable only for regular EPL and EVPL services. ELINE hairpin, local connect and partial services with EVPN are currently not supported by EPNM.

2. ELINE service provisioning with EVPN currently support SR TE policies as preferred path in case "enable-static-preferred-path" is provided as "true" in the NBI payload. EPNM currently don't support MPLS TE tunnels as preferred paths for EVPN based services.

3. When user tries to reuse the same evpn-instance-id for multiple services then they need to ensure that the values for input attributes route-distinguisher , import-route-target, export-route-target & enable-control-word are provided same as the value used for the existing EVPN service , otherwise EPNM will throw an error during creation or modification of the service.

Below is the sample request and response for ELINE EVPL service provisioning.

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision-EVPL-With-EVPN/request.xml
- samples/Provision-EVPL-With-EVPN/request.json

Response
- samples/Provision-EVPL-With-EVPN/response.xml

1.41.1.2.39   Provision EVPL service with CFM ICC format

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_With_CFM_ICC_Format/request.xml
- samples/Provision_EVPL_With_CFM_ICC_Format/request.json

Response
- samples/Provision_EVPL_With_CFM_ICC_Format/response.xml
- samples/Provision_EVPL_With_CFM_ICC_Format/response.json

1.41.1.2.40

1.41.1.2.41   Provision EP-LAN Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EP_LAN_Service/request.xml
- samples/Provision_EP_LAN_Service/request.json

Response
- samples/Provision_EP_LAN_Service/response.json

1.41.1.2.42   Provision EVP LAN Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVP_LAN_Service/request.xml
- samples/Provision_EVP_LAN_Service/request.json

Response
- samples/Provision_EVP_LAN_Service/response.xml

1.41.1.2.43   Provision EVP LAN with HVPLS Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVP_LAN_with_HVPLS_Service/request.xml

Response
- samples/Provision_EVP_LAN_with_HVPLS_Service/response.xml

1.41.1.2.44   Provision EP-Tree Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EP_Tree_Service/request.xml
- samples/Provision_EP_Tree_Service/request.json

Response
- samples/Provision_EP_Tree_Service/response.json

1.41.1.2.45   Provision EVP-Tree Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVP_Tree_Service/request.xml
- samples/Provision_EVP_Tree_Service/request.json

Response
- samples/Provision_EVP_Tree_Service/response.json

1.41.1.2.46   Provision EVP-Tree H-VPLS

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVP_Tree_H_VPLS/request.xml

Response
- samples/Provision_EVP_Tree_H_VPLS/response.json

1.41.1.2.47   Provision Access EPL Service

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Access_EPL_Service/request.xml
- samples/Provision_Access_EPL_Service/request.json

Response

- samples/Provision_Access_EPL_Service/response.json

1.41.1.2.48   Provision Access EVPL Service

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Access_EVPL_Service/request.xml
- samples/Provision_Access_EVPL_Service/request.json

Response

- samples/Provision_Access_EVPL_Service/response.json

1.41.1.2.49   Provision QoS Profile Service
**NOTE: This API support is deprecated from 3.x

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_QoS_Profile_Service/request.xml
- samples/Provision_QoS_Profile_Service/request.json

Response

- samples/Provision_QoS_Profile_Service/response.json

1.41.1.2.50   Provision UNI Service

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_UNI_Service/request.xml
- samples/Provision_UNI_Service/request.json

Response

- samples/Provision_UNI_Service/response.json

1.41.1.2.51   Provision ENNI Service

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_ENNI_Service/request.xml

Response

- samples/Provision_ENNI_Service/response.json

1.41.1.2.52   Provision CE Partial Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CE_Partial_Service/request.xml

Response
- samples/Provision_CE_Partial_Service/response.xml

1.41.1.2.53   Provision EVPL Service Over Uni Directional Tunnel Between Remote Office to Remote Office Devices with MPLS Enabled

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_Between_Remote_Office_to_Remote_Office_Devices_with_MPLS_Enabled/request.xml

Response
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_Between_Remote_Office_to_Remote_Office_Devices_with_MPLS_Enabled/response.xml

1.41.1.2.54   Provision EVPL Service Over Uni Directional Tunnel Between Central Office to Remote Office Devices with MPLS Enabled

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_Between_Central_Office_to_Remote_Office_Devices_with_MPLS_Enabled/request.xml

Response
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_Between_Central_Office_to_Remote_Office_Devices_with_MPLS_Enabled/response.xml

1.41.1.2.55   Provision EVPL Service Over Uni Directional Tunnel – NID to NID

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_NID_to_NID/request.xml

Response
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_NID_to_NID/response.xml

1.41.1.2.56 Provision EVPL Service Over Uni Directional Tunnel – NID to Remote Building

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_NID_to_Remote_Building/request.xml

Response
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_NID_to_Remote_Building/response.xml

1.41.1.2.57 Provision EVPL Service Over Uni Directional Tunnel – NID to Service Edge

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_NID_to_Service_Edge/request.xml

Response
- samples/Provision_EVPL_Service_Over_Uni_Directional_Tunnel_NID_to_Service_Edge/response.xml

1.41.1.2.58 Provision EVPL Service with Autoroute Enabled

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_EVPL_Service_with_Autoroute_Enabled/request.xml

Response
- samples/Provision_EVPL_Service_with_Autoroute_Enabled/response.xml

1.41.1.2.59 Provision L3 Link

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_L3_Link/request.xml
- samples/Provision_L3_Link/request.json

1.41.1.2.60 Provision L3 Link with BGP routing protocol

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_L3_Link_with_BGP_routing_protocol/request.xml
- samples/Provision_L3_Link_with_BGP_routing_protocol/request.json

1.41.1.2.61 Provision L3 Link with ISIS routing protocol

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_L3_Link_with_ISIS_routing_protocol/request.xml
- samples/Provision_L3_Link_with_ISIS_routing_protocol/request.json

1.41.1.2.62 Provision L3VPN

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_L3VPN_Service/request.xml
- samples/Provision_L3VPN_Service/request.json

Response
- samples/Provision_L3VPN_Service/response.xml

Request with BGP IPv4
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_L3VPN_BGP_IPV4/request.xml

Response
  samples/Provision_L3VPN_BGP_IPV4/response.xml

Request with BGP IPv6
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_L3VPN_BGP_IPV6/request.xml

Response
  samples/Provision_L3VPN_BGP_IPV6/response.xml

Request with BGP OSPFv3
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_L3VPN_OSPFV3/request.xml

Response
  samples/Provision_L3VPN_OSPFV3/response.xml

1.41.1.2.63 Provision Optical Service OCHNC

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Optical_Service/request.xml
- samples/Provision_Optical_Service/request.json

Response
- samples/Provision_Optical_Service/response.xml

Notification
- samples/Provision_Optical_Service/notification.xml

1.41.1.2.64   Provision OCHTrail UNI

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_OCHTrail_UNI/request.xml
- samples/Provision_OCHTrail_UNI/request.json

Response
- samples/Provision_OCHTrail_UNI/response.xml

1.41.1.2.65   Provision OCHNC Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_OCHNC_Service/request.xml
- samples/Provision_OCHNC_Service/request.json

Response
- samples/Provision_OCHNC_Service/response.xml

1.41.1.2.66   Provision OCHCC Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_OCHCC_Service/request.xml
- samples/Provision_OCHCC_Service/request.json

Response
- samples/Provision_OCHCC_Service/response.xml

1.41.1.2.67   Provision OCHTrail Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_OCHTrail_Service/request.xml
- samples/Provision_OCHTrail_Service/request.json

Response
- samples/Provision_OCHTrail_Service/response.xml

1.41.1.2.68   Provision ODU_Tunnel Service

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_ODU_Tunnel_Service/request.xml
- samples/Provision_ODU_Tunnel_Service/request.json

Response

- samples/Provision_ODU_Tunnel_Service/response.xml

1.41.1.2.69   Provision ODU_UNI Service

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_ODU_UNI_Service/request.xml
- samples/Provision_ODU_UNI_Service/request.json

Response

- samples/Provision_ODU_UNI_Service/response.xml

1.41.1.2.70   Provision ODU_UNI with default explicit path

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-servicetpref
- samples/Provision_ODU_UNI_Explicit_Path/request.xml
- samples/Provision_ODU_UNI_Explicit_Path/request.json

Response

- samples/Provision_ODU_UNI_Explicit_Path/response.xml
- samples/Provision_ODU_UNI_Explicit_Path/response.json

1.41.1.2.71   Provision Mutually Diverse OCHTrail UNI

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Mutually_Diverse_OCHTrail_UNI/request.xml
- samples/Provision_Mutually_Diverse_OCHTrail_UNI/request.json

Response

- samples/Provision_Mutually_Diverse_OCHTrail_UNI/response.xml

1.41.1.2.72   Provision OPU Over ODU

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_OPU_Over_ODU/request.xml
- samples/Provision_OPU_Over_ODU/request.json

Response

- samples/Provision_OPU_Over_ODU/response.xml

1.41.1.2.73 Provision ODU UNI Hairpin

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_ODU_UNI_Hairpin/request.xml

Response
- samples/Provision_ODU_UNI_Hairpin/response.xml

1.41.1.2.74 Provision ODU

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_ODU_Service/request.xml

Response
- samples/Provision_ODU_Service/response.xml

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_ODU_LocalCrossConnect_Service/request.xml

Response
- samples/Provision_ODU_LocalCrossConnect_Service /response.xml

1.41.1.2.75 Provision Media Channel Group

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Media_Channel_Group/request.xml

Response
- samples/Provision_Media_Channel_Group/response.xml

1.41.1.2.76 Provision Media Channel NC

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Media_Channel_NC/request.xml

Response
- samples/Provision_Media_Channel_NC/response.xml

1.41.1.2.77 Provision Media Channel CC

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Media_Channel_CC/request.xml

Response
- samples/Provision_Media_Channel_CC/response.xml

1.41.1.2.78 Provision Media Channel Trail

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Media_Channel_Trail/request.xml

Response
- samples/Provision_Media_Channel_Trail/response.xml

1.41.1.2.79 Provision OCHTrail MP(Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Managed_Plane_OCH_Trail/request.xml

Response
- samples/Provision_Managed_Plane_OCH_Trail/response.xml

1.41.1.2.80 Provision OCHCC MP(Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Managed_Plane_OCH_CC/request.xml

Response
- samples/Provision_Managed_Plane_OCH_CC/response.xml

1.41.1.2.81 Provision OCHNC MP(Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Managed_Plane_OCH_NC/request.xml

Response
- samples/Provision_Managed_Plane_OCH_NC/response.xml

1.41.1.2.82 Provision SR-TE Dynamic

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_Sr-Te_Dynamic/request.xml

Response
- samples/Provision_Sr-Te_Dynamic/response.xml

1.41.1.2.83   Provision SR-TE DynamicPCE

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/ Provision_Sr-Te_DynamicPCE/request.xml

Response
- samples/ Provision_Sr-Te_DynamicPCE/response.xml

1.41.1.2.84   Provision SR-TE Explicit

Request
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/ Provision_Sr-Te_Explicit/request.xml

Response
- samples/ Provision_Sr-Te_Explicit/response.xml

1.41.1.3   *Modify Service*

Operation	Description
Modify existing service	This operation can be used to modify existing service.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-activation:modify-service
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type modify-service-request that contains the details of the service type and order-data and other related data – see yang model for the data details.
Authorization Required	One or more from following • Circuit or VC Provisioning • Provisioning Access
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return a modify response of type **modify-service-response** that contains the details of the execution that includes service reference details, device cli details, etc. – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	• cisco-service-activation.yang

1.41.1.3.1 Modify Service Request

Name	Type	Description
modify-service-request	Container element	Holds the data for modifying an existing

		service.
cfs-ref	String (FDN)	FDN of the service to be modified.
ni-ref	String (FDN)	FDN of the Network Interface (UNI/ENNI) to be modified. This field is needed instead of cfs-ref in Network Interface (UNI/ENNI) modification case only.
service-order-data	service-order-data type	Container holding the service order data – see the order data sections for details on each service type data.
network-interface-list → network-interface → name		In Modify payload, ref , eq : sa.ref : "MD=CISCO_EPNM!NI=name" is sufficient. Name attribute is not needed

1.41.1.3.2 Modify Service Response

Name	Type	Description
modify-service-response	Container element	Holds the data for modify service response.
Refer Provision-service-response		

1.41.1.3.3 Modify CEM Service Example

Note: During CEM service modify, when user want to change HOP or LOP along with SINK end point details of the service then below tag need to be specified in NBI payload under. *termination-point-config → cem-data → is-hop-or-lop-changed*

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_CEM_Service/request.xml
- samples/Modify_CEM_Service/request.json

Response
- samples/Modify_CEM_Service/response.json

Notification
- samples/Modify_CEM_Service/notification.xml

1.41.1.3.4 Modify CEM Service with MPLS TE – RO to RO Devices

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_CEM_Service_with_MPLS_TE_RO_to_RO_devices/request.xml

Response
- samples/Modify_CEM_Service_with_MPLS_TE_RO_to_RO_devices/response.xml

1.41.1.3.5 Modify CEM Service with MPLS TE – RO to CO Devices

Request

- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_CEM_Service_with_MPLS_TE_RO_to_CO_devices/request.xml

Response

- samples/Modify_CEM_Service_with_MPLS_TE_RO_to_CO_devices/response.xml

1.41.1.3.6 Modify CEM Service with MPLS TE – CO to RO Devices

Request

- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_CEM_Service_with_MPLS_TE_CO_to_RO_devices/request.xml

Response

- samples/Modify_CEM_Service_with_MPLS_TE_CO_to_RO_devices/response.xml

1.41.1.3.7 Modify EPL Service

Request

- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_EPL_Service/request.xml
- samples/Modify_EPL_Service/request.json

Response

- samples/Modify_EPL_Service/response.json

1.41.1.3.8 Modify EVPL Service with EVPN

Request

- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_EPL_With_EVPN_Service/request.xml
- samples/Modify_EPL_With_EVPN_Service/request.json

Response

- samples/Modify_EPL_With_EVPN_Service/response.json

1.41.1.3.9 Modify ENNI Service

Request

- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_ENNI_Service/request.xml

Response

- samples/Modify_ENNI_Service/response.json

1.41.1.3.10   Modify L3 Link with OSPF routing protocol

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_L3_Link_with_OSPF_routing_protocol/request.xml
- samples/Modify_L3_Link_with_OSPF_routing_protocol/request.json

1.41.1.3.11   Modify L3 Link with BGP Routing Protocol

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_L3_Link_with_BGP_routing_protocol/request.xml
- samples/Modify_L3_Link_with_BGP_routing_protocol/request.json

1.41.1.3.12   Modify L3 Link with ISIS Routing Protocol

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_L3_Link_with_ISIS_routing_protocol/request.xml
- samples/Modify_L3_Link_with_ISIS_routing_protocol/request.json

1.41.1.3.13   Modify L3VPN Service (Add VRF)

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_L3VPN_Service_Add_VRF/request.xml
- samples/Modify_L3VPN_Service_Add_VRF/request.json

Response
- samples/Modify_L3VPN_Service_Add_VRF/response.json

1.41.1.3.14   Modify L3VPN Service (Modify VPN)

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_L3VPN_Service_Modify_VPN/request.xml

Response
- samples/Modify_L3VPN_Service_Modify_VPN/response.xml

1.41.1.3.15   Modify L3VPN Service (Modify VPN) with service MTU

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- sample/Modify_L3VPN_Service_Modify_VPN_Service_MTU/request.xml
- sample/Modify_L3VPN_Service_Modify_VPN_Service_MTU/request.json

Response
- samples/Modify_L3VPN_Service_Modify_VPN_Service_MTU/response.xml

- samples/Modify_L3VPN_Service_Modify_VPN_Service_MTU/response.json

1.41.1.3.16 Modify Optical Service OCHNC

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Optical_Service/request.xml
- samples/Modify_Optical_Service/request.json

Response
- samples/Modify_Optical_Service/response.xml

Notification
- samples/Modify_Optical_Service/notification.xml

1.41.1.3.17 Modify OCHTrail UNI

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_OCHTrail_UNI/request.xml
- samples/Modify_OCHTrail_UNI/request.json

Response
- samples/Modify_OCHTrail_UNI/response.xml

1.41.1.3.18 Modify OCHNC Service

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_OCHNC_Service/request.xml
- samples/Modify_OCHNC_Service/request.json

Response
- samples/Modify_OCHNC_Service/response.xml

1.41.1.3.19 Modify OCHCC Service

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_OCHCC_Service/request.xml
- samples/Modify_OCHCC_Service/request.json

Response
- samples/Modify_OCHCC_Service/response.xml

1.41.1.3.20 Modify OCHTrail Service

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service

- samples/Modify_OCHTrail_Service/request.xml
- samples/Modify_OCHTrail_Service/request.json

Response
- samples/Modify_OCHTrail_Service/response.xml

1.41.1.3.21   Modify ODU_Tunnel Service

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_ODU_Tunnel_Service/request.xml
- samples/Modify_ODU_Tunnel_Service/request.json

Response
- samples/Modify_ODU_Tunnel_Service/response.xml

1.41.1.3.22   Modify ODU_UNI Service

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_ODU_UNI_Service/request.xml
- samples/Modify_ODU_UNI_Service/request.json

Response
- samples/Modify_ODU_UNI_Service/response.xml

1.41.1.3.23   Modify OPU Over ODU

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_OPU_Over_ODU/request.xml
- samples/Modify_OPU_Over_ODU/request.json

Response
- samples/Modify_OPU_Over_ODU/response.xml

1.41.1.3.24   Modify ODU UNI Hairpin

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_ODU_UNI_Hairpin/request.xml

Response
- samples/Modify_ODU_UNI_Hairpin/response.xml

1.41.1.3.25   Modify ODU Service

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_ODU_Service/request.xml

- samples/Modify_ODU_Service/request.json

    Response
- samples/Modify_ODU_Servicee/response.xml

    Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_ODU_LocalCrossConnect_Service/request.xml

    Response
- samples/Modify_ODU_LocalCrossConnect_Service/response.xml

1.41.1.3.26 Modify Media Channel Group

   Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Media_Channel_Group/request.xml

   Response
- samples/Modify_Media_Channel_Group/response.xml

1.41.1.3.27 Modify Media Channel NC

   Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Media_Channel_NC/request.xml

   Response
- samples/Modify_Media_Channel_NC/response.xml

1.41.1.3.28 Modify Media Channel CC

   Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Media_Channel_CC/request.xml

   Response
- samples/Modify_Media_Channel_CC/response.xml

1.41.1.3.29 Modify Media Channel Trail

   Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Media_Channel_Trail/request.xml

   Response
- samples/Modify_Media_Channel_Trail/response.xml

1.41.1.3.30   Modify OCHTrail MP (Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Managed_Plane_OCH_Trail/request.xml

Response
- samples/Modify_Managed_Plane_OCH_Trail/response.xml

1.41.1.3.31   Modify OCHCC MP (Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Managed_Plane_OCH_CC/request.xml

Response
- samples/Modify_Managed_Plane_OCH_CC/response.xml

1.41.1.3.32   Modify OCHNC MP (Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Managed_Plane_OCH_NC/request.xml

Response
- samples/Modify_Managed_Plane_OCH_NC/response.xml

1.41.1.3.33   Modify SR-TE service

Request
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- samples/Modify_Sr-Te/request.xml

Response
- samples/Modify_Sr-Te/response.xml

1.41.1.4   *Terminate Service*

Operation	Description
Terminate existing Service	This operation can be used to terminate existing service.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-activation:terminate-service
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **terminate-service-request** that contains the details of the service type and service reference and other related data – see yang model for the data details.

Authorization Required	One or more from following
	• Circuit or VC Provisioning
	• Provisioning Access
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return a provisioning response of type **terminate-service-response** that contains the details of the execution that includes service reference details, device cli details, etc. – see yang model for the data details.
HTTP Status Code	• 200 OK- Success with response message-body
	• 401, 403– Authentication and Authorization errors.
	• 400 Bad Request - Invalid request message.
	• 500 Internal Server Error - operation-failed.
	Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	• cisco-service-activation.yang

1.41.1.4.1 Terminate Service Request

Name	Type	Description
terminate-service-request	Container element	Holds the data for terminating the service.
cfs-ref	String (FDN)	FDN of the service to be terminated.
ni-ref	String (FDN)	FDN of the Network Interface (UNI/ENNI) to be terminated. This field is needed instead of cfs-ref in Network Interface (UNI/ENNI) termination case only.

1.41.1.4.2 Terminate Service Response

Name	Type	Description
terminate-service-response	Container element	Holds the data for terminating the service's response.
Refer Provision-service-response		

CEM, Optical and MPLS-TE service provisioning is supported through the set of operations defined as RESTCONF Operations. When the OSS client uses this interface for service provisioning, a set of CFS (Customer Facing Service) and RFS (Resource Facing Service) objects will be created or modified to handle the service management in Cisco EPN Manager.

The API provides support for provisioning the following services:

Technology	Service Type	Service Sub Type
CE	carrier-ethernet-vpn	EPL, EVPL, ACESS EPL, ACESS EVPL, EP-LAN, EVP-LAN, EP-Tree, EVP-Tree
CEM	tdm-cem	T1, T3, E1, E3,VT1.5,OC1,OC3, OC12,OC48
MPLS-TE	mpls-te-tunnel	Bidirectional, Unidirectional TE Tunnel, Layer 3 Link
L3VPN	mpls-l3-vpn	L3VPN
Optical	optical	OCHNC, OCHCC, OCHTrail, OCHTrail-UNI, OPU-Over-ODU, ODU_UNI, ODU_TUNNEL

1.41.1.4.3 Terminate CEM Service

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_CEM_Service/request.xml
- samples/Terminate_CEM_Service/request.json

Response
- samples/Terminate_CEM_Service/response.json

Notification
- samples/Terminate_CEM_Service/notification.xml

1.41.1.4.4 Terminate CEM Service with MPLS TE

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_CEM_Service_with_MPLS_TE/request.xml

Response
- samples/Terminate_CEM_Service_with_MPLS_TE/response.xml

1.41.1.4.5 Terminate EPL Service

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_EPL_Service/request.xml
- samples/Terminate_EPL_Service/request.json

Response
- samples/Terminate_EPL_Service/response.json

1.41.1.4.6 Terminate EVPL Service Along with Tunnels

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_EVPL_Service_along_with_Tunnels/request.xml
- samples/Terminate_EVPL_Service_along_with_Tunnels/request.json

Response

1.41.1.4.7 Terminate ENNI Service

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_ENNI_Service/request.xml

Response
- samples/Terminate_ENNI_Service/response.json

1.41.1.4.8 Terminate L3 Link Service (OSPF/BGP/ISIS)

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_L3_Link_Service/request.xml

1.41.1.4.9 Terminate L3VPN

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_L3VPN/request.xml
- samples/Terminate_L3VPN/request.json

Response
- samples/Terminate_L3VPN/response.json

1.41.1.4.10 Terminate Optical Service OCHNC

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Optical_Service/request.xml
- samples/Terminate_Optical_Service/request.json

Response
- samples/Terminate_Optical_Service/response.xml

Notification
- samples/Terminate_Optical_Service/notification.xml

1.41.1.4.11 Terminate OCHTrail UNI

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_OCHTrail_UNI/request.xml
- samples/Terminate_OCHTrail_UNI/request.json

Response
- samples/Terminate_OCHTrail_UNI/response.xml

1.41.1.4.12 Terminate OCHNC Service

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_OCHNC_Service/request.xml

Response
- samples/Terminate_OCHNC_Service/response.xml

1.41.1.4.13 Terminate OCHCC Service

Request

- POST /restconf/operations/v1/cisco-service-activation:terminate-service
  samples/Terminate_OCHCC_Service/request.xml
  Response
- samples/Terminate_OCHCC_Service/response.xml

1.41.1.4.14 Terminate OCHTrail Service

Request

- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_OCHTrail_Service/request.xml
- samples/Terminate_OCHTrail_Service/request.json

Response

- samples/Terminate_OCHTrail_Service/response.xml

1.41.1.4.15 Terminate OCHTrail Service

Request

- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_ODU_Tunnel_Service/request.xml
- samples/Terminate_ODU_Tunnel_Service/request.json

Response

- samples/Terminate_ODU_Tunnel_Service/response.xml

1.41.1.4.16 Terminate ODU_UNI Service

Request

- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_ODU_UNI_Service/request.xml

Response

- samples/Terminate_ODU_UNI_Service/response.json

1.41.1.4.17 Terminate OPU Over ODU

Request

- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_OPU_Over_ODU/request.xml
- samples/Terminate_OPU_Over_ODU/request.json

Response

- samples/Terminate_OPU_Over_ODU/response.xml

1.41.1.4.18   Terminate ODU UNI Hairpin

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_ODU_UNI_Hairpin/request.xml

Response
- samples/Terminate_ODU_UNI_Hairpin/response.xml

1.41.1.4.19   Terminate ODU Service

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_ODU_Service/request.xml

Response
- samples/Terminate_ODU_Service/response.xml

1.41.1.4.20   Terminate Media Channel Group

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Media_Channel_Group/request.xml

Response
- samples/Terminate_Media_Channel_Group/response.xml

1.41.1.4.21   Terminate Media Channel NC

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Media_Channel_NC/request.xml

Response
- samples/Terminate_Media_Channel_NC/response.xml

1.41.1.4.22   Terminate Media Channel CC

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Media_Channel_CC/request.xml

Response
- samples/Terminate_Media_Channel_CC/response.xml

1.41.1.4.23   Terminate Media Channel Trail

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Media_Channel_Trail/request.xml

Response
- samples/Terminate_Media_Channel_Trail/response.xml

1.41.1.4.24   Terminate OCHTrail MP (Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Managed_Plane_OCH_Trail/request.xml

Response
- samples/Terminate_Managed_Plane_OCH_Trail/response.xml

1.41.1.4.25   Terminate OCHCC MP (Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Managed_Plane_OCH_CC/request.xml

Response
- samples/Terminate_Managed_Plane_OCH_CC/response.xml

1.41.1.4.26   Terminate OCHNC MP (Managed Plane)

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Managed_Plane_OCH_NC/request.xml

Response
- samples/Terminate_Managed_Plane_OCH_NC/response.xml

1.41.1.4.27   Terminate SR-TE service

Request
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_Sr-Te/request.xml

Response
- samples/Terminate_Sr-Te/response.xml

1.41.1.5   *Roll Service*

Operation	Description
Roll from one service to another service	Given local connect CEM service as roll-from-service and CEM service between 2 devices as roll-to-service, delete the CEM roll-from-service and modify CEM roll-to-service connect moving Z endpoint to roll-from-service Z endpoint.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-activation:roll-service

Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type modify-service-request that contains the details of the service type and order-data and other related data – see yang model for the data details.
Authorization Required	One or more from following • Circuit or VC Provisioning • Provisioning Access
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return a modify response of type **roll-service-response** that contains the details of the execution that includes service reference details, device cli details, etc. – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	• cisco-service-activation.yang

1.41.1.5.1 Roll Service Request

Name	Type	Description
modify-service-request	Container element	Holds the data for modifying an existing service.
cfs-ref	String (FDN)	FDN of the service to be modified.
ni-ref	String (FDN)	FDN of the Network Interface (UNI/ENNI) to be modified. This field is needed instead of cfs-ref in Network Interface (UNI/ENNI) modification case only.
service-order-data	service-order-data type	Container holding the service order data – see the order data sections for details on each service type data.

1.41.1.5.2 Roll Service Response

Name	Type	Description
modify-service-response	Container element	Holds the data for modify service response.
Refer Provision-service-response		

1.41.1.5.3 Roll Service Request/Response

Request
• samples/Roll_Service/request.xml

Response
• samples/Roll_Service/response.json

Notification
• samples/Roll_Service/notification.json

1.41.1.6 *Force Terminate Service*

Operation	Description
Terminate existing Service	This operation can be used to force terminate delete failed services. It's not applicable to optical services currently.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-activation:terminate-service
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **terminate-service-request** that contains the details of the service type and service reference and other related data – see yang model for the data details.
Authorization Required	One or more from following • Circuit or VC Provisioning • Provisioning Access
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return a provisioning response of type **terminate-service-response** that contains the details of the execution that includes service reference details, device cli details, etc. – see yang model for the data details.
HTTP Status Code	• 200 OK- Success with response message-body • 401, 403– Authentication and Authorization errors. • 400 Bad Request- Invalid request message. • 500 Internal Server Error- operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-activation.yang

1.41.1.6.1 Force Terminate Service Request

Name	Type	Mandatory	Description
terminate-service-request	Container element	Yes	Holds the data for terminating the service.
cfs-ref	String (FDN)	Yes	FDN of the service to be terminated.
service-name	String	No	Name of the service being deleted.
service-type	String	Yes	Service type of the service being deleted.
service-subtype	String	Yes	Service sub type of the service being deleted.
force-delete	Boolean	Yes	For force delete/terminate of a service value of this tag should be "true" or else EPNM will consider it as regular service terminate.

1.41.1.6.2 Force Terminate Service Response

Name	Type	Description
terminate-service-response	Container element	Holds the data for terminating the service's response.
Refer Provision-service-response		

CEM, Optical and MPLS-TE service provisioning is supported through the set of operations defined as RESTCONF Operations. When the OSS client uses this interface for service provisioning, a set of CFS (Customer Facing Service) and RFS (Resource Facing Service) objects will be created or modified to handle the service management in Cisco EPN Manager.

The API provides support for Termination of the following services:

Technology	Service Type	Service Sub Type

Technology	Service Type	Service Sub Type
CE	carrier-ethernet-vpn	EPL, EVPL, ACESS EPL, ACESS EVPL, EP-LAN, EVP-LAN, EP-Tree, EVP-Tree
CEM	tdm-cem	t1, t3, e1,e3,vt1.5,oc1,oc3, oc12,oc48 , STS-1 , STS-3c , STS-12c , STS-48c , VC4 , VC4-4c, VC4-16c , vc11 and vc12.
MPLS-TE	mpls-te-tunnel	bi-directional-te-tunnel, uni-directional-te-tunnel , layer3-link
L3VPN	mpls-l3-vpn	L3VPN

Force Terminate Sample Response:

- samples/Force_Terminate_Service/response.xml

1.41.1.7   *Save and Schedule service deployment (BETA VERSION)*

NBI supports service deployment which can be saved or scheduled to a specified time for all supported services except optical. This is applicable for provide, amend and terminate operations.

In order to schedule a service, NBI user needs to specify "deploy-schedule-time" tag along with "deploy-action" as "Scheduled" in the NBI input payload.

In order to save a service, "deploy-action" value should be specified as "Later" in NBI provide, amend or terminate payloads.

1.41.1.7.1 Save and Schedule service deployment for provide operation

1.41.1.7.1.1 Request

   deploy-action: Scheduled
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Save_Schedule_Services/Evpl-DeploySchedule-Provide-Request.xml
- samples/Save_Schedule_Services/EPTree-DeploySchedule-Provide-Request.xml

   deploy-action: Later
- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Save_Schedule_Services/Cem_vc11_provision_save_request.xml
- samples/Save_Schedule_Services/Mpls-te-tunnel_bi_directional_provide_save_request.xml

1.41.1.7.1.2 Response

deploy-action: Scheduled
- [samples/Save_Schedule_Services/Evpl-DeploySchedule-Provide-Response.xml](#)
- [samples/Save_Schedule_Services/EPTree-DeploySchedule-Provide-Response.xml](#)

deploy-action: Later
- [samples/Save_Deployment/Cem_vc11_provision_save_response.xml](#)
- [samples/Save_Deployment/Mpls-te-tunnel_bi_directional_provision_save_response.xml](#)

1.41.1.7.2 Save and Schedule service deployment for amend operation

1.41.1.7.2.1 Request

deploy-action: Scheduled
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- [samples/Save_Schedule_Services/Ce_EPTree_modify_schedule_request.xml](#)
- [samples/Save_Schedule_Services/Mpls-te-tunnel_uni_directional_modify_schedule_request.xml](#)

deploy-action: Later
- POST /restconf/operations/v1/cisco-service-activation:modify-service
- [samples/Save_Deployment/Ce_Epl_modify_save_request.xml](#)
- [samples/Save_Deployment/Ce_AccessEPL_modify_save_request.xml](#)

1.41.1.7.2.2 Response

deploy-action: Scheduled
- [samples/Schedule_Deployment/Ce_EPTree_modify_schedule_response.xml](#)
- [samples/Schedule_Deployment/ Mpls-te-tunnel_uni_directional_modify_schedule_response.xml](#)

deploy-action: Later
- [samples/Save_Deployment/Ce_Epl_modify_save_response.xml](#)
- [samples/Save_Deployment/Ce_AccessEPL_modify_save_response.xml](#)

1.41.1.7.3 Save and Schedule service deployment for terminate operation

1.41.1.7.3.1 Request

deploy-action: Scheduled
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Schedule_Deployment/Cem_t1_terminate_schedule_request.xml
- samples/Schedule_Deployment/L3vpn_terminate_schedule_request.xml

deploy-action: Later
- samples/Schedule_Deployment/Cem_t1_terminate_save_request.xml
- samples/Schedule_Deployment/L3vpn_terminate_save_request.xml

1.41.1.7.3.2 Response

deploy-action: Scheduled
- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Save_Deployment/L3vpn_terminate_schedule_response.xml
- samples/Save_Deployment/Cem_t1_terminate_schedule_response.xml

deploy-action: Later
- samples/Save_Deployment/L3vpn_terminate_save_response.xml
- samples/Save_Deployment/Cem_t1_terminate_save_response.xml

1.41.1.7.4 Manage Planned Services

NBI supports service re-deployment and cancel for the planned services.

In order to deploy a planned service, user needs to specify "action-type" tag as "Deploy" in the NBI input payload.

In order to cancel a planned service, user needs to specify "action-type" tag as "Cancel" in the NBI input payload.

Name	Type	Mandatory	Description
manage-planned-service-request	Container	Yes	Container to hold manage planned services request parameters.
service-order-data	Container	Yes	Container to hold the service order data tags
cfs-ref	String (FDN)	Yes, if its service	FDN of the service to be managed. Ex: MD=CISCO_EPNM!CFS=<serviceName>
ni-ref	String (FDN)	Yes, if its network-interface	FDN of the Network Interface (UNI/ENNI) to be managed. Ex: MD=CISCO_EPNM!NI=<niName>
service-name	String	No	Service name.

service-type	String	Yes	Service type.
service-subtype	String	Yes	Service subtype.
action-type	String	Yes	Possible values: • Deploy • Cancel

Note: This API (manage-planned-service) is supported for the following services mentioned in the below table.

Service Type	Service SubType
mpls-te-tunnel	• uni-directional-te-tunnel • bi-directional-te-tunnel • layer3-link.
carrier-ethernet-vpn	• EP-Tree • Access EPL • Access EVPL

1.41.1.7.4.1 Manage planned service (Deploy operation)

1.41.1.7.4.1.1 Request

POST /restconf/operations/v1/cisco-service-activation:manage-planned-service
• samples/Save_Deployment/Mpls-te-tunnel_bi_directional_redeploy_request.xml

1.41.1.7.4.1.2 Response

• samples/Save_Deployment/Mpls-te-tunnel_bi_directional_redeploy_response.xml

1.41.1.7.4.2 Manage planned service (Cancel operation)

1.41.1.7.4.2.1 Request

POST /restconf/operations/v1/cisco-service-activation:manage-planned-service
• samples/Save_Deployment/Mpls-te-tunnel_uni_directional_cancel_request.xml

1.41.1.7.4.2.2 Response
• samples/Save_Deployment/Mpls-te-tunnel_uni_directional_cancel_response.xml

Service Order Data

The following sub-sections provide the details of each service provisioning order data which is required in the provision and modify operations of the service activation interface as a POST data in a request object.

1.41.1.8 *Service Order Data – Carrier Ethernet (CE)*

The table below lists the Order Data elements and the supported values for carrier ethernet services. Note that the table below describes all the elements in service order data combined for service and endpoint configuration for all the CE services (ELINE, ELAN, ETREE, and EACCESS). See schema restconf-sai-carrier-ethernet.xsd for more details.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
service-name	String	Yes	No	All	Unique name to identify the circuit/VC.
service-description	String	No	Yes	All	Description of the VC that will help to identify the VC.
service-type	String	Yes	No	All	Service Type. Possible value: carrier-ethernet-vpn
service-subtype	String	Yes	No	All	Service SubType. Possible Values: EPL, EVPL, ACESS EPL, ACESS EVPL, EP-LAN, EVP-LAN, EP-Tree, EVP-Tree
customer-ref	String	No	No	All	Customer FDN. e.g., MD=CISCO_EPNM!CUSTOMER=<customer name> default value of CUSTOMER is "Infrastructure"
service-activate	Boolean	No	Yes	All	Activate Service. Default value is: true
deploy-action	String	No	No	All	This is the tag to specify deploy action in the payload. Default value : Deploy Possible Values : Preview , Deploy , Scheduled, Later
deploy-schedule-time	Date	No	No	All non-optical services	This tag is to specify deploy schedule time and applicable only when value of deploy action is "Scheduled". Supported format : yyyy-MM-ddThh:mm:ss-TZD e.g. 2018-10-25T09:10:00-00:00
signaling-protocol	String	Yes, for EVPN based service provisioning	No	EPL, EVPL	This is to specify if signaling protocol to be used. Supported value : bgp If its value is "bgp" then that means service need to use EVPN during provisioning.
termination-point-list	List container	Yes	N/A	All	List of connection termination point configurations.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
network-interface-list	List container	Yes	N/A	All	List of network interface configurations.
forwarding-path	container	Yes	N/A		List of Forward paths.
ce-data	container	Yes	N/A	All	Container for CE service configuration.
bundling	Boolean	yes	Yes	EVPL, EVP-LAN, EVP-TREE	Enables multiple VLANs on this VC. Multiple CE-VLAN IDs are bundled to one EVC. Default value: true
ccm-interval	String	Yes (when enable-cfm = true)	Yes		Service-wide setting for all Maintenance Entities – e.g. 1 sec, 1 min , 10 min , 10 sec, 100 ms , 3.33 ms. default value : 1 sec
ce-vlan-id-preservation	Boolean	Yes	Yes	EVPL, EVP-LAN, EVP-TREE	CE-VLAN ID Preservation. Ensures that the CE-VLAN ID of an egress service frame is identical in value to the CE-VLAN ID of the corresponding ingress service frame. This must be enabled, if bundling is enabled.
ce-vlan-cos-preservation	Boolean	No	Yes	EVPL, EVP-LAN, EVP-TREE	CE-VLAN ID CoS Preservation. Ensures that the CE-VLAN CoS of an egress service frame is identical in value to the CE-VLAN CoS of the corresponding ingress service frame. The CoS markings are unaltered.
mtu-size	Integer	Yes	Yes	All	Service MTU. The maximum size, in bytes, of any frame passing through the VC. Values can be between 64 and 9216. The service MTU must be lower than or equal to the MTU defined on the UNI.
enable-cfm	Boolean	No	Yes	All	True/false for enable CFM. Default is 'true'
cfm-domain-name	String	No	Yes	All	This represent CFM domain name used. Default : EVC
cfm-domain-level	String	No	Yes	All	This represents CFM domain level. Possible value : 1 to 7 Default : 4
configure-remote-mep	boolean	No	Yes	All	Flag to indicate for configuring remote mep or not. Default value : false.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
fault-management-map	FaultManagementMapType	No	N/A	All	Service OAM - Define the probe profiles between MEP Groups (groups of UNIs whose membership to a group is marked at each endpoint). See the entries in this container below in Fault Management Map Data.
max-uni-endpoints	Integer	No	No	All	Max UNI endpoints , default: 2
vpn-id	Long	No	No	All	Vpn Id
auto-allocate-vlan-id	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Indicator for auto allocation of VLAN Id, allowed values:true/false; Default value: false

The table below lists the containers for Fault Management map entries applicable to different types of fault management maps:

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
fault-management-map	Container element	Yes	N/A	All	Container for Fault Management Map Entries.
Entry	Container element for entries	Yes	N/A	All	Zero or more elements of the Fault Management Map Entry.
Fault Management Map Entry Data		Yes	N/A	All	Container of the entries for Fault Management Map.
from	String	Yes	Yes	All	Value should be one of - ENNI Z, UNI Z, UNI A, or ENNI A. The source of the traffic flow across the EVC/OVC.
to	String	Yes	Yes	All	Value should be one of - ENNI Z, UNI Z, UNI A, or ENNI A. The destination of the traffic flow across the EVC/OVC.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
cos	String	Yes	Yes	All	Values: • EXTRA HIGH • HIGH • HIGHEST AVAILABLE • LOW • MEDIUM The Class of Service identifier that should be associated with the frame.
oam-profile	String	Yes	Yes	All	Provide a name to the profile that can be identified for the set of OAM attributes that should be applied to the frame to enable performance monitoring. **Note:** This is just a label. The actual values should be passed through CChk, SEDM, DEDM, and SyLM elements mentioned below. For example: – Performance Monitoring 1: Enables continuity check and synthetic loss measurement. (CChk=Yes, SEDM= No, DEDM=No, SyLM=Yes, SLM=No). – Performance Monitoring 2: Enables continuity check, synthetic loss measurement, and single-ended delay measurement (CChk=Yes, SEDM= Yes, DEDM=No, SyLM=Yes, SLM=No). – Performance Monitoring 3: Enables continuity check, synthetic loss measurement, and dual-ended delay measurement (CChk=Yes, SEDM= No, DEDM=Yes, SyLM=Yes, SLM=No).

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
termination-point-list	Container	Yes	N/A	All	termination point list
termination-point-config	Container	Yes	N/A	All except UNI , QoS Profile	termination point config
tp-ref	String (FDN)	Yes	No	All	FDN of the port to use - set of RNDs that consists of MD, ME and PTP or FTP instance ids. For example: "MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-2.cisco.com!FTP=name=GigabitEthernet t0/4;lr=lr-gigabit-ethernet "
directionality	Identity	Yes	No	All	source, sink, and bi-directional.
ingress-qos-policy-ref	String (FDN)	No	Yes	All except EVP-Tree	Ingress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=TestQosProfile
egress-qos-policy-ref	String (FDN)	No	Yes	All except EVP-Tree	Egress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=TestQosProfile
network-interface-name	String	Yes (for new UNI)	No	All	It's the name of the new NI being created Mandatory while creating new UNI e.g., any unique uni name like UniA , UniZ etc.
network-interface-ref	String (FDN)	Yes (for existing UNI)	No	All	It's the FDN of the existing NI being re-used. Mandatory while re-using existing UNI e.g., MD=CISCO_EPNM!NI=<name of the existing UNI>
ce-data	Container	Yes	N/A	All	Container for CE Endpoint configuration

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
l2-cp-profile	String	No	Yes	All except EVPL	Layer 2 Control Protocol Profile. Profile that determines how the various communication protocols are handled. Frames using the various protocols are tunneled, dropped, or peered. Refer to MEF 6.1 for details. Values: EPL, Access EPL: MEF Option1 or MEF Option2 Access EVPL: EVPL/EVP-LAN/EVP-Tree EP-LAN, EP-Tree: MEF EP-LAN/EP-Tree EVP-LAN, EVP-Tree: MEF EVPL/EVP-LAN/EVP-Tree
untagged	Boolean	No	Yes	EVPL, EVP-LAN, EVP-TREE	Untagged – true/false. Preserves a VLAN ID for untagged traffic. If there is no bundling, only one VLAN is allowed, therefore, if the Untagged check box is selected, you cannot specify an additional VLAN ID.
mep-group	String	No	Yes	E-LAN	Name of the Mep Group – UNI A or UNI Z. For CFM configuration, specify the group to which this endpoint belongs. Based on your selection, a CFM service will be created and a MEP ID will be assigned.
service-vlan-list	String	No	Yes	Access EPL, EVPL	Service VLAN Id.
qinq-data	Container	Yes	N/A	EVPL, Access EVPL, EVP-LAN	QinQ Configuration

The table below describes the different endpoint data types and lists the services, they are applicable to:

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
network-interface-list	Container	Yes	N/A	All	Network Interface config list
network-interface	Container	Yes	N/A	All	Network Interface config.
operation	Enum	No	N/A	All	add, update, and remove.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
ref	String (FDN)	No	No	All	FDN of the existing NI – set of RDNs that consists of MD and NI. Mandatory for Modify operation e.g., MD=CISCO_EPNM!NI=<name of the existing uni>
name	String	No	No	All	Name of the new NI to be created. Mandatory while creating new UNI e.g., name of the new uni like UniA , UniZ etc.
ce-data	Container	Yes	N/A		Container for CE Network Interface configuration.
description	String	No	Yes	All	Description of the new NI to be created.
activate	Boolean	Yes	Yes	All	true/false for Activate NI. Default =true
designation	String	No	No	E-TREE	Possible Values: Root or Leaf.
use-p2-p-connection-with-root	Boolean	No	Yes		Possible Values: true , false
ingress-qos-policy-ref	String (FDN)	No	No	All except EVP-Tree	Ingress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=TestQosProfile
egress-qos-policy-ref	String (FDN)	No	No	All except EVP-Tree	Egress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=TestQosProfile
mtu	Integer	Yes	No	All	The maximum transmission size, in bytes, of a packet passing through the interface. The MTU of the UNI must be greater than or equal to the MTU defined on the service level. MTU Value should be between 64 and 9216 Default value: 1522
auto-negotiation	boolean	No	Yes	All	This is a flag to indicate of auto-negotiation. Possible values : false/true Default value : false

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
speed	String	No	No	All	Port speed. You can reduce the speed if this is supported on the port. The port speed provided has to be equal to or smaller than the speed of the port selected.
mode	String	Yes	No	All	Mode – values: • FULL DUPLEX—Uses simultaneous communication in both directions between the UNI and the customer's access switch, assuming that both sides support full duplex. If one side does not support full duplex, the port will be brought down. • AUTO NEGOTIATION —Uses the mode that is agreed upon between the two devices, depending on what is supported. Full Duplex will be attempted but if one device does not support it, half duplex will be used. Default value: FULL DUPLEX
enable-link-management	Boolean	No	Yes	All	Enable/disable IEEE 803.1ah Link Management (E-LMI) Enables the customer access switch to get information about this UNI, VLAN IDs, and services on the UNI, and so on. Default value: false
enable-link-oam	Boolean	No	No	All	Enables IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch. Default value: false **NOTE**: For **LAG** Ports this parameter should be set to false.
ce-vlan-id	String	No	No	EVPL, EVP-LAN, EVP-TREE	Untagged CE-VLAN ID – e.g. 1333. The ID of the CE-VLAN assigned to untagged traffic.
service-multiplexing	Boolean	No	No	EVPL, EVP-LAN, EVP-TREE	Allows multiple services to be provisioned on this UNI. Default value: true
bundling	Boolean	No	Yes	EVPL, EVP-LAN, EVP-TREE	UNI Allows Bundling. Allows the use of multiple VLANs for this UNI. Default value: false
designation	String	No	No	EP-TREE, EVP-TREE	Designation. Select the role of the UNI in the VC. Values: Root or Leaf.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
operator-ref	String (FDN)	No	No	Access EPL, Access EVPL	FDN of the customer object – set of RDN types with MD, CUSTOMER.
protection-mechanism	String	No	No	Access EPL, Access EVPL	Protection Mechanism. Specify a protection mechanism if ENNI comprises of more than one port. Values: None, Link Aggregation, and other.
frame-format	String	No	No	Access EPL, Access EVPL	Frame Format Values: Double Tagged.
all-to-one-bundling	Boolean	No	No		true or false.

The table below describes the match and advanced criteria for the QinQ Configuration (applicable to only EVPL, Access EVPL, and EVP-LAN):

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
qinq-data	Container	Yes	N/A	EVPL, Access EVPL, EVP-LAN, EVP-Tree	QinQ Configuration
match-type	MatchTypeEnumType	Yes	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Possible Values: default, dot1q, dot1ad, and untagged.
vlan-id-list	String	Yes	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Outer VLANs. The VLAN or range of VLANs to be used for this service, e.g. 12 or 123-145, 155.
inner-vlan-id-list	String	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Inner VLANs The VLAN or range of VLANs to be used, e.g. 12 or 123-145, 155.
untagged	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Allow the service frames to be untagged (one service allowed per UNI). Default value: false
priority-tagged	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Mentions priority tagged or not Default value: false

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
qinq-data	Container	Yes	N/A	EVPL, Access EVPL, EVP-LAN, EVP-Tree	QinQ Configuration
match-exact	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Mentions do exact match or not Default value: false
vlan-cos	String	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Outer VLAN CoS e.g., any string value
inner-vlan-cos	String	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Inner VLAN CoS e.g., any string value
ether-type	EtherType	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Container for EtherType options that holds following elements: ipv4, ipv6, pppoeAll, pppoeDiscovery, and pppoeSession.
ipv4	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Ethertype - ipv4 Default value = false
ipv6	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Ethertype -ipv6 Default value = false
pppoe-all	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Ethertype -pppoeAll Default value = false
pppoe-discovery	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Ethertype -pppoeDiscovery Default value = false
pppoe-session	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Ethertype - pppoeSession Default value = false
rewrite-definition	rewrite-definition-type	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Container element for Rewrite Definition (Advanced Frame Manipulation). Contains the following elements: pop-operation, push-operation, translate-operation and none.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
qinq-data	Container	Yes	N/A	EVPL, Access EVPL, EVP-LAN, EVP-Tree	QinQ Configuration
pop-operation	Container	No	N/A	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Pop action configuration container element.
push-operation	Container	No	N/A	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Push action configuration container element.
translate-operation	translate-operation-type	No	N/A	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Translate action configuration container element.
tag-count	tag-count-enum-type	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Values: one and two. Child element of pop-operation and push-operation.
tag-translation	Tag-translation-enum-type	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Values: one-to-one, one-to-two, two-to-one, two-to-two Child element of translate-operation.
match-type	match-type-enum-type	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Values: dot1q and dot1ad. Child element of push-operation, translate-operation.
inner-vlan-id	String	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	VLAN ID Child element of push-operation, translate-operation.
outer-vlan-id	String	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	VLAN ID Child element of push-operation, translate-operation.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
forwarding-path	Container element	Yes	N/A	EPL/EVPL over tunnel	Container for Forwarded Path entries.
pseudowire-settings	Container element for entries	No	N/A	EPL, EVPL	Container for Pseudowire Settings.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
preferred-path-ref	String (FDN)	No	Yes	EPL, EVPL	Preferred Path reference for bi-directional-tunnel. e.g., MD=CISCO_EPNM!VC=<existing path name> where "existing path name" could be any value like "TE Link 301_6.6.6.6_0"
src-dest-preferred-path-ref	String (FDN)	Yes (for uni-directional tunnel)	Yes	EPL, EVPL	Preferred Path reference from source to detination e.g., MD=CISCO_EPNM!VC=<existing path name> where "existing path name" could be any value like "TE Link 301_6.6.6.6_0"
dest-src-preferred-path-ref	String (FDN)	Yes (for uni-directional tunnel)	Yes	EPL, EVPL	Preferred Path reference from destination to source e.g., MD=CISCO_EPNM!VC=<existing path name> where "existing path name" could be any value like "TE Link 301_6.6.6.6_0"
enable-control-word	Boolean	No	Yes	EPL, EVPL	Enable Control Word Default value = true
fallback-to-ldp	Boolean	No	Yes	EPL, EVPL	Fallback to LDP Default value = false
interworking-option	String	No	Yes	EPL, EVPL	Interworking Option
service-bandwidth	Long	No	Yes	EPL	Service bandwidth
pw-bandwidth	String	No	Yes	EPL	Pseudowire bandwidth
mpls-te-data	Container element for mpls te data	No	N/A	EPL, EVPL	Container for MPLS TE See schema restconf-sai-mpls-te.xsd for more details.
te-tunnel-type	String	No	No	EPL, EVPL	Tunnel Type: values – uni-directional, bi-directional For EPL, default value is bi-directional For EVPL, default value is uni-directional
enable-fault-oam	Boolean	No	Yes	EPL, EVPL	Enable fault OAM True/False, Default is True
enable-autoroute	Boolean	No	Yes	EPL, EVPL	This attribute specifies whether to enable autoroute option Default value: false

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
enable-frr	Boolean	No	Yes	EVPL	Enable Fast Re-route. Applicable for uni-directional tunnel only
enable-auto-bandwidth	Boolean	No	Yes	EVPL	Enable Auto Bandwidth. Applicable for uni-directional tunnel only Default value : true
enable-lockdown	Boolean	No	Yes	EVPL	This attribute specifies whether to enable lockdown option
protection-type	Enum	Yes	Yes	EVPL	This attributes specifies protection type and allowed values are: Working, Protected, Working+Protected, Working+Restore, Working+Protected+Restore
tunnel-setting	Container	Yes	N/A	EPL, EVPL	Container for tunnel settings.
affinity-bits	String (Range: 0x0-0xFFFFFFFF, Default: 0x0)	No	Yes	EPL, EVPL	Affinity Value
affinity-mask	String (Range: 0x0-0xFFFFFFFF, Default: 0x0)	No	Yes	EPL, EVPL	Affinity mask on desired link attributes.
bfd-settings	Container	No	N/A	EPL, EVPL	Container for bfd settings.
enable	Boolean	Yes	No	EPL, EVPL	Enable bfd.
is-new-bfd-template	Boolean	No	No	MPLS TE tunnels	This flag indicates if bfd-template is new or existing. Default value : false Possible values : true/false
bfd-template	String	Yes	No	MPLSTE tunnels	BFD Template name
min-interval	integer(Range: 15 to 200 Default: 100)	Yes	Yes	EPL, EVPL	The minimum control packet interval for BFD sessions in milliseconds.
multiplier	integer (default 3)	Yes	Yes	EPL, EVPL	Number of times a packet is missed before BFD declares the session down.
evpn-settings	Container	No	Yes	EPL, EVPL	Container for EVPN settings related inputs
bgp-settings	Container	No	Yes	EPL, EVPL	Container for EVPN bgp settings related attributes
is-auto-route-distinguisher	Boolean	Yes	Yes	EPL, EVPL	Boolean flag to indicate if auto RD need to be enabled or not. Default: true

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
`route-distinguisher`	String	Yes when `is-auto-route-distinguisher = false`	Yes	EPL , EVPL	Route distinguisher value Allowed format: "Num:Num" or "IPAddr:Num" .
`is-auto-route-target`	Boolean	Yes	Yes	EPL, EVPL	Boolean flag to indicate auto RT need to be enabled or not. Default: true
`import-route-target`	String	Yes when `is-auto-route-target = false`	Yes	EPL , EVPL	Import route target value Allowed format: "Num:Num" or "IPAddr:Num" .
`export-route-target`	String	Yes when `is-auto-route-target = false`	Yes	EPL , EVPL	Export route target value Allowed format: "Num:Num" or "IPAddr:Num" .
`vpws-settings`	Container	No	Yes	EPL , EVPL	Container for EVPN service settings related tags
`evpn-instance-id`	String	No	Yes	EVP , EVPL	Ethernet VPN Id Allowed range: 1-65534
`aend-attachment-circuit-id`	String	No	Yes	EPL , EVPL	A END attachment circuit ID Allowed range: 1-16777215
`zend-attachment-circuit-id`	String	No	Yes	EPL , EVPL	Z END attachment circuit ID Allowed range: 1-16777215
`enable-static-preferred-path`	Boolean	No	Yes	EPL , EVPL	Flag to indicate if user want to enable static preferred path or not. Default value: false
`enable-control-word`	Boolean	No	Yes	EPL , EVPL	Enable Control Word Default value = true

The table below lists the containers for Y1731 test config entries applicable to different types of CE services.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
y1731-test-config	Container	No	N/A	EPL, EVPL	Container for y1731 test data. Refer section 4.23.4.1.3 for details
y1731-result-list	Container	No	N/A	EPL,EVPL	Container for Y1731 result list
y1731-result-row	Container	No	N/A	EPL,EVPL	Container for Y1731 result row

service-ref	String	No	Yes	EPL,EVPL	service reference (fdn) for this test results. e.g., MD=CISCO_EPNM!CFS=CemLink#Con_26 551659
source-tp-ref	String	No	Yes	EPL,EVPL	source tp reference (fdn) e.g., MD=CISCO_EPNM!ND=SJ-NCS4216-23.CISCO!PTP=name=T1 0/5/21;lr=lr-t1
destination-tp-ref	String	No	Yes	EPL,EVPL	destination tp reference (fdn) e.g., MD=CISCO_EPNM!ND=SJ-NCS4206-21.CISCO!PTP=name=T1 0/3/21;lr=lr-t1
delay-result	**Container**	**No**	**Yes**	**EPL,EVPL**	**Container for delay result**
Availability	Int	No	Yes	EPL,EVPL	Availability
Status	String	No	Yes	EPL,EVPL	Status
two-way-delay	String	No	Yes	EPL,EVPL	Two Way Delay
two-way-delay-unit	String	No	Yes	EPL,EVPL	Two Way Delay Unit
two-way-jitter	String	No	Yes	EPL,EVPL	Two Way Jitter
two-way-jitter-unit	String	No	Yes	EPL,EVPL	Two Way Jitter Unit
loss-result	**Container**	**No**	**N/A**	**EPL,EVPL**	**Container for loss result**
Availability	Int	No	Yes	EPL,EVPL	Availability
backward-fLR	String	No	Yes	EPL,EVPL	Backward FLR
forward-fLR	String	No	Yes	EPL,EVPL	Forward FLR
Status	String	No	Yes	EPL,EVPL	Status
y1564-test-config	**Container**	**No**	**N/A**	**EPL, EVPL**	**Container for y1564 test data. Refer section 4.23.4.1.2 for details**
y1564-result	**Container**	**No**	**N/A**	**EPL,EVPL**	**Container of the Y1564 result**
service-ref	String	No	Yes	EPL,EVPL	service reference (fdn) for this test results. e.g., MD=CISCO_EPNM!CFS=CemLink#Con_26 551659
source-tp-ref	String	No	Yes	EPL,EVPL	source tp reference (fdn) e.g., MD=CISCO_EPNM!ND=SJ-NCS4216-23.CISCO!PTP=name=T1 0/5/21;lr=lr-t1
destination-tp-ref	String	No	Yes	EPL,EVPL	destination tp reference (fdn) e.g., MD=CISCO_EPNM!ND=SJ-NCS4206-21.CISCO!PTP=name=T1 0/3/21;lr=lr-t1
source-device-name	String	No	Yes	EPL,EVPL	Source Device Name
destination-device-name	String	No	Yes	EPL,EVPL	Destination Device Name
source-eFP	Int	No	Yes	EPL,EVPL	Source EFP

destination-eFP	Int	No	Yes	EPL,EVPL	Destination EFP
Duration	String	No	Yes	EPL,EVPL	test duration
Timestamp	String	No	Yes	EPL,EVPL	Timestamp
Steps	String	No	Yes	EPL,EVPL	Steps
throughput	String	No	Yes	EPL,EVPL	Throughput
y1564-result-row-list	**Container**	**No**	**N/A**	**EPL,EVPL**	**Container for Y1564 Result Row List**
y1564-result-row	**Container**	**No**	**N/A**	**EPL,EVPL**	**Container for Y1564 Result Row**
Availability	String	No	Yes	EPL,EVPL	Availability
bytes-received	String	No	Yes	EPL,EVPL	bytes received
bytes-transmitted	String	No	Yes	EPL,EVPL	bytes transmitted
packets-size	String	No	Yes	EPL,EVPL	packet size
packets-received	String	No	Yes	EPL,EVPL	packets received
packets-transmitted	String	No	Yes	EPL,EVPL	packets transmitted
Duration	String	No	Yes	EPL,EVPL	test duration
frame-loss	String	No	Yes	EPL,EVPL	frame loss
frame-loss-rate	String	No	Yes	EPL,EVPL	frame-loss-rate
configured-rate	Int	No	Yes	EPL,EVPL	configured-rate
actual-rate	Int	No	Yes	EPL,EVPL	actual rate
Range	String	No	Yes	EPL,EVPL	Range
Step	Int	No	Yes	EPL,EVPL	Step

1.41.1.9   *Service Order Data – CEM*

See schema restconf-sai-cem.xsd for more details.

CEM Service Order Data	Data Type	Mandatory	Modifiable	Description
service-type	String (CEM)	Yes	No	The type of service.
service-subtype	String	Yes	No	Service subtypes Supported values. t1,t3,e1,e3,vt1.5,STS-1, STS-3c,STS-12c, STS-48c,VC4,VC4-4c, VC4-16c,VC11, VC12, DS0
service-template	String	No	Yes	The template to be associated with the service.
customer-ref	FDN	No	No	Customer FDN
service-name	String	Yes	No	A unique name for the service.
service-	String	No	Yes	A unique description about the service.

description				
service-activate	Boolean	No	Yes	Turn service on/off.
frame-type	Enum	No	No	CEM Framing Type. Possible values : CEP, SATOP, FRAMED_SATOP CESoPSN. • For DS0 service – supported frame-type is CESoPSN. • For T1 , T3 & E1 service – supported frame-types are SATOP, FRAMED_SATOP. • For E3 service – supported frame-types are SATOP, FRAMED_SATOP & CEP. • For STS-1 , STS-3c , STS-12c, STS-48c , vt1.5 , VC11 & VC12 – supported frame-type is CEP. • For VC4 , VC4-4c & VC4-16c – supported frame-types is CEP.
payload-size	Integer (Range; 92-960)	No	Yes	The number of bytes in the payload of each packet.
dejitter-buffer-size	Integer (Range: 1 - 32)	No	Yes	The size of the buffer, in milliseconds.
idle-pattern-length	Integer	No	Yes	
idle-pattern	String (Range: 0x0 to 0xFF, Default: 0xFF)	No	Yes	The idle pattern option specifies the idle pattern to transmit when the circuit goes down.
dummy-mode	Enum (last-frame, user-defined)	No	Yes	Dummy mode enables a bit pattern for filling in for lost or corrupted frames.
dummy-pattern	String (Range: 0x0 to 0xFF, Default: 0xFF)	No	Yes	User Define Dummy Pattern
rtp-header-enabled	Boolean	No	Yes	Enable RTP Header.
rtp-header-compression-enabled	Boolean	No	Yes	Enable RTP Compression.
termination-point-list	Container	Yes	N/A	termination point list
termination-point-config	Container	Yes	N/A	termination point config
tp-ref	String (FDN)	Yes	No	port reference FDN for working path controller.
ingress-qos-policy-ref	String (FDN)	No	Yes	QoS policy FDN for ingress policy in FDN format e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=TestQosProfile
egress-qos-policy-ref	String (FDN)	No	Yes	QoS policy FDN for egress policy in FDN format. e.g.,

				MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=TestQosProfile
is-hop-or-lop-changed	Boolean	No	No	Applicable for Z end HOP/LOP change during service modify. This need to be specified in modify payload when there is any change in HOP or LOP value being done.
working-path	PathType	Yes	No	Working path
protecting-path	PathType	No	No	Protection path
clock-source	String (Line, Internal)	No	Yes	Clock Source
recovered-clock	String (Adaptive Clock Recovery, Differential Clock Recovery)	No	Yes	Recovered Clock
higher-order-path				
available-path-ref	String	Yes	No	High Order Path reference FDN.
available-paths	String	Yes	No	Higer order available paths values **For VC4:** AU-4 1, AU-4 2,…,AU-4 48 **For VC4-4c:** AU-4 1-4, AU-4 5-8,…,AU-4 45-48 **For VC4-16c :** AU-4 1-16,…,AU-4 33-48 **For E1, T1, E3 , T3 , DS0, VC11 and VC12 :** AU-4 1, TUG-3 1, AU-4 1, TUG-3 2, AU-4 1, TUG-3 3, AU-4 2, TUG-3 1, AU-4 2, TUG-3 2, AU-4 2, TUG-3 3, AU-4 3, TUG-3 1, AU-4 3, TUG-3 2, AU-4 3, TUG-3 3, AU-4 4, TUG-3 1, AU-4 4, TUG-3 2, AU-4 4, TUG-3 3, AU-4 5, TUG-3 1, AU-4 5, TUG-3 2, AU-4 5, TUG-3 3 AU-4 6, TUG-3 1, AU-4 6, TUG-3 2, AU-4 6, TUG-3 3, AU-4 7, TUG-3 1, AU-4 7, TUG-3 2, AU-4 7, TUG-3 3, AU-4 8, TUG-3 1, AU-4 8, TUG-3 2, AU-4 8, TUG-3 3, AU-4 9, TUG-3 1, AU-4 9, TUG-3 2,

				AU-4 9, TUG-3 3,
				AU-4 10, TUG-3 1,
				AU-4 10, TUG-3 2,
				AU-4 10, TUG-3 3,
				AU-4 11, TUG-3 1,
				AU-4 11, TUG-3 2,
				AU-4 11, TUG-3 3,
				AU-4 12, TUG-3 1,
				AU-4 12, TUG-3 2,
				AU-4 12, TUG-3 3,
				AU-4 13, TUG-3 1,
				AU-4 13, TUG-3 2,
				AU-4 13, TUG-3 3,
				AU-4 14, TUG-3 1,
				AU-4 14, TUG-3 2,
				AU-4 14, TUG-3 3,
				AU-4 15, TUG-3 1,
				AU-4 15, TUG-3 2,
				AU-4 15, TUG-3 3,
				AU-4 16, TUG-3 1,
				AU-4 16, TUG-3 2,
				AU-4 16, TUG-3 3,
				AU-3 1,
				AU-3 10,
				AU-3 11,
				AU-3 12,
				AU-3 13,
				AU-3 14,
				AU-3 15,
				AU-3 16,
				AU-3 17,
				AU-3 18,
				AU-3 19,
				AU-3 2,
				AU-3 20,
				AU-3 21,
				AU-3 22,
				AU-3 23,
				AU-3 24,
				AU-3 25,
				AU-3 26,
				AU-3 27,
				AU-3 28,
				AU-3 29,
				AU-3 3,
				AU-3 30,
				AU-3 31,
				AU-3 32,
				AU-3 33,
				AU-3 34,
				AU-3 35,
				AU-3 36,

				AU-3 37, AU-3 38, AU-3 39, AU-3 4, AU-3 40, AU-3 41, AU-3 42, AU-3 43, AU-3 44, AU-3 45, AU-3 46, AU-3 47, AU-3 48, AU-3 5, AU-3 6, AU-3 7, AU-3 8, AU-3 9
path-mode	String	Yes	No	Mode of the path used Allowed values: STS-1, STS-3c, STS-12c, STS-48c, T3,E3, VT15, T1, E1, CT3, CT3_E1, VC11_T1, VC12_E1, UNFRAMED. **VC4 over SDH controllers :** VC4 **VC4-4c over SDH controllers :** VC4-4c **VC4-16c over SDH controllers :** VC4-16c **DS0 over SDH controllers :** VC12-E1 **T1 over SDH controllers :** VC11-T1 **E1 over SDH controllers :** VC12-E1 **T3 over SDH controllers :** T3 **E3 over SDH controllers :** E3 **VC11 and VC12 over SDH controllers :** VC1X
lower-order-path	String			Low Order Path
available-path-ref	String	No	No	Low Order Path reference **DS0 over SDH controllers:** TUG-2 1, E1 1 TUG-2 1, E1 2 TUG-2 1, E1 3 TUG-2 2, E1 1 TUG-2 2, E1 2 TUG-2 2, E1 3 TUG-2 3, E1 1 TUG-2 3, E1 2 TUG-2 3, E1 3 TUG-2 4, E1 1 TUG-2 4, E1 2 TUG-2 4, E1 3 TUG-2 5, E1 1 TUG-2 5, E1 2 TUG-2 5, E1 3

				TUG-2 6, E1 1
				TUG-2 6, E1 2
				TUG-2 6, E1 3
				TUG-2 7, E1 1
				TUG-2 7, E1 2
				TUG-2 7, E1 3
				E1 over SDH controllers :
				TUG-2 1, E1 1
				TUG-2 1, E1 2
				TUG-2 1, E1 3
				TUG-2 1, E1 4
				TUG-2 2, E1 1
				TUG-2 2, E1 2
				TUG-2 2, E1 3
				TUG-2 2, E1 4
				TUG-2 3, E1 1
				TUG-2 3, E1 2
				TUG-2 3, E1 3
				TUG-2 3, E1 4
				TUG-2 4, E1 1
				TUG-2 4, E1 2
				TUG-2 4, E1 3
				TUG-2 4, E1 4
				TUG-2 5, E1 1
				TUG-2 5, E1 2
				TUG-2 5, E1 3
				TUG-2 5, E1 4
				TUG-2 6, E1 1
				TUG-2 6, E1 2
				TUG-2 6, E1 3
				TUG-2 6, E1 4
				TUG-2 7, E1 1
				TUG-2 7, E1 2
				TUG-2 7, E1 3
				TUG-2 7, E1 4
				VC11 and VC 12 over SDH controllers :
				TUG-2 1, VC 1
				TUG-2 1, VC 2
				TUG-2 1, VC 3
				TUG-2 1, VC 4
				TUG-2 2, VC 1
				TUG-2 2, VC 2
				TUG-2 2, VC 3
				TUG-2 2, VC 4
				TUG-2 3, VC 1
				TUG-2 3, VC 2
				TUG-2 3, VC 3
				TUG-2 3, VC 4
				TUG-2 4, VC 1
				TUG-2 4, VC 2

				TUG-2 4, VC 3
				TUG-2 4, VC 4
				TUG-2 5, VC 1
				TUG-2 5, VC 2
				TUG-2 5, VC 3
				TUG-2 5, VC 4
				TUG-2 6, VC 1
				TUG-2 6, VC 2
				TUG-2 6, VC 3
				TUG-2 6, VC 4
				TUG-2 7, VC 1
				TUG-2 7, VC 2
				TUG-2 7, VC 3
				TUG-2 7, VC 4
				VT1.5 over SDH controllers :
				VTG 1, T1 2
				VTG 1, T1 3
				VTG 1, T1 4
				VTG 2, T1 1
				VTG 2, T1 2
				VTG 2, T1 3
				VTG 2, T1 4
				VTG 3, T1 1
				VTG 3, T1 2
				VTG 3, T1 3
				VTG 3, T1 4
				VTG 4, T1 1
				VTG 4, T1 2
				VTG 4, T1 3
				VTG 4, T1 4
				VTG 5, T1 1
				VTG 5, T1 2
				VTG 5, T1 3
				VTG 5, T1 4
				VTG 6, T1 1
				VTG 6, T1 2
				VTG 6, T1 3
				VTG 6, T1 4
				VTG 7, T1 1
				VTG 7, T1 2
				VTG 7, T1 3
				VTG 7, T1 4
				CT3 over SDH controllers :
				T1 1
				T1 10
				T1 11
				T1 12
				T1 13
				T1 14
				T1 15

				T1 16
				T1 17
				T1 18
				T1 19
				T1 2
				T1 20
				T1 21
				T1 22
				T1 23
				T1 24
				T1 25
				T1 26
				T1 27
				T1 28
				T1 3
				T1 4
				T1 5
				T1 6
				T1 7
				T1 8
				T1 9
ds0-time-slots	String	No	No	Comma separated ds0 time slot numbers.
forwarding-path	Container element	Yes	N/A	Container for Forwarded Path entries.
pseudowire-settings	Container element for entries	No	N/A	Container for Pseudowire Settings.
preferred-path-ref	String (FDN)	Yes	Yes	Preferred Path reference, FDN of Bi-directional tunnel e.g., MD=CISCO_EPNM!VC=<existing path name> where "existing path name" could be any value like "TE Link 301_6.6.6.6_0"
enable-control-word	Boolean	No	Yes	Enable Control Word Default value = true
fallback-to-ldp	Boolean	No	Yes	Fallback to LDP Default value = false
interworking-option	String	No	Yes	Interworking Option Default value = could be left blank
service-bandwidth	Long	No	Yes	Interworking Option
pw-bandwidth	String	No	Yes	Service bandwidth

enable-static-preferred-path	Boolean	No	Yes	Flag to indicate if user want to enable static preferred path or not. Default value : false
mpls-te-data	Container	No	N/A	Container for MPLS TE See schema restconf-sai-mpls-te.xsd for more details.
te-tunnel-type	String	No	No	Tunnel Type: values – uni-directional, bi-directional For CEM. Default value: bi-directional
enable-fault-oam	Boolean	No	Yes	Enable fault OAM true/false. Defaut value: true
enable-frr	Boolean	No	Yes	Enable Fast Re-route. Applicable for uni-directional tunnel only Default value: false
enable-auto-bandwidth	Boolean	No	Yes	Enable Auto Bandwidth. Applicable for uni-directional tunnel only Default value: false
enable-autoroute	Boolean	No	Yes	This attribute specifies whether to enable autoroute option Default value: false
enable-lockdown	Boolean	No	Yes	This attribute specifies whether to enable lockdown option Default value: false
protection-type	Enum	No	Yes	This attributes specifies protection type and allowed values are: Working , Working+Protected, Working+Restore, Working+Protected+Restore Default value: Working
bfd-settings	Container	No	N/A	Container for bfd settings.
enable	Boolean	Yes	No	Enable BFD Default value: true
min-interval	integer	Yes	Yes	The minimum control packet interval for BFD sessions in milliseconds. Range: 15 to 200 Default value: 100
multiplier	integer	Yes	Yes	Number of times a packet is missed before BFD declares the session down. Range: 3 to 50 Default value: 3

The table below lists the containers for BERT config entries applicable to different types of CEM services.

CEM Service Order Data	Data Type	Mandatory	Modifiable	Description
bert-config	Container	No	N/A	Container for bert config. Refer section

				4.23.4.1.1 for details
bert-result-list	Container	No	N/A	Container of the BERT Result List
bert-result	Container	No	N/A	Container of the BERT result
service-ref	String	No	N/A	FDN of the customer facing service
source-tp-ref	String	No	N/A	FDN of the source port. If not specified, takes source end tp-ref of the provisioning order data e.g. , MD=CISCO_EPNM!ND=SJ-NCS4216-23.CISCO!PTP=name=T1 0/5/21;lr=lr-t1
destination-tp-ref	String	No	N/A	FDN of the destination port. If not specified, takes sink end tp-ref in the provisioning order data. e.g., MD=CISCO_EPNM!ND=SJ-NCS4206-21.CISCO!PTP=name=T1 0/3/21;lr=lr-t1
unmanaged-destination	Boolean	No	Yes	"true" if destination is unmanaged. default "false"
direction	Enum (system,line)	No	Yes	Test direction
errors	Int	No	Yes	error count
duration	Int (minutes)	No	Yes	Duration in minutes
pattern	String	No	Yes	bert patterns. valid values: 0s, 1s, 2^11, 2^15, 2^20-O153, 2^20-QRSS, 2^23, alt-0-1

1.41.1.10 *Service Order Data – UNI*

The table below lists the Order Data elements and the supported values for UNI. Note that the table below describes all the elements in service order data combined for service and endpoint configuration for UNI. See schema restconf-sai-common.xsd for more details.

UNI Service Order Data	Data Type	Mandatory	Modifiable	Description
service-name	String	Yes	No	Unique name to identify the circuit/VC.
service-description	String	No	Yes	Description of the VC that will help to identify the VC.
service-type	String	Yes	No	Service Type. Possible value: carrier-ethernet-vpn
service-subtype	String	Yes	No	Service SubType. Possible Values: UNI
customer-ref	String	No	No	Customer FDN. e.g., D=CISCO_EPNM!CUSTOMER=<customer name> Default value of "customer name" is "Infrastructure"
service-activate	Boolean	No	Yes	Activate Service. Default value = true
termination-point-list	List container	Yes	N/A	List of connection termination point configurations.
termination-point-config	Container	Yes	N/A	termination point config

UNI Service Order Data	Data Type	Mandatory	Modifiable	Description
tp-ref	String (FDN)	Yes	No	FDN of the port to use - set of RNDs that consists of MD, ME and PTP or FTP instance ids. For example: "MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-2.cisco.com!FTP=name=GigabitEthernet0/4;lr=lr-gigabit-ethernet"
network-interface-name	String	No	No	Name of the new NI to be created. Mandatory while creating new UNI e.g., new uni name like UniA , UniZ etc.
network-interface-ref	String	No	No	Name of the existing NI to be re-used. Mandatory while using existing UNI e.g.,MD=CISCO_EPNM!NI=<existing NI name>
network-interface-list	List container	Yes	N/A	List of network interface configurations.
network-interface	Container	Yes	N/A	Network Interface config.
ref	String (FDN)	No	No	FDN of the existing NI – set of RDNs that consists of MD and NI. Mandatory for Modify operation e.g., MD=CISCO_EPNM!NI=<existing uni name> Note: existing uni name value should be same as the one mentioned for "network-interface-ref".
name	String	No	No	Name of the new NI to be created. Mandatory while creating new UNI e.g., it's value should be same as the value mentioned for "network-interface-name" tag
ce-data	ce-data-network-interface-type	Yes	N/A	Container for CE Network Interface configuration.
description	String	No	Yes	Description of the new NI to be created.
activate	Boolean	Yes	Yes	true/false for Activate NI. Default value: true
ingress-qos-policy-ref	String (FDN)	No	No	Ingress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=<TestQosProfile>

UNI Service Order Data	Data Type	Mandatory	Modifiable	Description
egress-qos-policy-ref	String (FDN)	No	No	Egress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=<TestQosProfile>
mtu	Integer	Yes	No	The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the UNI must be greater than or equal to the MTU defined on the service level. MTU Value should be between 64 and 9216 Default value: 1522
speed	String	No	No	Port speed. You can reduce the speed if this is supported on the port.
mode	String	Yes	No	Mode – values: • FULL DUPLEX—Uses simultaneous communication in both directions between the UNI and the customer's access switch, assuming that both sides support full duplex. If one side does not support full duplex, the port will be brought down. • AUTO NEGOTIATION —Uses the mode that is agreed upon between the two devices, depending on what is supported. Full Duplex will be attempted but if one device does not support it, half duplex will be used. Default value: FULL DUPLEX
enable-link-management	Boolean	No	Yes	Enables the customer access switch to get information about this UNI, VLAN IDs, and services on the UNI, and so on. Default value = false
enable-link-oam	Boolean	No	No	Enables IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch. **NOTE**: For **LAG** Ports this parameter should be set to false.
ce-vlan-id	String	No	No	Untagged CE-VLAN ID – e.g. 1333. The ID of the CE-VLAN assigned to untagged traffic.
service-multiplexing	Boolean	No	No	Allows the UNI to participate in more than one EVC instance. Default value: true
bundling	Boolean	No	Yes	UNI Allows Bundling. Allows the use of multiple VLANs for this UNI. Default value: false
all-to-one-bundling	Boolean	No	No	true or false. Default value: false

1.41.1.11 *Service Order Data – ENNI*

The table below lists the Order Data elements and the supported values for ENNI. Note that the table below describes all the elements in service order data combined for service and endpoint configuration for ENNI. See schema restconf-sai-common.xsd for more details.

ENNI Service Order Data	Data Type	Mandatory	Modifiable	Description
service-name	String	Yes	No	Unique name to identify the circuit/VC.
service-description	String	No	Yes	Description of the VC that will help to identify the VC.
service-type	String	Yes	No	Service Type. Possible value: carrier-ethernet-vpn
service-subtype	String	Yes	No	Service SubType. Possible Values: ENNI
customer-ref	String	No	No	Customer FDN. e.g., D=CISCO_EPNM!CUSTOMER=<customer name> Default value of "customer name" is "Infrastructure"
service-activate	Boolean	No	Yes	Activate Service. Default value = true
termination-point-list	List container	Yes	N/A	List of connection termination point configurations.
termination-point-config	Container	Yes	N/A	termination point config
tp-ref	String (FDN)	Yes	No	FDN of the port to use - set of RNDs that consists of MD, ME and PTP or FTP instance ids. For example: "MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-2.cisco.com!FTP=name=GigabitEthernet0/4;lr=lr-gigabit-ethernet"
network-interface-name	String	No	No	Name of the new NI to be created. Mandatory while creating new ENNI e.g., new uni name like UniA , UniZ etc.
network-interface-ref	String	No	No	Name of the existing NI to be re-used. Mandatory while using existing ENNI e.g.,MD=CISCO_EPNM!NI=<existing NI name>
network-interface-list	List container	Yes	N/A	List of network interface configurations.
network-interface	Container	Yes	N/A	Network Interface config.

ENNI Service Order Data	Data Type	Mandatory	Modifiable	Description
ref	String (FDN)	No	No	FDN of the existing NI – set of RDNs that consists of MD and NI. Mandatory for Modify operation e.g., MD=CISCO_EPNM!NI=<existing uni name> Note: existing uni name value should be same as the one mentioned for "network-interface-ref".
name	String	No	No	Name of the new NI to be created. Mandatory while creating new ENNI e.g., it's value should be same as the value mentioned for "network-interface-name" tag
ce-data	ce-data-network-interface-type	Yes	N/A	Container for CE Network Interface configuration.
description	String	No	Yes	Description of the new NI to be created.
activate	Boolean	Yes	Yes	true/false for Activate NI. Default value: true
ingress-qos-policy-ref	String (FDN)	No	No	Ingress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=<TestQosProfile>
egress-qos-policy-ref	String (FDN)	No	No	Egress QOS Policy Reference. FDN of the existing QOS profile with MD, PROFILE_QOS RDNs. e.g., MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-3!POLICY_QOS=<TestQosProfile>
mtu	Integer	Yes	No	The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the ENNI must be greater than or equal to the MTU defined on the service level. MTU Value should be between 64 and 9216 Default value: 1522
speed	String	No	No	Port speed. You can reduce the speed if this is supported on the port.

ENNI Service Order Data	Data Type	Mandatory	Modifiable	Description
mode	String	Yes	No	Mode – values: • FULL DUPLEX—Uses simultaneous communication in both directions between the UNI and the customer's access switch, assuming that both sides support full duplex. If one side does not support full duplex, the port will be brought down. • AUTO NEGOTIATION —Uses the mode that is agreed upon between the two devices, depending on what is supported. Full Duplex will be attempted but if one device does not support it, half duplex will be used. Default value: FULL DUPLEX
enable-link-management	Boolean	No	Yes	Enables the customer access switch to get information about this ENNI, VLAN IDs, and services on the UNI, and so on. Default value = false
enable-link-oam	Boolean	No	No	Enables IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this ENNI and the customer's access switch. **NOTE**: For **LAG** Ports this parameter should be set to false.
ce-vlan-id	String	No	No	Untagged CE-VLAN ID – e.g. 1333. The ID of the CE-VLAN assigned to untagged traffic.
service-multiplexing	Boolean	No	No	Allows the ENNI to participate in more than one EVC instance. Default value: true
Bundling	Boolean	No	Yes	ENNI Allows Bundling. Allows the use of multiple VLANs for this ENNI. Default value: false
all-to-one-bundling	Boolean	No	No	true or false. Default value: false

1.41.1.12 *QoS policy support*

- The device discovered QoS policy is supported for CEM provisioning: ingress-qos-policy-ref and egress-qos-policy-ref.
- It requires the QoS policy to be configured on the device and discovered in Cisco EPN Manager.
- This means on the CEM request service end, the QoS policy device should be the same as the network interface device.

1.41.1.13 *Partial service support*

- One of the "<termination-point-config>" in a CE or CEM provisioning request can be an Unmanaged endpoint.
- If both 2 "<termination-point-config>" are unmanaged, an error occurs.
- Use this XML structure for an unmanaged endpoint in the request:
```
<p:termination-point-config>
<p:directionality>sink</p:directionality>
```

```xml
            <p:unmanaged-termination-point>
                <p:device-name>testabc2</p:device-name>
                <p:new-device>true</p:new-device>
                <p:device-ip-address>3.2.1.3</p:device-ip-address>
                <p:device-ldp-address>2.3.1.6</p:device-ldp-address>
                <p:vc-id>200</p:vc-id>
            </p:unmanaged-termination-point>
    </p:termination-point-config>
```

- o <device-name> is mandatory. Use a string as a third party device name.
- o <directionality> is mandatory. Allowed values are source, sink and bidirectional
- o <new-device> is optional boolean tag and is used to indicate if device details passed is new or existing device.
    - o If it is true, you also need to provide a <device-ip-address> which should not exist in Cisco EPN Manager.
    - o If it is false, there is no need to provide a <device-ip-address>. However you need to provide the third party device with the same <device-name> that exists in Cisco EPN Manager.
- o <device-ip-address> is the management IP address of the third party device. When <new-device> is true, the <device-ip-address> should not exist in Cisco EPN Manager.
- o <device-ldp-address> is the LDP IP address on the third party LDP configuration.
- o <vc-id> is an integer for vc.

Note: if "new-device" is not provided by user in payload, then backend logic should be able to figure out if unmanaged device details provided by user is new or existing but device-name , device-ip-address and device-ldp-address has to be provided by user in the payload from EPNM 4.1 onward.

1.41.1.14 *Service Order Data - MPLS Layer3 Link*

See schema restconf-sai-l3link.xsd for more details.

service-order-data - Order Data for MPLS-TE Service				
Service Configuration				
Data	**Type**	**Mandatory**	**Modifiable**	**Description**
service-name	String	Yes	Yes	A unique name for the L3 Link.
service-description	String	No	Yes	Description of L3 Link.
service-type	String (mpls-te-tunnel)	Yes	No	The type of service.
service-subtype	String (layer3-link)	Yes	No	Service subtypes.
l3-link-data	Container	Yes	No	Container for Layer3 link settings.
l2-discovery-protocol	String	Yes	Yes	L2 discovery protocol used for L3 Link. Possible values: NONE ,CDP , LLDP and ALL Default: NONE
routing-protocol	String	Yes	No	Routing protocol value used for L3 Link. Possible values: OSPF , BGP and ISIS Default: OSPF
link-vlan	Integer	No	Yes	Link VLAN in the range from 1 to 4094.
enable-mpls-te	Boolean	No	Yes	This is a flag to enable MPLS TE on the L3 Link. Default value: false
termination-	**List**	**Yes**	**No**	**List of termination point configurations.**

point-list	container			
termination-point-config		**Yes**	**No**	**Termination point config.**
directionality	Enum	Yes	No	Values: source, sink, and bidirectional.
tp-ref	fdn	Yes	No	FDN - is device from/to where link is created. e.g., MD=CISCO_EPNM!ND=EPNNCS4216-120.20!FTP=name=GigabitEthernet0/2/0;lr=lr-gigabit-ethernet
ip-address	String	Yes	No	IP address of A or Z end.
subnet-mask	String	Yes	No	Subnet mask of A or Z end. Possible values: 8 to 31.
ingress-qos-policy-ref	fdn	No	Yes	Ingress QOS Policy Reference. FDN of the existing QOS profile with MD, POLICY_QOS RDNs. e.g., ingress-qos-policy-ref>MD=CISCO_EPNM!ND=EPASR907-120.22.SWIM.cisco.com!POLICY_QOS=<qos policy name>
egress-qos-policy-ref	fdn	No	Yes	Egress QOS Policy Reference. FDN of the existing QOS profile with MD, POLICY_QOS RDNs. e.g., MD=CISCO_EPNM!ND=EPASR907-120.22.SWIM.cisco.com!POLICY_QOS==<qos policy name>
L3-link-data	Container	Yes	No	Container for L3 Link Data.
enable-bv-interface	Boolean	No	No	This is a flag to enable bridge + virtual interface on the L3 Link. Default value: true
loopback-interface-ref	String	No	No	This is required only for OSPF and ISIS. Not applicable for BGP. e.g., MD=CISCO_EPNM!ND=EPNNCS4216-120.41!FTP=name=Loopback79;lr=lr-loopback
Ospf	Container	No	No	Container for OSPF data. **Note:** This tag is mandatory when value of "routing-protocol" is OSPF.
process-id	String	Yes	No	OSPF process ID configured on the device.
area	String	No	No	Allowed Value: '0' , NOTE: NCS4K supports only one OSPF instance and it should have area id is 0.
metric	String	No	Yes	OSPF link Path selection metric. Value within 1-65535 range.
enable-synce	Boolean	No	Yes	Flag to indicate synce enable or not for OSPF L3 Link. Default value: false
synce-bridge-domain	Boolean	No	No	Flag to indicate sync e bridge domain or not for OSPF L3 Link. Default value: false
mpls-te	Container	No	No	Container for MPLS TE. See schema restconf-sai-mpls-te.xsd for more details.
te-metric	String	No	Yes	TE Tunnel path selection metric. Value within 1-65535 range.

te-attributes	String	No	Yes	TE related attributes values used for L3 Link. Possible values: 00, 03, 0 or 3.
is-percentage	Boolean	No	Yes	Flag indicate link bandwidth allocation in percentage. Default value: false
bandwidth-unit	String	No	Yes	This attribute specifies the associated transport link Bandwidth (Units in Kbps, Mbps or Gbps).
global-bandwidth	String	No	Yes	Total Bandwidth reserved for the interface in percentage or Bandwidth Unit for input.
subpool-bandwidth	String	No	Yes	Portion of bandwidth reserved for the interface in percentage or Bandwidth Unit for input.
Isis	Container	No	No	Container for ISIS data. **Note:** This tag is mandatory when value of "routing-protocol" is ISIS.
process-id	String	Yes	Yes	ISIS process id configured on the device.
Networks	String	Yes	No	Network Id configured on the device.
Metric	String	No	Yes	ISIS metric used for L3 Link. Value within 1-65535 range.
circuit-type	String	No	Yes	Circuit type used. Possible values: NONE , LEVEL1_IS, LEVEL2_IS, LEVEL1_L2_IS. Default value: NONE
level1-metric	String	No	Yes	Level1 metric , it will be used only when value of "circuit-type" is LEVEL1_IS or LEVEL1_L2_IS Value within 1-65535 range.
level2-metric	String	No	Yes	Level2 metric , it will be used only when value of "circuit-type" is LEVEL2_IS or LEVEL1_L2_IS Value within 1-65535 range.
authentication-mode	String	No	Yes	Authentication mode used. Possible values: HMAC_SHA1, HMAC_SHA256, HMAC_SHA384, HMAC_SHA512, HMAC_MD5, TEXT
authentication-key-chain	String	No	Yes	Authentication key chain configured on the device.
authentication-for-send-only	Boolean	No	Yes	Flag to indicate authentication-for-send-only. Default value: false
enable-synce	Boolean	No	Yes	Flag to indicate synce enable or not. Default value: false
synce-bridge-domain	Boolean	No	No	Flag to indicate sync e bridge domain or not. Default value: false
bgp	Container	No	No	Container for BGP data. **Note:** This tag is mandatory when value of "routing-protocol" is BGP.
bgp-as-number	String	Yes	No	Bgp as number configured on the device for BGP link.
route-policy	String	No	Yes	Route policy configured on the device used for BGP link.
route-reflector-client	Boolean	No	Yes	Flag to indicate route reflector client to be used or not.

				Default value: false
use-aigp	Boolean	No	Yes	Flag to indicate use-aigp or not. Default value: false
update-source-ref	String	No	Yes	Update source for BGP link. This should not be part of user input when value of "use-aigp" true. e.g., MD=CISCO_EPNM!ND=NCS4206-C!FTP=name=BDI1;lr=lr-bridge
password-type	String	No	Yes	Password type used for BGP L3 Link. Possible values: Encrypted or PlainText Default value: Encrypted
Password	String	No	Yes	Password used for BGP L3 Link.
enable-mpls	Boolean	No	Yes	Flag to indicate enable mpls or not. Default value: false
enable-synce	Boolean	No	Yes	Flag to indicate enable sync e or not. Default value: false
synce-bridge-domain	Boolean	No	No	Flag to indicate enable sync e bridge domain or not. Default value: false
bfd-settings	Container	No	No	Container for BFD Settings.
bfd-template	String	No	Yes	Bfd template configured on selected device and port of L3 Link.
bfd-min-interval	String	No	No	Bfd min interval to be used for L3 Link. This tag should be used as input only when "bfd-template" is not used. Default value =100.
bfd-multiplier	String	No	Yes	Bfd multiplier to be used for L3 Link. This tag should be used as input only when "bfd-template" is not used.
bfd-fast-detect	Boolean	No	Yes	Flag to indicate bfd fast detect to be used or not for the L3 Link. This tag should be used as input only when "bfd-template" is not used.

1.41.1.15 *Service Order Data - MPLS-TE*

See schema restconf-sai-mpls-te.xsd for more details.

service-order-data - Order Data for MPLS-TE Service			
Service Configuration			
Data	**Type**	**Mandatory**	**Description**
service-type	String (mpls-te-tunnel)	Yes	The type of service.
service-subtype	String (Bidirectional TE Tunnel)	Yes	Service subtypes
service-template	String	No	The template to be associated with the service.
Customer	Fdn	Yes	Customer FDN
service-name	String	Yes	A unique name for the service.
service-description	String	No	A unique description about the service.
service-activate	Boolean	No	Field to specify if service need to be activated or not post service creation.

	Tunnel Configuration		
Data	**Type**		**Description**
termination-point-list	List container	Yes	List of connection termination point configurations.
directionality	Enum	Yes	Values: source, sink, and bidirectional.
nd-ref	Fdn	Yes	Source Node FDN - is device from where tunnel is created.
mpls-te-data	Container	No	Container for MPLS-TE data.
routing-process	Container	Yes	Container for routing details.
router-address	String	Yes	Routing process address for which MPLS TE router is enabled.
routing-process-id	String	Yes	Routing process id.
loopback-address	String	Yes	Loopback address.
	Path Configuration		
forwarding-path	Container	No	Container for Forwarded Path entries.
mpls-te-data	Container	No	Container for MPLS-TE data.
te-tunnel-type	Enum(uni-directional, bi-directional)	No	Type of te tunnel
tunnel-service-profile-ref	String (FDN)	No	Service profile refrence for tunnel. e.g. MD=CISCO_EPNM!PROFILE_SERVICE=TE-Bi
wrap-protection	Boolean	No	Wrap Protection
enable-fault-oam	Boolean	No	Enable fault OAM
enable-frr	Boolean	No	This attribute specifies whether to enable autoroute option.
enable-auto-bandwidth	Boolean	No	This attribute specifies whether to enable autobandwidth option.
enable-autoroute	Boolean	No	This attribute specifies whether to enable autoroute option.
enable-lockdown	boolean	No	This attribute specifies whether to enable lockdown option.
protection-type	Enum (Working, Working+Protected, Working+Restore, Working+Protected+Restore)	Yes	Type of MPLS Tunnel Path Protection.
tunnel-setting		No	Container for tunnel settings.
global-id	Integer (Range:1-4294967295)	Yes (for bi-directional-tunnel), No (for uni-directional-tunnel)	ID used with association ID and source address to form bidirectional tunnel uniqueness.
affinity-bits	String (Range: 0x0-0xFFFFFFFF, Default: 0x0)	No	Affinity Value
affinity-mask	String (Range: 0x0-0xFFFFFFFF, Default: 0x0)	No	Affinity mask on desired link attributes.
setup-priority	Integer (Range:0-7, Default: 7)	No	Tunnel Setup Priority
hold-priority	Integer (Range:0-7, Default:	No	Tunnel Hold Priority

	7)		
enable-record-route	boolean	No	This attribute specifies whether to enable record route option.
bandwidth-pool-type	String (Global, Subpool, Empty)	Yes	This attribute specifies whether global or subpool bandwidth reservation is used
Bandwidth	Integer	Yes	This attribute specifies the associated transport tunnel Bandwidth
bandwidth-unit	String	No	Units to be specified for bandwidth field. Possible Values: Kbps, Mbps, Gbps Default Value: Kbps
auto-bandwidth-frequency	Integer	No	This attribute specifies the auto bandwidth frequency.
max-bandwidth	String	No	This attribute specifies the associated transport tunnel max Bandwidth
bandwidth-change-frequency	String	Yes	This attribute specifies the bandwidth change frequency. Frequency range should be 300 to 604800 Default value : 300
max-auto-bandwidth	String	No	This attribute specifies the maximum auto bandwidth.
max-auto-bandwidth-unit	String	No	Units to be specified for max-auto-bandwidth. Possible Values: Kbps, Mbps, Gbps Default Value: Kbps
min-auto-bandwidth	String	No	This attribute specifies the minimum auto bandwidth.
min-auto-bandwidth-unit			Units to be specified for min-auto-bandwidth. Possible Values: Kbps, Mbps, Gbps Default Value: Kbps
enable-bw-collection	string	No	This attribute specifies if auto bandwidth collection is enabled. Applicable only for Uni directional tunnel.
adjustment-threshold	Integer	No	This attribute specifies the auto bandwidth adjustment threshold. Applicable only for Uni directional tunnel.
overflow-limit	Integer	No	This attribute specifies the auto bandwidth overflow limit. Applicable only for Uni directional tunnel.
overflow-threshold	Integer	No	This attribute specifies the auto bandwidth overflow threshold. Applicable only for Uni directional tunnel.
BFD Settings			
bfd-settings	Container	No	Container for bfd settings.
Enable	Boolean	No	Enable bfd.
min-interval	integer(Range: 15 to 200 Default: 100)	Yes	The minimum control packet interval for BFD sessions in milliseconds.
multiplier	integer (default 3)	Yes	Number of times a packet is missed before BFD declares the session down.

	MplsTe Path Options		
mpls-te-path-options	mpls-path-options	No	Container for MPLS-TE path options.
working-path	mpls-path	No	Container for working path.
protection-path	mpls-path	No	Container for protection path.
restore-path	mpls-path	No	Container for restore path.
	Mpls Path		
new-lsp-attribute-list	Boolean	No	Specifies if the path uses a new or existing lsp path. Applicable only for Bi directional te tunnel.
lsp-attribute-list-name	String		Name of the lsp attribute list. Applicable only for Bi directional te tunnel.
lsp-attributes	Mpls-lsp-attribute-type		Container for the new LSP attribute configuration. Applicable only for Bi directional te tunnel.
enable-lockdown	Boolean	No	This attribute specifies whether to enable lockdown option on working-path, protection-path or *restore-path (*Only for XR devices).
enable-sticky	Boolean	No	This attribute specifies whether to enable sticky on working-path.
enable-non-revertive	Boolean	No	This attribute specifies whether to enable non-revertive on protection-path.
enable-srlg	Boolean	No	This attribute specifies whether to enable srlg on protected path.
	Mpls lsp attribute type		
affinity-bits	String	No	This attribute specifies Affinity bits on desired link attributes
affinity-mask	String	No	This attribute specifies Affinity mask on desired link attributes
setup-priority	Int	No	This attribute specifies the associated transport tunnel Setup Priority. Range:0-7, Default: 7
hold-priority	Int	No	This attribute specifies the associated transport tunnel Hold Priority. Range:0-7, Default: 7
enable-record-route	boolean	no	This attribute specifies whether to enable record route option.
path-type	Enum (dynamic, explicit)	Yes	Path type enum
is-existing-path	Boolean	No	Choose a new or existing path option.
explicit-path-name	String	No	IP explicit path name.
explicit-path-hop	Container	No	Explicit path hop container.
node-ref	String	No	Node Fdn
interface-ip-address	String	No	Mpls interface ip address.
constraint-type	Enum (include, exclude)	No	Explicit path constraint type.

1.41.1.16 *Service Order Data - MPLS L3VPN*

This section describes the order data required for provisioning MPLS L3VPN services.

See schema restconf-sai-mpls-l3vpn.xsd for more details.

	service-order-data - Order Data for MPLS L3VPN Service			
	Service Configuration			
Data	**Type**	**Mandatory**	**Description**	
service-type	String	Yes	The type of service.	
service-subtype	String	Yes	Service sub type. Supported value: UNICAST.	
service-activate	Boolean	No	Option to activate the service.	
customer-ref	FDN	Yes for amend/terminate	Customer FDN.	
service-name	String	Yes	Name for the service.	
Vpn-id	String	Yes	VPN-ID for the service	
service-profile-ref	String (FDN)	Yes	Service profile reference used to create a service. e.g. MD=CISCO_EPNM!PROFILE_SERVICE=CEM-Profile1	
service-description	String	No	Service description.	
service-mtu	Integer(Default 1520)	Yes	Maximum Transmission Unit that interfaces can optimally process.	
create-full-mesh	Boolean	No	Enables you to create a Full Mesh.	
enter-full-mesh-prefix	Boolean	Yes	Allows you to enter full mesh prefix value from User Input.	
full-mesh-prefix	Integer	Yes	The actual full mesh prefix value.	
	Route Target Allocation			
Data	**Type**		**Description**	
address-family	String	No	Address family- either IPv4 or IPv6.	
route-target	String	No	Route target value for which the interface enables packets to pass through if they have the matching ID.	
	VRF Details			
vrf-device-name	String	Yes	Device FDN.	
vrf-description	String	No	A unique description about the VRF.	
vrf-name	String	Yes	The name for the VRF.	
is-auto-rd	String	Yes	Auto Route Distinguisher, either ture or false has to be provided	
	Route Targets			
ip-v4-route-target/ip-v6-route-target	String	No	The Route Target value. Needed if Route Target allocation was provided	
direction	Enum (Import/Export/Both/None)	No	Direction of the packet flow through the interface (based on the match with the route target ID). Needed if Route Target allocation was provided	

	Route Distribution		
protocol	Enum	No	Supported values are: OSPF, RIP, Connected, and Static.
metric	Boolean	No	Option to enable autoroute. Mandatory if OSPF protocol is selected
route-policy	String	No	Types of Routing Policy the VRF will use for Route Distribution.
routing-process-id	Integer	No	The $process\text{-}id$ argument that identifies the OSPF process. Mandatory if OSPF protocol is selected
route-match-type	String	no	Only if OSPF protocol selected, one of the following values can be provided Internal External External 1 External 2 NSSA External NSSA External 1 NSSA External 2 LEVEL 1 LEVEL INTER-AREA Level 2
	UNI		
uni-name	String	Yes	Name of the UNI.
uni-ref	String	Yes	Uni fdn if using an existing UNI
port	String	Yes	Port ID as FDN.
device	String	Yes	Device name as FDN.
create-uni	Boolean	No	Value determines if new UNI is being created or existing UNI is being used.
vrf-name-select	String	Yes	To VRF under which the UNI is being created.
enable-link-oam	Boolean	no	To enable or disable Link Operations, Administration, and Maintenance.
service-multiplexing	Boolean	no	Allows multiple services to be provisioned on this UNI.
uni-duplex-mode	Enum (FULL DUPLEX/ AUTO NEGOTIATION)	No	Duplex mode setting.
sep-ipv6-address	IPv6	No	Service end-point IPv6 address.
sep-outer-vlan	Integer	yes	Outer VLAN ID.
sep-ipv4-address	IPv4	Yes	Service end-point IPv4 address.
sep-ipv4-subnet-mask	Integer	Yes	Subnet mask value.
sep-ipv6-subnet-mask	Integer	No	Subnet mask value.
uni-mtu	Integer	Yes	Maximum Transmission Unit that UNI can optimally process.
uni-description	String	No	A unique description about the UNI.

enable-link-management	Boolean	No	
existing-uni-id	Integer	No	If choosing the existing UNI instead of creating new UNI.
service-state	Boolean (default true)	Yes	Service state
use-irb	Boolean (default true)	no	Use integrated routing and bridging.
encapsulation	Enum	no	TAGGED UNTAGGED DEFAULT.
	Termination Point		
termination-point-list	Container	Yes	N/A
termination-point-config	Container	Yes	N/A
tp-ref	String (FDN)	Yes	Termination-point FDN
nd-ref	String (FDN)	Yes	Node FDN
network-interface-name	String	Yes	Network interface name
l3vpn-data	Container	Yes	Container for l3vpn data
hsrp	Container	Yes	Container for hsrp data
group-number	Integer	Yes	HSRP group number.
priority	Integer	Yes	HSRP priority or weight of using this among the members.
virtual-ip-address	IP-address	Yes	Virtual ip address of either ipv4 or ipv6.
authentication-key	String	No	The authentication key can be up to 8 characters in length; the default string is cisco. The authentication key is carried in all HSRP messages.
hello-timer	Integer	No	HSRP hello timer.
hold-timer	Integer	No	HSRP hold timer.
min-delay-interval	Integer	No	The minimum delay that is applied after any subsequent interface up event (if the interface flaps).
reload-delay-interval	Integer	No	The reload delay that is applied after the first interface up event.

preempt-min-delay	Integer	No	Set to cause the local router to postpone taking over the active role for the shown number of seconds.
preempt-reload-delay	Integer	No	Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown.
	Routing Protocol Settings		
device-ref	String	Yes	String
vrf	String	Yes	String
routing-protocol-type	ENUM	Yes	BGP OSPF OSPFv3
address-family	ENUM	Yes	IPv4 IPv6
authentication-type	ENUM	No	MD5
password-type	String	No	Applicable only for BGP routing-protocol-type Possible values : 1. Plain Text 2. Encrypted
password	String	No	String
authentication-type	String	No	Applicable only for OSPFv3 KEYCHAIN is the value currently supported
key-chain	String	no	String
	BGP Neighbors		
neighbor-address	IP Address	Yes	IP address of the neighbor- either IPv4 or IPv6.
neighbor-as	Integer (1-65536)	Yes	Autonomous System number of the neighbor.
ingress-rp	String	No	
egress-rp	String	No	
local-as	Integer (1-65536)	No	Local Autonomous system number.
as-action	String	no	-
	OSPF Process Information		
router-id	IP Address	Yes	IP address of the neighbor- either IPv4 or IPv6.
area-id	Integer (0-4294967295)	Yes	Range between 0-4294967295.
domain-type	Hexadecimal	No	0x0005 0x0105 0x0205 0x8005
domain-value	Hexadecimal	yes	Hexadecimal number less than or equal to 6 Octet

	IPSLA Details		
operation-name	String	yes	Name of the IPSLA name.
operation-vrf	String	yes	-
operation-source-port-ref	integer	Yes	please give the value between 1024 and 65535
operation-destination-port-ref	String	Yes	Port FDN
ipsla-operation-type	String	yes	UDP ECHO, ICMP ECHO, ICMP JITTER, and UDP JITTER.
operation-source-device-ref	String	yes	-
reaction-action-variable	String	No	CONNECTION LOSS, RTT, TIMEOUT ERROR, and VERIFY ERROR.
reaction-action-type	Enum	no	NONE, TRAP AND TRIGGER, TRAP ONLY, and TRIGGER ONLY.
reaction-upper-threshold-value	String	no	Reaction action type will be triggered when this upper threshold value is breached.
operation-destination-device-ref	Integer	yes	please give the value between 1024 and 65535
reaction-lower-threshold-value	String	no	Reaction action type will be triggered when this lower threshold value is breached.
reaction-threshold-type	String	yes	AVERAGE, CONSECUTIVE, IMMEDIATE, NEVER, X out of Y occurrences.
average-number-value	Integer	No Yes when reaction-threshold-type is AVERAGE	Determines the average number of entities.
consecutive-n-values	Integer	No Yes when reaction-threshold-type is CONSECUTIVE	The threshold breach is applied for n entities. Yes when reaction-threshold-type is CONSECUTIVE
reaction-x-axis-values	Integer	No Yes when reaction-threshold-type is X out of Y occurrences	Determines the number of occurrence out of Y.
reaction-y-axis-values	Integer	No Yes when reaction-threshold-type is X out of Y occurrences	Determines the total occurrence of the given entity.
simple-frequency-value	Integer	no	Indicates the periodicity

			of this SLA (how frequently this check should be performed). Please enter the value between 5 and 604800 seconds
simple-life-time-value	Integer	no	Indicates that if the event does not occur, the check will be performed after the time (in milli seconds) specified in this value. Please enter the value between 0 and 2147483647 seconds
simple-age-out-value	Integer	no	Indicates the maximum time in milliseconds until when this IPSLA should function. Please enter the value between 0 and 2073600 seconds
start-now	Boolean	no	Indicates that the execution can start immediately.
start-time	Integer	no	Indicates that the execution must start after the given number of seconds.

1.41.1.17 *Service Order Data – Optical*

The table below lists the Order Data elements and the supported values for optical services. Note that the table below describes all the elements in the service order data combined for service and endpoint configuration for all the optical services (OCHNC, OCHCC, OCHTrail, OCHTRAIL_UNI, OPU_OVER_ODU, ODU_TUNNEL,ODU_UNI and ODU).

See schema restconf-sai-optical.xsd for more details.

Spectrum Switch Optical Network (SSON) – Media Channels: Purpose of the feature is the optimization of the use of optical bandwidth. That is obtained by creating services without spare "guard" band within, delegating Control Plane SW in the device to choose the exact frequencies to be used. (For example: MCHG, MCHNC, MCHCC and MCHTrail)

Services can use Media Channels, that can use multiple individual carriers of different frequencies splitting the payloads coming from client ports into multiple channels when the single channel cannot transport the entire required bandwidth (For example a 500Gb payload split into two 250Gb Trunk ports).

Managed Plane OCH-Trail/OCHNC/OCHCC services (MP): The Cisco NCS 2000 SVO provides benefits to in the areas of new interfacing and models by virtualizing the network elements and enhanced web applications.

The latest generation of computing involves virtualization, extending this to the network element by virtualizing the network functions over an SVO line module hosting multiple network elements of a network.

Each network element is operating in high-availability mode of operation between the SVO line modules hosted inside the NCS 2006 or NCS 2015 chassis.

For creating OCHCC MP service, it required underlying OCH-Trail MP service available on network. It won't create underlying OCH-Trail as WSON/SSON services.

Discovery is not supported for MP circuits

Optical Service Order Data	Data Type	Applicable to Service Type	Modifiable	Description
service-name	String	All	yes	Unique name to identify the circuit/VC.
service-description	String	All	yes	Description of the VC that will help to identify the VC.
service-type	String	All	No	Service Type. Possible value: **optical** – for Optical Services **explicit-path** – for MPLS TE Explicit Path
service-subtype	String	All	No	Service SubType. Possible Values: OCHNC, OCHCC, OCHTrail, OCHTRAIL_UNI, ODU_TUNNEL, ODU_UNI, ODU – for Optical Services **mplste-explicit-path** – for MPLS TE Explicit Path
customer-ref	String	All	Yes	Customer FDN.
mutual-diverse	Boolean	OCHTRAIL_UNI	No	For mutual Diverse from one another.
diverse-from-name	String	OCHTRAIL_UNI	No	Diverse from Service name.
diverse-from-cfs-ref	FDN	OCHTRAIL_UNI and ODU UNI	No	Diversing current Service from the service which have the same AEND owning Entity value.
service-activate	Boolean	true/false	Yes	Activate Service.
direction	String	ALL	No	Service/Circuit direction. Possible Values: BIDIRECTIONAL, UNIDIRECTIONAL
optical-data	optical-data-service-type	ALL	N/A	Container for OPTICAL service configuration.
termination-point-list	List container	All	N/A	List of connection termination point configurations.
path-diversity	container	OCHNC, OCHCC and OCHTrail	N/A	This container is applicable only for the services of type OCHNC, OCHCC and OCHTrail.
constraints	container	All OCH and MCH service	N/A	Constraints container will holds list of constraint values to be applied for a particular service.
constraint	container	All OCH and MCH service	Yes, only for OCHTrail, MCHTrail and OCHTrail Uni Service	This Constraint will hold set of attributes which can be applied on a constraint.

The table below describes the optical data types and lists the services they are applicable to:

Optical Service Order Data	Data Type	Applicable to Service Type	Modifiable	Description
state-type	Enum	All	Yes	This attribute represents generic state type of the service. Possible Values: IN_SERVICE, OUT_OF_SERVICE, UP, DOWN
admin-state	Enum	All	Yes	This attribute represents generic admin state of the. Possible Values: IN_SERVICE, OUT_OF_SERVICE, UP, DOWN
uni	Boolean	All	No	UNI Allows Bundling. Allows the use of multiple VLANs for this UNI.
label	String	All	Yes	Label for service provisioning.
protection	Enum	All	No	Protection Mechanism for service provisioning. Possible Values: NONE,Y_CABLE,SPLITTER , PSM, ONE_PLUS_ONE, ONE_PLUS_ZERO, ONE_PLUS_R, ONE_PLUS_ONE_PLUS_R
validation	Enum	OCHNC, OCHNC MP, OCHCC, OCHTrail and OCHTRAIL_UNI	No	This attribute represents validation of the service. Possible Values: NONE, FULL, INHERITED
manage-constraints	Boolean	All		Boolean flag to specify if constraints need to be considered or not. Default value: false **Note**: while provisioning optical service using existing service profile containing constraints information, <manage-constraints> tag needs to be set to true.
qualifier	Enum	All	NO	During OCHTRAIL/OCHCC MP services CRUD Operations, user should provide 'qualifier' as "MP". Same is applicable for service-profile during provide/amend/terminate operations.
payload	Enum	OCHCC MP and OCHTRAIL MP	NO	payload attribute for service provisioning. Possible values: 10GIGE, 100GIGE, 400GIGE, OTU2, OTU4, OTU4C2, OC192, STM64
administrative-status	Enum	OCHCC MP ,OCHNC MP and OCHTRAIL MP	NO	administrative-status attribute for service provisioning. Possible values: IN_SERVICE, IN_SERVICE_AUTOMATIC_IN_SERVICE, OUT_OF_SERVICE_DISABLED, OUT_OF_SERVICE_MAINTENANCE
bandwidth	Enum	OCHCC MP and OCHTRAIL MP	NO	bandwidth attribute for service provisioning. Possible values: OTU3, OTU4, OTU4C2, OTUC3, OTUC4, OTUC5, OTUC6, OTUC2_30, OTUC3_30, OTUC4_30, OTUC5_30, OTUC6_30
grid-type	Enum	OCHCC MP ,OCHNC MP and OCHTRAIL MP	NO	grid-type attribute for service provisioning Possible values: FIXED_50, FLEX_6_25, FLEX_100, FIXED_75
optical-threshold	String	OCHNC, OCHCC, OCHTRAIL and OCHTRAIL_UNI	No	Optical Threshold for service provisioning.

optical-threshold-protected	String	OCHNC, OCHCC and OCHTrail.	No	Optical Threshold Protected for service provisioning.
up-stream-channel-power-offset	String	OCHNC, OCHCC and OCHTrail.	No	Up Stream Channel Power Offset for service provisioning.
down-stream-channel-power-offset	String	OCHNC, OCHCC and OCHTrail.	No	Down Stream Channel Power Offset for service provisioning.
ignore-path-alarm	Boolean	OCHNC, OCHCC and OCHTrail.	Yes	True or false.
allow-regeneration	Boolean	OCHNC, OCHCC, OCHTrail and OCHTRAIL_UNI	Yes	True or false.
restoration	String	OCHNC, OCHCC, OCHTrail, OCHNC MP and OCHTRAIL_UNI	Yes	Restoration for service provisioning.
revert	String	OCHNC, OCHCC,OCHNC MP and OCHTrail.	Yes	Revert for service provisioning.
soak-time	String	OCHNC , OCHNC MP and OCHTrail.	Yes	Soak Time for service provisioning.
priority	String	OCHNC, OCHCC, OCHTrail and OCHTRAIL_UNI	Yes	Priority for service provisioning.
validation-restoration	String	OCHNC, OCHNC MP, OCHCC and OCHTrail.	Yes	Validation Restoration for service provisioning.
optical-threshold-restoration	String	OCHNC, OCHCC and OCHTrail.	Yes	Optical Threshold Restoration for service provisioning.
optical-threshold-restoration-protected	String	OCHNC, OCHCC and OCHTrail.	Yes	Optical Threshold Restoration Protected for service provisioning.
frequency	String	OCHNC , OCHNC MP and OCHTrail.	No	Frequency for service provisioning. (deprecated)
width	String	OCHNC and OCHTrail.	No	Width for service provisioning.
frequency-required	Boolean	OCHTrail MP and OCHNC MP	No	frequency-required attribute is required for providing restoration frequency for ochtrail MP service. And its deprecated for others possible values: true or false.

frequency-protected	String	OCHNC , OCHNC MP and OCHTrail.	No	Frequency Protected for service provisioning. (deprecated)
width-protected	String	OCHNC and OCHTrail.	No	Width Protected for service provis(deprecated)ioning.
frequency-protected-required	Boolean	OCHNC and OCHTrail.	No	True or false. (deprecated)
alien-card-id	String	OCHNC MP	Yes	Alien Card Id for Provisioning.
alien-trunk-mode	String	OCHNC MP	Yes	Alien Trunk Mode for Provisioning
alien-fec-mode	String	OCHNC MP	Yes	Alien Fec Mode for Provisioning
open-end	Boolean	OCHTrail, ODU_TUNNEL and ODU_UNI	No	True or false.
record-route	Boolean	ODU_TUNNEL and ODU_UNI	yes	True or false.
otn-service-type	String	ODU_TUNNEL, ODU_UNI and ODU	Yes	OTN Service Type for service provisioning.
bandwidth	Enum	ODU_TUNNEL, ODU_UNI and ODU	yes	Bandwidth for service provisioning. Possible values: NONE, ODU0, ODU1, ODU1E, ODU1F, ODU2, ODU2E, ODU2F, ODU3, ODU3E1, ODU3E2, ODU4, ODUFLEX For ODU
framing-type	String	ODU_TUNNEL and ODU_UNI	No	Framing Type for service provisioning.
bit-rate	String	ODU_TUNNEL and ODU_UNI	No	Bit Rate for service provisioning.
protection-profile	String	ODU_TUNNEL and ODU_UNI	No	Protection Profile for service provisioning.
client-port-status	Enum	OCHCC and MCHCC	No	Applicable values Ex: UP and DOWN. 1. UP for create/provision a service 2. DOWN for delete/terminate a service
explicit-path	container	ODU_UNI	No	Explicit path for service provisioning

The table below describes the explicit path data types and lists the services they are applicable to:

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
explicit-path	container	ODU_UNI	No	No	Explicit path for service provisioning
option	Enum	ODU_UNI	Yes	No	Path Option Applicable values Ex: PROTECTED, RESTORED and WORKING
type	Enum	ODU_UNI	Yes	No	Path type Applicable values Ex: DYNAMIC and EXPLICIT

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
path-ref	String	ODU_UNI	Yes	No	For example: MD=CISCO_EPNM!ND=NCS4K-146-18.cisco-lab!PATH=EP_171221
protected-by	String	ODU_UNI	No	No	Protected By
restored-by	String	ODU_UNI	No	No	Restored By
mplsTEExplicitPath	List container	ODU_UNI	Yes NA if type is DYNAMIC	No	List of explicit path Entries
pathEntries	Container	ODU_UNI	Yes	No	Explicit path entries
meRef	String	ODU_UNI	Yes	No	For example: MD=CISCO_EPNM!ND=NCS4K-146-25.cisco-lab
tpRef	String	ODU_UNI	Yes	No	For example: MD=CISCO_EPNM!ND=NCS4K-146-25.cisco-lab!CTP=name=OTU20/6/0/5;lr=lr-och-transport-unit-2
constraintType	ENUM	ODU_UNI	Yes	No	Applicable values Ex: STRICT, LOOSE and EXCLUDE

The table below describes the different endpoint data types and lists the services they are applicable to:

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
termination-point-list	Terminationpoint-list container	All	Yes	No	termination point list
termination-point-config	container	All	Yes	No	termination point configuration
tp-ref	String (FDN)	All	Yes	No	FDN of the port to use - set of RNDs that consists of MD, ME and PTP or FTP instance ids. For example: "MD=CISCO_EPNM!ND=M6-234-248!FTP=name=PCHAN-2-14-RX;lr=LR_PHYSICAL_OPTICAL". Note: For ODU LocalCrossConnect's Provisioning request tp-ref value should be populate from tp-ref correspond to port-name of get PortDetails API response **(1.88-Port Details Retrieval)**. For ODU LocalCrossConnect's Modify request tp-ref value should be populate from getVC response (fdn attribute under termination-point).
directionality	Identity	All	Yes	NO	source, sink, and bi-directional

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
optical-data	**optical-data-**	For All Optical services	Yes		Container for All OPTICAL services Ex: OCHCC,OCHNC, OCHTrail, ODU Tunnel, ODU UNI and OCHTrail Uni etc.
ochnc-data	container	OCHNC	Yes	No	OCHNC service container
ochcc-data	container	OCHCC	Yes	No	OCHCC service container
och-trail-data	container	OCHTrail	Yes	No	OCHTrail service container
och-trail-uni-data	container	OCHTRAIL_UNI	Yes	No	OCHTRAIL_UNI service container
odu-tunnel-data	container	ODU_TUNNEL	Yes	No	ODU_TUNNEL service container
odu-uni-data	container	ODU_UNI	Yes	No	ODU_UNI service container
odu-data	container	ODU	Yes	No	ODU service container
drop-port-ref	String	OCHNC	Yes	No	FDN of the port to use as drop port – set of RNDs that consists of MD, ME and PTP or FTP instance ids. For example: "MD=CISCO_EPNM!ND=M6-234-248!FTP=name=PCHAN-2-14-RX;lr=LR_PHYSICAL_OPTICAL"
diverse-from-path-ref	String	OCHNC, OCHCC and OCHTrail	Yes, if 'path-diversity' is provided in payload	No	FDN value for service to use diverse-path, Ex :MD=CISCO_EPNM!CFS=TRAIL-OCHCC_10GIGE_MXP_1
constraint-type	Enum	OCHNC, OCHCC and OCHTrail	Yes, if 'path-diversity' is provided in payload	No	Possible Values: LOOSE and STRICT
diversity-type	Enum	OCHNC, OCHCC OCHTrail and ODU	Yes, if 'path-diversity' is provided in payload	No	Possible Values: NE, LINK and SRRG
constraint	String	All OCH and MCH services	No	No	Name of the constraint
link-fdn	String	All OCH and MCH services	Yes, if constraint-type is LINK	No	FDN of TL, Ex: MD=CISCO_EPNM!TL=10.225.120.39:[WDMSIDE-B]--10.225.120.41:[WDMSIDE-A]
link-direction-reverse	Boolean	All OCH and MCH services	No	No	This attribute is used to use link constraint in reverse direction. Possible values are 'true'. Note: Applicable only when user need the link direction reverse.
nd-ref	String	All OCH and MCH services	Yes, if constraint-type is NODE	No	FDN of Node, Ex : MD=CISCO_EPNM!ND=tcc200
constraint-type	Enum	All OCH and MCH services	Yes, if Constraints are part of payload	No	LINK, NODE

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
as	Enum	All OCH and MCH services	Yes, if Constraints are part of payload	Yes	INCLUDE, EXCLUDE and INCLUDE_REGEN
route	Enum	All OCH and MCH services	Yes, if Constraints are part of payload	Yes	Possible values are 'WORK', 'PROTECTED', 'WORK_RESTORE', 'PROTECTED_RESTORE and 'WORK_AND_PROTECTED' (Deprecated)
reversion-time	String	ODU	No	No	Possible values in mins. Value in range [5-12] * 60 * 1000, with increment step of 30 * 1000
hold-off-timer	String	ODU	No	No	Possible values in ms. Value in range [0-10000], with increment step of 100
path-computation-strategy	Enum	ODU	No	No	Possible values are "ODU" and "PCE". Note: while modifying **ODU** service the possible value is "NETWORK".
local-cross-connect	Boolean	ODU	No	No	This attribute is used to create LocalCrossConnect service. Possible value is 'true'. Note: Applicable only when user need to create ODU LOCAL CROSS CONNECT Service.
odu-nd-ref	String	ODU	Yes, If local-cross-connect value is 'true'	No	FDN of Node, Ex : MD=CISCO_EPNM!ND=tcc200
source-port-name	String	ODU	Yes, If local-cross-connect value is 'true'	No	This attribute value populates from the getPortDetails API response **(1.88- Port Details Retrieval)**. Note: The **port-name** attribute value should be use where the **type** attribute value is "CLIENT or TRUNK" in the getPortDetails API response. If source-port-name value is Client Port then the destination-port value will be Trunk Port and vice-versa.
secondary-source-port-name	String	ODU	Yes, If local-cross-connect value is 'true' and protection value is 'ONE-PLUS-ONE'	No	This attribute value populates from the getPortDetails API response. **(1.88- Port Details Retrieval)**. Note: The **port-name** attribute value should be use where the **type** attribute value is "TRUNK" in the getPortDetails API response.

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
destination-port-name	String	ODU	Yes, If local-cross-connect value is 'true'	No	This attribute value populates from the getPortDetails API response. **(1.88- Port Details Retrieval)**. Note: The **port-name** attribute value should be use where the **type** attribute value is "CLIENT or TRUNK" in the getPortDetails API response. If source-port-name value is Client Port then the destination-port value will be Trunk Port and vice-versa.
source-odu-slice	String	ODU	Yes, If local-cross-connect value is 'true'	No	This attribute value populates from the getPortDetails API response. **(1.88- Port Details Retrieval)**. Note: The **odu-slice** attribute value should be use from the getPortDetails API response.
secondary-source-odu-slice	String	ODU	Yes, If local-cross-connect value is 'true' and protection value is 'ONE-PLUS-ONE'	No	This attribute value populates from the getPortDetails API response. **(1.88- Port Details Retrieval)**. Note: The **odu-slice** attribute value should be use from the getPortDetails API response.
destination-odu-slice	String	ODU	Yes, If local-cross-connect value is 'true'	No	This attribute value populates from the getPortDetails API response. **(1.88- Port Details Retrieval)**. Note: The **odu-slice** attribute value should be use from the getPortDetails API response.

Media Channels - spectrum switched optical network (SSON)

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
mch-group-data	container	MCHG	Yes, for MCHGroup	No	Hold's List of mchgroup service attributes
mchcc-data	container	MCHCC	Yes, for MCHCC	No	Holdsl List of mchcc service attributes
mchnc-data	container	MCHNC	Yes, for MCHNC	No	Holdsl List of mchnc service attributes
mch-trail-data	container	MCHTrail	Yes, for MCHTrail	No	Holdsl List of mchtrail service attributes
width	float	All MCH services	Yes	No	Default value is 50.0
auto-provisioning	Enum	All MCH services	Yes, for all MCH services	No	TRUE/FALSE
central-wavelength-required	Enum	All MCH services	Yes, only if "auto-provisioning" set FALSE.	No	TRUE/FALSE

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	modifiable	Description
central-wavelength	Float	All MCH services	Yes, only if "auto-provisioning" set FALSE.	No	Values range: 1528.773 To :1566.723
containing-mchg	String	All MCH services	No	No	MCH Group service id, this will take as group for the currently creating MCH service

1.41.1.18 *Service Order Data – SR-TE*

See schema restconf-sai-sr-te.xsd for more details.

service-order-data - Order Data SR-TE Service Service Configuration				
Data	**Type**	**Mandatory**	**Modifiable**	**Description**
service-template	String	No	Yes	The template to be associated with the service.
customer-ref	FDN	No	Yes	Customer FDN e.g. MD=CISCO_EPNM!CUSTOMER=Infrastructure
service-name	String	Yes	No	A unique name for the service.
service-type	String	Yes	No	The type of service. e.g. sr-te
service-description	String	No	Yes	A unique description about the service.
service-activate	Boolean	No	Yes	Boolean flag to indicate if service to be activated or not.
deploy-action	String	No	No	This is the input parameter using which user can specify if service provisioning request need to be run in preview, deploy mode or should be saved or scheduled for future. Possible values: Preview , Deploy , Later , Scheduled Default value: Deploy
deploy-schedule-time	Date	No	No	This tag is to specify deploy schedule time and applicable only when value of deploy-action is "Scheduled". Supported format : yyyy-MM-ddThh:mm:ss-TZD e.g. 2018-10-25T09:10:00-00:00
sr-data	Container	Yes	N/A	Container to specify SR policy related input tags.
policy-name	String	Yes	No	A unique name for the SR Policy.

headend-device-ref	String	Yes	No	Source end device FDN e.g., MD=CISCO_EPNM!ND=<deviceName>
color	String	Yes	No	Indicates color attribute associated to headend-device-ref Allowed range: 1 to 4294967295 If user don't pass its value in the payload then it is fetched from resource pool maintained by EPNM.
endpoint-device-ref	String	Yes	No	SINK end device FDN e.g., MD=CISCO_EPNM!ND=<deviceName>
delete-unused-segment-list	Boolean	NO	No	Boolean flag to indicate if un used segment list should be removed or not during SR Policy Amend and terminate operations Default value: false
binding-sid				Binding SID value Allowed range: 16 to 1048575
candidate-path-list	Container	Yes	N/A	Container to specify candidate path list related input attributes
bandwidth	String	No	Yes	Bandwidth value for candidate path Allowed range: 1 to 4294967295 kbps **Note**: NBI support this value in Kpbs unit only, if user want to specify Mbps or Gbps, then they need to convert it in Kbps and specify converted value in the input payload.
preference	String	Yes	Yes	Input tag to specify preference for candidate path. Allowed range: 1 to 65535
autoroute-settings	Container	No	N/A	Container to specify auto route settings details.
autoroute-metric-mode	Enum	No	Yes	Tag to specify auto route metric mode Allowed values: constant, relative
autoroute-metric	String	No	Yes	Tag to specify auto route metric value For autoroute-metric-mode = constant Allowed range: 1 to 2147483647 For autoroute-metric-mode = relative Allowed range: -10 to 10
allow-all-prefixes	Boolean	No	Yes	Boolean flag to indicate if all prefixes should be allowed or not. Possible value: true/false Default value: true
ip-prefix-list	List container	Yes , if allow-all-prefixes = false	N/A	List container to specify list of ip-prefix values
ip-prefix	String	Yes	Yes	Tag to specify ip prefix value Allowed format: <ip>/24 e.g., 192.168.1.1/24
affinity-operations	Container	No	N/A	Container to specify affinity operations related inputs
affinity-operation	Enum	No	Yes	Input tag to indicate affinity operation value Possible values: exclude-any, include-any,

				include-all
affinity-name	List Container	No	N/A	Container to specify affinity name details It can have multiple name and bit-position values.
name	String	No	Yes	Name to Exclude/Include Affinity in Path Constraints These names are usually existing names.
bit-position	String	No	Yes	Bit Position for Affinity Name in Path Constraints
path-type	Enum	Yes	Yes	Input tag to indicate candidate path value Possible values: explicit, dynamic, dynamic-pce.
explicit	Container	Yes, if path-type= EXPLICIT	Yes	Container to specify explicit path related input tags.
new-segment-list	Boolean	No	Yes	Flag to indicate if segment list is new or existing Possible values: true/false
segment-list-name	String	Yes	Yes	Segment List Name for Path Details
weight	String	Yes	Yes	Input tag to specify explicit path weight Allowed range : 1 to 4294967295
sid-list	Container	Yes, if path-type= EXPLICIT	Yes	Container to specify SID related inputs
id	String	Yes	Yes	Index of Segment
device-ref	String	Yes	Yes	Device Reference of Segment e.g., MD=CISCO_EPNM!ND=<deviceName>
segment-type	Enum	Yes	Yes	Input tag to specify segment type Possible values: node-sid, adjacency-sid
interface	Container	Yes	Yes	Container to specify interface value
name	String	Yes	Yes	Input tag to specify input tag name e.g., Loopback0 this value is for device name mentioned in device-ref
label	String	Yes	Yes	Input tag to specify value of label Value for this field is calculated based on device-ref, interface and name field values.
dynamic	Container	Yes, if path-type= DYNAMIC	Yes	Container to specify dynamic path related inputs
metric-type	Enum	Yes	Yes	Input tag to specify metric type Possible values: igp, latency, te, hop-count
metric-margin-type	Enum	No	Yes	Metric Margin Type for Path Details Possible values: absolute, relative
metric-margin-value	String	No	Yes	Metric Margin Value for Path Details. Allowed range: 0 to 2147483647
max-sid-limit	String	No	Yes	Max SID Limit for Path Details Allowed range: 1 to 255

dynamic-pce	Container	Yes, if path-type= DYNAMIC_WITH_PCE	Yes	Container to specify dynamic with PCE path related inputs
metric-type	Enum	Yes	Yes	Input tag to specify metric type Possible values: igp, latency, te, hop-count
metric-margin-type	Enum	No	Yes	Metric Margin Type for Path Details Possible values: absolute, relative
metric-margin-value	String	No	Yes	Metric Margin Value for Path Details. Allowed range: 0 to 2147483647
max-sid-limit	String	No	Yes	Max SID Limit for Path Details Allowed range: 1 to 255
path-constraints-details	Container	No	N/A	Container to specify path constraints details related input tags.
sid-algorithm	String	No	Yes	Input tag to specify sid-algorithm value Allowed range: 128 to 255
disjoint-group-type	Enum	No	Yes	Input tag to specify disjoint-group-type values. Possible values: link, node, srlg, srlg-node.
disjoint-group-id	String	No	Yes	Input tag to specify disjoint-group-id value.
disjoint-sub-group-id	String	No	Yes	Input tag to specify disjoint-sub-group-id value.

Templates Support

The following sub-sections provide the details of service provisioning with template support in the order which is required in the provision and modify operations of the service activation interface as a POST data in a request object.

The table below lists the Template Order Data elements and the supported values for any service.

Template Order Data	Data Type	Applicable to Service Type	Description
service-templates		All	Container for Templates service configuration.
service-template		All	Container for Template service configuration.
type	template-type-enum-type	All	Type. Possible value: preconfig , postconfig
name	String	All	Template name.
usage	String	All	Template Usage. Eg: Service Create Only Service Create Modify Service Create Delete Service Create Modify Delete Service Modify Only Service Delete Only
variables		All	Container for Variables configuration.
variable		All	Container for Variable configuration.
name	String	All	Name of the template for NBI request. You can give any name e.g., xyz
value	String	All	Name of the created template that you want to use in your NBI input request.

Template Order Data	Data Type	Applicable to Service Type	Description
Required	String	All	To indicate if it's required or not. Possible values "Yes" or "No"
Description	String		Variable Description.

1.41.1.19 Template Request Example

POST /restconf/operations/v1/cisco-service-provision:provision-service HTTP/1.1
Host: <epnm-host>
Content Type: application/yang.operation+xml

- samples/Template_Request_Example/request.xml

Service Performance Test Support

The following sections provide the details of service performance test support.
The Service Performance Test can be conducted standalone as well as part of service provisioning.

1.41.1.20 *Standalone Service Performance Test Execution*

Restconf NBI supports standalone performance test execution.

Operation	Description
service-oam-config	This operation is to run service performance test, including BERT, Y1564 and Y1731 performance test.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam:service-oam-config
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **service-oam-config** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return response of type **service-oam-results** that contains the information of the service performance test which can be used to retrieve the service performance test result.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam.yang

1.41.1.20.1 Request for BERT

Name	Type	Description
service-oam-config	Container element	Holds service test config data
bert-config	Container element	Holds bert test config data
service-ref	String (FDN)	CFS fdn
source-tp-ref	String (FDN)	source tp fdn

destination-tp-ref	String (FDN)	destination tp fdn
unmanaged-destination	String	the destination is unmanaged or not: true or false
Direction	String	test traffic direction: system or line
Errors	String	Inject Errors, value range 0 to 255
Duration	String	Test duration time in minutes, value between 1 to 14400
Pattern	String	BERT pattern, valid value: 0s, 1s, 2^9, 2^11, 2^15, 2^23, 2^31, 2^20-O151, 2^20-O153

1.41.1.20.2   Request for Y1564

Name	Type	Description
service-oam-config	Container element	Holds service test config data
Y1564-test-config	Container element	Holds Y1564 test config data
service-ref	String (FDN)	CFS fdn
source-tp-ref	String (FDN)	source tp fdn
destination-tp-ref	String (FDN)	destination tp fdn
is-one-way	Boolean	is one way test flag
Duration	Int	Time duration for traffic generation in secs.
is-custom-rates	Boolean	mode selection • When is-custom-rates = true, attribute *rates* should be used • When is-custom-rates = false, attributes *eir-rate* / *cir-rate* should be used
Rates	String	Bytes to send in kbps. Ex: 1000 kbps
eir-rate	Int	EIR rate value in kbps
cir-rate	Int	CIR rate value in kbps
is-step-load-cir	Boolean	In mode of CIR/EIR, points if requires additional 3 rates for 25% 50% and 75% from CIR value
packet-size	Int	Packet size in bytes
ip-type	String	Possible Values: IPv4, IPv6
inner-tag	Container element	Holds inner vlan data
vlan-id	String	Vlan id. Allowed Values: 1 to 4094
outer-tag	Container element	Holds outer vlan data
vlan-id	String	Vlan id. Allowed Values: 1 to 4094
acceptable-flr	Int	Acceptance criteria for Frame Lost
acceptable-ftd	Int	Acceptance criteria for Delay
acceptable-fdv	Int	Acceptance criteria for Jitter

is-unmanaged-me3600	Boolean	In case of unmanaged destination, points if type of unmanaged device is ME3600

1.41.1.20.3   Request for Y1731

Name	Type	Description
service-oam-config	Container element	Holds service test config data
Y1731-test-config	Container element	Holds Y1731 test config data
service-ref	String (FDN)	CFS fdn
source-tp-ref	String (FDN)	source tp fdn
destination-tp-ref	String (FDN)	destination tp fdn
is-loss-required	Boolean	is loss required test flag
is-delay-required	Boolean	is delay required test flag
Cos	String	cos value
probe-length	int	probe length in seconds
burst-interval	int	Burst interval in seconds
packet-count	int	Packet count
packet-size	int	Packet size in bytes
packet-interval	int	Packet interval in milli-secs
Duration	int	Time duration for traffic generation in mins

1.41.1.20.4   Request for MPLS LSP Ping and Traceroute

Name	Type	Description
service-oam-config	Container element	Holds service test config data
mpls-lsp-ping-config	Container element	Holds LSP Ping test config data
service-ref	String (FDN)	CFS fdn
source-tp-ref	String (FDN)	source tp fdn
destination-tp-ref	String (FDN)	destination tp fdn

1.41.1.20.5   Response

Name	Type	Description
service-oam-results	Container element	Holds the data for response of template execution.
request-id	String	request-id which is to get performance test result
service-ref	String	CFS fdn
test-ids	String	test id

1.41.1.20.6   Standalone BERT Test

Request
- POST /restconf/operations/v1/cisco-service-oam:service-oam-config
- samples/Standalone_BERT_Test/request.xml
- samples/Standalone_BERT_Test/request.json

Response
- samples/Standalone_BERT_Test/response.xml

1.41.1.20.7   Standalone Y1564 Test

Request

- POST /restconf/operations/v1/cisco-service-oam:service-oam-config
- samples/Standalone_Y1564_Test/request.xml
- samples/Standalone_Y1564_Test/request.json
- samples/Standalone_Y1564_Test/request_custom_rate_true.json
- samples/Standalone_Y1564_Test/request_custom_rate_false.json

Response

- GET /restconf/operations/v1/cisco-service-oam:service-oam-config/<request-id>
- samples/Standalone_Y1564_Test/response.json
- samples/Standalone_Y1564_Test/response_custom_rate_true.json
- samples/Standalone_Y1564_Test/response_custom_rate_false.json

1.41.1.20.8   Standalone Y1731 Test

Request

- POST /restconf/operations/v1/cisco-service-oam:service-oam-config
- samples/Standalone_Y1731_Test/request.xml
- samples/Standalone_Y1731_Test/request.json

Response
- samples/Standalone_Y1731_Test/response.json

1.41.1.20.9   MPLS LSP Ping

Operation	Description
service-oam-config	This operation is to run mpls lsp ping test for CE & L3VPN services.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam:service-oam-config
Request Message	
Request Content Type	application/xml, application/yang.operation +xml
Request Data	Request data of type **service-oam-config** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of tunnel-te ping operation with request-id.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam.yang

Request

Name	Type	Description
service-oam-config	Container element	Holds service LSP ping test config data
mpls-lsp-ping-config	Container element	Holds mpls-lsp-ping-config data
service-ref	String (FDN)	CFS fdn
source-tp-ref	String(FDN)	Source tp-ref FDN
destination-tp-ref	String(FDN)	Destination tp-ref FDN
service-state-role	String	Service state role , it's an optional input. Possible values : Active , Protected

Response

Name	Type	Description
request-id	Integer	Holds integer value which is used to get the tunnel-te ping response.
service-ref	String (FDN)	CFS fdn
test-ids	Long	Uniquely generated test-id for each request e.g. 1001 , 1002 ,….

Request

- POST /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
- samples/LSP_Ping/request.xml
- samples/LSP_Ping/request.json

Response

- samples/LSP_Ping/response.json

1.41.1.20.10   MPLS LSP traceroute

Operation	Description
service-oam-config	This operation is to run mpls lsp ping test for CE & L3VPN services.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam:service-oam-config
Request Message	
Request Content Type	application/xml, application/yang.operation +xml
Request Data	Request data of type **service-oam-config** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of tunnel-te ping operation with request-id.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.

Yang file name	cisco-service-oam.yang

Request

Name	Type	Description
service-oam-config	Container element	Holds service LSP ping test config data
mpls-lsp-traceroute-config	Container element	Holds mpls-lsp-ping-config data
service-ref	String (FDN)	CFS fdn
source-tp-ref	String(FDN)	Source tp-ref FDN
destination-tp-ref	String(FDN)	Destination tp-ref FDN
service-state-role	String	Service state role , it's an optional input. Possible values : Active , Protected

Response

Name	Type	Description
request-id	Integer	Holds integer value which is used to get the tunnel-te ping response.
service-ref	String (FDN)	CFS fdn
test-ids	Long	Uniquely generated test-id for each request e.g. 1001 , 1002 ,….

Request

- POST /restconf/operations/v1/cisco-service-oam:service-oam-config
- samples/LSP_Traceroute/request.xml
- samples/LSP_Traceroute/request.json

Response

- samples/LSP_Traceroute/response.json

Note: LSP ping and traceroute service test is applicable for those CE and CEM services which is not passing through unidirectional/bidirectional tunnels.

1.41.1.20.11   Tunnel-TE Ping

Operation	Description
service-oam-config	This operation is to run tunnel-te (Uni-directional Tunnel)Ping
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of tunnel-te ping operation with request-id.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors.

	• 400 Bad Request - Invalid request message.
	• 500 Internal Server Error - operation-failed.
	Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config-ext	Container element	Holds service test config data
tunnel-te-ping	Container element	Holds tunnel-te ping config data
service-ref	String (FDN)	CFS fdn

Response

Name	Type	Description
request-id	Integer	Holds integer value which is used to get the tunnel-te ping response.
service-ref	String (FDN)	CFS fdn

Request

- POST /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
- Samples/OAM_Ping_And_Traceroute/Tunnel-TE-Ping/request.xml

Response

- Samples/OAM_Ping_And_Traceroute/Tunnel-TE-Ping/response.xml

1.41.1.20.12   Tunnel-TE TraceRoute

Operation	Description
service-oam-config	This operation is to run tunnel-te(Uni-directional Tunnel) Traceroute
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of tunnel-te traceroute operation with request-id.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config-ext	Container element	Holds service test config data
tunnel-te-traceroute	Container element	Holds tunnel-te traceroute config data
service-ref	String (FDN)	CFS fdn

Response

Name	Type	Description
request-id	Integer	Holds integer value which is used to get the tunnel-te traceroute response.
service-ref	String (FDN)	CFS fdn

Request

- POST /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
- samples/OAM_Ping_And_Traceroute/Tunnel-TE-Traceroute/request.xml

Response

- samples/OAM_Ping_And_Traceroute/Tunnel-TE-Traceroute/response.xml

1.41.1.20.13   Flex Ping

Operation	Description
service-oam-config	This operation is to run Flex (Bi-directional tunnel)Ping
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of flex ping operation with request-id.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config-ext	Container element	Holds service test config data
flex-ping	Container element	Holds Flex ping config data
service-ref	String (FDN)	CFS fdn
service-state-role	String	Holds path either (active, protected or working)

Response

Name	Type	Description
request-id	Integer	Holds integer value which is used to get the flex ping response.
service-ref	String (FDN)	CFS fdn

Request

- POST /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
- samples/OAM_Ping_And_Traceroute/Flex-Ping/request.xml

Response

- samples/OAM_Ping_And_Traceroute/Flex-Ping/response.xml

1.41.1.20.14   Flex Traceroute

Operation	Description
service-oam-config	This operation is to run Flex(Bi-directional tunnel) Traceroute
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of flex traceroute operation with request-id.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config-ext	Container element	Holds service test config data
flex-traceroute	Container element	Holds Flex traceroute config data
service-ref	String (FDN)	CFS fdn
service-state-role	String	Holds path either (active, protected or working)

Response

Name	Type	Description
request-id	Integer	Holds integer value which is used to get the flex traceroute response.
service-ref	String (FDN)	CFS fdn

Request

- POST /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
- samples/OAM_Ping_And_Traceroute/Flex-Traceroute/request.xml

Response

- samples/OAM_Ping_And_Traceroute/Flex-Traceroute/response.xml

1.41.1.20.15   PW Ping and Traceroute

Operation	Description
service-oam-config-ext	This operation is to run PW ping and Traceroute
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return response of type **service-oam-results** that contains the information of the service performance test which can be used to retrieve the service performance test result.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config-ext	Container element	Holds service test config data
pw-ping	Container element	Holds PW ping config data
service-ref	String (FDN)	CFS fdn
service-state-role	Enum	Values supported • active • protected
from-tp-ref	String (FDN)	source tp fdn

Response

Name	Type	Description
service-oam-results	Container element	Holds the data for response of template execution.

request-id	String	request-id which is to get performance test result
service-ref	String	CFS fdn

Note: PW ping and traceroute service test is applicable for CE and CEM services. For EVPN based CE services it's not applicable.

Request

- POST /restconf/operations/v1/cisco-service-oam:service-oam-config-ext
- samples/PW_Ping_and_Traceroute/request.xml
- samples/PW_Ping_and_Traceroute/request.json
- samples/PW_Ping_and_Traceroute/request.2.xml
- samples/PW_Ping_and_Traceroute/request.2.json
- samples/PW_Ping_and_Traceroute/Pw-ping-with-endpoints-request.json
- samples/PW_Ping_and_Traceroute/Pw-traceroute-with-endpoints-request.json

Response

- samples/PW_Ping_and_Traceroute/response.xml
- samples/PW_Ping_and_Traceroute/response.2.json
- samples/PW_Ping_and_Traceroute/Pw-ping-with-endpoints-response.json
- samples/PW_Ping_and_Traceroute/Pw-traceroute-with-endpoints-response.json

1.41.1.20.16   CFM Ping

Operation	Description
service-oam-config-ext	This operation is to run CFM Ping
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return response of type **service-oam-results** that contains the information of the service performance test which can be used to retrieve the service performance test result.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config-ext	Container element	Holds service test config data
cfm-ping	Container element	Holds CFM-Ping config data
service-ref	String (FDN)	CFS fdn
service-state-role	Enum	Values supported • active • protected
from-tp-ref	String (FDN)	source tp fdn
to-tp-ref	String (FDN)	destination tp fdn

Response

Name	Type	Description
service-oam-results	Container element	Holds the data for response of template execution.
request-id	String	request-id which is to get performance test result
service-ref	String	CFS fdn

Request

- POST /restconf/operations/v1/cisco-service-oam:service-oam-config-ext
- samples/CFM_Ping/request.xml
- samples/CFM_Ping/request.json
- samples/CFM_Ping/Cfm-ping-with-endpoints-request.xml

Response

- samples/CFM_Ping/response.json
- samples/CFM_Ping/Cfm-ping-with-endpoints-response.xml

1.41.1.20.17   CFM Traceroute

Operation	Description
service-oam-config-ext	This operation is to run CFM Traceroute
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return response of type **service-oam-results** that contains the information of the service performance test which can be used to retrieve the service performance test result.
HTTP Status Code	• 200 OK - Success with response message-body

	• 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config-ext	Container element	Holds service test config data
cfm-traceroute	Container element	Holds CFM Traceroute config data
service-ref	String (FDN)	CFS fdn
service-state-role	Enum	Values supported • active • protected
from-tp-ref	String (FDN)	source tp fdn
to-tp-ref	String (FDN)	destination tp fdn

Response

Name	Type	Description
service-oam-results	Container element	Holds the data for response of template execution.
request-id	String	request-id which is to get performance test result
service-ref	String	CFS fdn

1.41.1.20.18   BERT Test on Single Controller

Operation	Description
service-oam-config-ext	This operation is to run BERT test on single TDM Interface
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **service-oam-config-ext** that contains the details of the service performance test.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return response of type **service-oam-results** that contains the information of the service performance test which can be used to retrieve the service performance test result.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.

Yang file name	cisco-service-oam-ext.yang

Request

Name	Type	Description
service-oam-config	Container element	Holds service test config data
bert-sc	Container element	Holds bert test config data
tp-ref	String (FDN)	TDM interface in FDN format
loopback	String	Supported loopback on the TDM controller being used for test. e.g., `use-configured-loopback-on-remote-side, use-remote-loopback-locally`
Duration	String	Test duration time in minutes, value between 1 to 14400
Pattern	String	BERT SC pattern, valid value: 2^9, 2^11, 2^15, 2^23, 2^31, 2^20-O151, 2^20-O153 There can be diffrence in supported values from controller to controller .

Response

Name	Type	Description
service-oam-results	Container element	Holds the data for response of template execution.
request-id	String	request-id which is to get BERT SC test result

Request
- POST /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext
- samples/BERT_SC/request.json

Response
- samples/BERT_SC/response.json

1.41.1.21 *Standalone Service Performance Test Retrieval*

This API retrieves standalone service performance test result in Cisco EPN Manager.

Resource	Description	
	Retrieves standalone service performance test result in Cisco EPN Manager.	
HTTP Method	**Resource Path**	
GET	/restconf/operations/v1/cisco-service-oam:service-oam-config/{request-id}	
Path Parameters		
Name	**Type**	**Description**
request-id	String	The request-id which in the response of standalone service performance test execution. Given this, the performance test result will be returned.
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or 1 **service-oam-results** – see yang model for the data details.	

HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam.yang

1.41.1.21.1 GET Test Result for BERT

Request
- GET /restconf/operations/v1/cisco-service-oam:service-oam-config/bert-config$4250249

Response
- samples/GET_Test_Result_for_BERT/response.json

1.41.1.21.2 GET Test Result for Y1564

Request
- GET /restconf/operations/v1/cisco-service-oam:service-oam-config/y1564-test-config$154136052$15413605

Response
- samples/GET_Test_Result_for_Y1564/response.json

1.41.1.21.3 GET Test Result for Y1564

Request
- GET /restconf/operations/v1/cisco-service-oam:service-oam-config/y1731-test-config$154136052$15413605

Response
- samples/GET_Test_Result_for_Y1731/response.json

1.41.1.21.4 LSP Ping and Trace – GET Ping Details

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/mpls-lsp-ping/<request-id>?check-ready=true

Response
- samples/LSP_Ping_And_Trace_GET_Ping_Details/lsp-ping-response.xml

1.41.1.21.5 GET LSP Traceroute Details

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/mpls-lsp-trace-route/<test-id>?check-ready=true

Response
- samples/LSP_Ping_And_Trace_GET_Ping_Details/lsp-traceroute-response.xml

1.41.1.21.6   GET PW Ping and Traceroute

Resource	Description	
	Retrieves standalone service performance test result in Cisco EPN Manager.	
HTTP Method	**Resource Path**	
GET	/restconf/operations/v1/cisco-service-oam:service-oam-config-ext/{request-id}	
Path Parameters		
Name	**Type**	**Description**
request-id	String	The request-id which in the response of standalone service performance test execution. Given this, the performance test result will be returned.
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or 1 **service-oam-results** – see yang model for the data details.	
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Yang file name	cisco-service-oam-ext.yang	

Request

- GET /restconf/operations/v1/cisco-service-oam:service-oam-config-ext/pw-ping/<request-id>
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/pw-trace-route/<request-id>

Response

- samples/GET_PW_Ping_and_Traceroute/response.xml
- samples/GET_PW_Ping_and_Traceroute/response.2.xml
- samples/GET_PW_Ping_and_Traceroute/Pw-ping-with-endpoints-get-response.json
- [samples/GET_PW_Ping_and_Traceroute /Pw-traceroute-with-endpoints-get-response.json](samples/GET_PW_Ping_and_Traceroute/Pw-traceroute-with-endpoints-get-response.json)

1.41.1.21.7   GET CFM Ping

Request

- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/cfm-ping/<request-id>

Response

- samples/GET_CFM_Ping/response.xml
- samples/GET_CFM_Ping/Cfm-ping-with-endpoints-get-response.xml

1.41.1.21.8   GET CFM Traceroute

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/cfm-traceroute/<request-id>

Response
- samples/CFM_Traceroute/response.json
- samples/CFM_Traceroute /Cfm-traceroute-with-endpoints-get-response.xml

1.41.1.21.9   GET Tunnel-TE - Ping

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/tunnel-te-ping/<test-id>

Response
- samples/Tunnel_TE_GET_Ping_Details/response.xml

1.41.1.21.10   GET Tunnel-TE – Traceroute

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/tunnel-te-trace-route/<test-id>

Response
- samples/Tunnel_TE_GET_Traceroute_Details/response.xml

1.41.1.21.11   GET Flex –Ping

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/flex-ping/<test-id>

Response
- samples/Flex_GET_Ping_Details/response.xml

1.41.1.21.12   GET Flex –Traceroute

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/flex-trace-route/<test-id>

Response
- samples/Flex_GET_Traceroute_Details/response.xml

1.41.1.21.13   GET BERT SC Response

Request

- GET /restconf/operations/v1/cisco-service-oam:service-oam-config?request-id=bert-sc$2015013$1714043

Response

- samples/BERT_SC/getResponse.xml

1.41.1.21.14   Device OAM Ping and Trace

This interface helps the user to perform ping and traceroute operation from server to managed device and one managed device to another managed device and get the operation output.

Device Ping (Operation from Server to Managed Device)

Operation	Description
service-oam-config	This operation is to perform ping and get the output
HTTP Method	**Resource Path**
GET	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/device-ping?nodeFdn=<nodeFdn-value>
Authorization Required	One or more from following - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of **device-oam-results**
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Device Trace Operation (Operation from Server to Managed Device)

Operation	Description
service-oam-config	This operation is to perform traceroute and get the output
HTTP Method	**Resource Path**
GET	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/device-traceroute?nodeFdn=<nodeFdn-value>
Authorization Required	One or more from following - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml

Response Data	Return response of **device-oam-results**
HTTP Status Code	• 200 OK - Success with response message-body
	• 401, 403 – Authentication and Authorization errors.
	• 400 Bad Request - Invalid request message.
	• 500 Internal Server Error - operation-failed.
	Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Device to Device Ping (Operation from Managed Device to Managed Device)

Operation	Description
service-oam-config	This operation is to perform ping and get the output
HTTP Method	**Resource Path**
GET	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/device-to-device-ping?nodeFdn=<nodeFdn-value>&targetIP=<IPAddress>&sourceIP=<IPAddress> Mandatory Parameter: nodeFdn and targetIP Optional Parameter: sourceIP nodeFdn - Managed Device Name from where the operation starts targetIP - Managed device IP where the operation ends sourceIP- IP address of out-going interface in which path the operation should leave from source device to reach target device.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of **device-oam-results**
HTTP Status Code	• 200 OK - Success with response message-body
	• 401, 403 – Authentication and Authorization errors.
	• 400 Bad Request - Invalid request message.
	• 500 Internal Server Error - operation-failed.
	Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Device to Device Traceroute (Operation from Managed Device to Managed Device)

Operation	Description
service-oam-config	This operation is to perform traceroute and get the output
HTTP Method	**Resource Path**
GET	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/device-to-device-traceroute?nodeFdn=<nodeFdn-value>&targetIP=<IPAddress>&sourceIP=<IPAddress> Mandatory Parameter: nodeFdn and targetIP Optional Parameter: sourceIP

	nodeFdn - Managed Device Name from where the operation starts targetIP - Managed device IP where the operation ends sourceIP - IP address of out-going interface in which path the operation should leave from source device to reach target device.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Message	
Response Content Type	application/xml, application/yang.operation +xml
Response Data	Return response of **device-oam-results**
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang

Request

- GET /restconf/operations/v1/cisco-service-oam:service-oam-config-ext/device-ping?nodeFdn=<nodeFdn-value>
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/device-traceroute?nodeFdn=<nodeFdn-value>

- GET /restconf/operations/v1/cisco-service-oam:service-oam-config-ext/device-to-device-ping?nodeFdn=<nodeFdn-value>&targetIP=<IPAddress>
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/device-to-device-traceroute?nodeFdn=<nodeFdn-value>&targetIP=<IPAddress>

Response

- samples/GET_Device_Ping/response.xml
- samples/GET_Device_Traceroute/response.xml
- samples/GET_Device_Ping/Device-ping-with-endpoints-get-response.json
- samples/GET_Device_Traceroute /Device-traceroute-get-response.json

- samples/GET_Device_to_Device_Ping/response.xml
- samples/GET_Device_to_Device_Traceroute/response.xml
- samples/GET_Device_to_Device_Ping/Device-to-Device-ping-with-endpoints-get-response.json
- samples/GET_Device_to-Device_Traceroute /Device-to-Device-traceroute-get-response.json

1.41.1.21.15   VRF Ping and Trace

This interface helps the user to perform VRF ping and traceroute operation from server to managed device, Vrf , endpoint associated to VRF and get the operation output.

VRF Ping

Resource	Description
Service Profile	Retrieves all Service Profiles added in Cisco EPN Manager.
HTTP Method	**Resource Path**
GET	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/vrf-ping?sourceNodeManagedAddress=<device_ip>&vrfName=l3vpn-nbi-1&targetEndPointIP=<endpoint_ip>
Query Parameters		

Name	Type	Description
sourceNodeManagedAddress	String	Source Managed device IP address Example: sourceNodeManagedAddress=1.1.1.1
vrfName	String	VRF Name for which the ping or trace being initiated. Example: vrfName=vrf_name
targetEndPointIP	String	Target endpoint associated with the provide VRF. Example: targetEndPointIP=2.2.2.2

Authorization Required	One or more from following. • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting
Response Content Type	
Response Data	Return response of **device-oam-results**
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-service-oam-ext.yang
Response Content Type	application/xml, application/yang.operation +xml

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/vrf-ping?sourceNodeManagedAddress=<device_ip>&vrfName=l3vpn-nbi-1&targetEndPointIP=<endpoint_ip>

Response
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<vrf-oam-results xmlns="urn:cisco:params:xml:ns:yang:service:oam:ext:v1">
<vrf-ping>
<raw-output>ping vrf l3vpn-nbi-1 2.3.11.1

&#13;Thu Oct 20 04:48:52.036 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.3.11.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
</raw-output>
</vrf-ping>
</vrf-oam-results>
```

VRF TraceRoute

Resource	Description	
Service Profile	Retrieves all Service Profiles added in Cisco EPN Manager.	
HTTP Method	**Resource Path**	
GET	/restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/vrf-traceroute?sourceNodeManagedAddress=<device_ip>&sourceNodeFdn=<device_fdn>&vrfName=<vrf_name>&targetEndPointIP=<endpoint_ip>	
Query Parameters		
Name	**Type**	**Description**
sourceNodeManagedAddress	String	Source Managed device IP address Example: sourceNodeManagedAddress=1.1.1.1
vrfName	String	VRF Name for which the ping or trace being initiated. Example: vrfName=vrf_name
sourceNodeFdn	String	Source Node Fdn Example: MD=CISCO_EPNM!ND=ASR9006-SR-71
targetEndPointIP	String	Target endpoint associated with the provide VRF. Example: targetEndPointIP=2.2.2.2
Authorization Required	One or more from following. • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting	
Response Content Type		
Response Data	Return response of **device-oam-results**	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Yang file name	cisco-service-oam-ext.yang	
Response Content Type	application/xml, application/yang.operation +xml	

Request
- GET /restconf/operations/v1/cisco-service-oam-ext:service-oam-config-ext/vrf-traceroute?sourceNodeManagedAddress=<device_ip>&sourceNodeFdn=<device_fdn>&vrfName=<vrf_name>&targetEndPointIP=<endpoint_ip>

Response
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<vrf-oam-results xmlns="urn:cisco:params:xml:ns:yang:service:oam:ext:v1">
<vrf-traceroute>
<raw-output>traceroute vrf l3vpn-nbi-1 2.3.11.1

Thu Oct 20 05:02:08.764 UTC

Type escape sequence to abort.
Tracing the route to 2.3.11.1

```
1 192.168.1.9 4 msec * 4 msec
</raw-output>
</vrf-traceroute>
</vrf-oam-results>
```

Consolidated Provisioning Support

The consolidated provisioning is supported in Cisco EPN Manager service activation. In one provision request, user can do the following 3 tasks together:

- Provisioning MPLS TE tunnel, providing <mpls-te-data>
- Provisioning CE or CEM, providing <ce-data> or <cem-data>
- Executing service performance test, providing < service-oam-config>

The following scenario are supported:

- mpls-te, ce, Y1731
- mpls-te, ce, Y1564
- mpls-te, cem, BERT

Each service-order-data sub-section such as mpls-te, ce, cem are the same as when those used in non-consolidated fashion.

Please find consolidated provisioning example in chapter 7.

Service Profile Support

Service Profiles contain pre-defined provisioning request (order data) that can be used in provisioning each circuit/VC type.

In NBI Provisioning request, a service profile reference can be used to get provisioning request data to be used in the provisioning. If the provisioning data is provided in the request along with the service profile reference, but the user provided data and the data stored in the service profile gets merged with user provided data overriding the profile data before the request is sent to execute provisioning.

Service profile can be created using EPNM Service Profile wizard GUI. For more information on how to create the service profile please refer to EPNM User and Administrative Guide under section "Create Circuit/VC Profiles". Typical workflow to use the NBI with service profiles is

1. Create service profile using EPNM Service Profile wizard GUI
2. Retrieve the service profile details using Service Profile Retrieval NBI
3. Use the FDN of the service profile (retrieved from the retrieval NBI) as a service profile reference in the NBI provisioning request.
4. Add any data to NBI provisioning request to override what is there in the service profile
5. Execute provision nbi with service profile reference.

1.41.1.22 *Service Profile Reference*

When using the service profile reference in the NBI service provisioning request, the immune required data that is need is

1. Service type
2. Service subtype
3. Service name

Sample provisioning request with service profile:

- samples/Service_Profile_Reference/request.xml

1.41.1.23 *Service Profile Provision*

Request

- samples/Service_Profile_Provision/request.1.xml
- samples/Service_Profile_Provision/request.1.json
- samples/Service_Profile_Provision/request.2.xml
- samples/Service_Profile_Provision/request.2.json

1.41.1.24 *Service Profile Retrieval*

This API retrieves Service Profiles in Cisco EPN Manager. This API can be used to get the FDN of the Service Profile which can be passed in the service profile reference (as FDN) in service provision request.

Resource	Description	
Service Profile	Retrieves all Service Profiles added in Cisco EPN Manager.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-service-profile:service-profile	
Query Parameters		
Name	**Type**	**Description**
fdn	String (FDN Format)	Fully Distinguished Name (FDN) of the Service Profile. Given this, a corresponding single Service will be returned. FDN: MD=<CISCO_EPNM>!PROFILE_SERVICE=<profilename>.
type	String	Service type for which the service profiles will be retrieved. If not specified all service profiles for all service types will be returned. Possible values: carrier-ethernet-vpn, tdm-cem, mpls-te-tunnel, layer3-link, mpls-l3-vpn,optical
subtype	String	Service subtype for which the of the CFS to retrieve. If not specified all sub types will be returned. Should be used in conjunction with Type.
Authorization Required	One or more from following • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Contains 0 or more Service Profiles of type **service-profile** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Yang file name	cisco-service-profile.yang	

1.41.1.25 *Get All Service Profiles*

Request

- GET /restconf/data/v1/cisco-service-profile:service-profileHTTP

Response

- samples/Get_All_Service_Profiles/response.xml

1.42 Customer CRUD

Customer resource path to create, retrieve, update, and delete Customer values.

Retrieve Customer

Resource	Description
Customer	Customer resource that is used in the provisioning order data. Retrieves the Customer resource.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-customer:customer/{name}
Path Parameters	

Name	Type	Description
Name	String	Customer Name – to retrieve a single customer resource. Without this parameter, all Customers will be retrieved.

Authorization Required	One or more from following • Circuit or VC Provisioning
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more customer resources of type **customer** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0060 = Cannot determine customer id for name %s - multiple customers found with the name. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-customer.yang

1.42.1.1 *Get All Customers*

Request

• GET /restconf/data/v1/cisco-customer:customer

Response

- samples/Get_All_Customers/response.xml

Create Customer

Resource	Description
Customer	Creates a Customer Resource - Customer resource that is used in the provisioning order data.
HTTP Method	**Resource Path**
POST	/restconf/data/v1/cisco-customer:customer/
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **customer** that contains the details of the customer – see yang model for the data details.
Authorization Required	One or more from following • Circuit or VC Provisioning
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	No response if the operation succeeds. Error message is displayed if the operation fails.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0007 = Cannot Create Customer with name = %s - %s • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-customer.yang

Request

- samples/Create_Customer/request.xml
- samples/Create_Customer/request.json

Update Customer

Resource	Description
Customer	Update the customer - Customer resource that is used in the provisioning order data.
HTTP Method	**Resource Path**
PUT	/restconf/data/v1/cisco-customer:customer/{name}
Path Parameters	
Name	**Type**	**Description**

Name	String	Name of the customer which will be updated.
Request Message		
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json	
Request Data	Request data of type **customer** that contains the details of the customer – see yang model for the data details.	
Authorization Required	One or more from following • Circuit or VC Provisioning	
Response Message		
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json	
Response Data	No response if the operation succeeds. Error messages is displayed if the operation fails.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number> - any tag starting with "FW." prefix for any internal errors like FW.0009=Cannot Update Customer with name = %s - %s • CORE.\<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-customer.yang	

Request

- samples/Update_Customer/request.xml
- samples/Update_Customer/request.json

Delete Customer

Resource	Description
Customer	Deletes the Customer - Customer resource that is used in the provisioning order data.
HTTP Method	**Resource Path**
DELETE	/restconf/data/v1/cisco-customer:customer/{name}
Path Parameters	
Name	**Type**	**Description**
Name	String	Name of the customer for the delete operation.
Authorization Required	One or more from following • Circuit or VC Provisioning	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Error response or no data	
HTTP Status Code	• 200 OK - Success with response message-body	

	• 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0010=Cannot Delete Customer with name = %s - %s • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-customer.yang

Request

- PUT /restconf/data/v1/cisco-customer:customer/MyCustomer

Response

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+xml

1.43 Resource Activation

RESTCONF NBI supports the setting up of the resource level configuration using various operations like Termination Point Configuration, Template Based Configuration (TBC), and Model Based Configuration (MBC). The operations listed below are supported as part of Resource Activation.

Operations

1.43.1.1 *CLI Configuration Execution*

Restconf NBI supports configuration using CLI Templates. Invoking this NBI will run the CLI Configuration in the template on the target device with the set of parameters applied.

Operation	Description
run-cli-configuration	This operation can be used to run cli configuration using templates.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:run-cli-configuration
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type run-cli-configuration that contains the details of the template to run.
Authorization Required	One or more from following • Configure Templates • View Job
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return response of type config-response that contains the details of the job

	executing the cli configuration which can be used to check the status.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format RA.<number> are generated by this API. For example: RA.0088 for 'Error occurred in MBC config service creation - [%s], transcript - [%s]' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-resource-activation.yang

1.43.1.1.1 Run CLI Configuration Request

Name	Type	Description
run-cli-configuration	Container element	Holds the data for template details.
template-name	String	Template Name of which the CLI template to be configured on devices.
last-job-name	String	Last failed job name for which template execution need to be retried.
is-retry	Boolean	Boolean flag to indicate if template execution needs to be retried or not. Default: false
target-list	List	List of device target of which the CLI template to be deployed.
Target	Container element	Holds the target deploy information including device and corresponding configuration parameters
node-ref	String (FDN)	FDN of the device where the cli from the template gets executed.
parameter-list	List	List of name/value pairs for the parameters for the template.
Name	String	Name of the parameter.
Value	String	Value of the parameter.

1.43.1.1.2 Run CLI Configuration Response

Name	Type	Description
config-response	Container element	Holds the data for response of template execution.
job-name	String	Name of the job executing the template – can be used to check the status.
Message	String	A message from job execution.

1.43.1.1.3 Run CLI Template

Request
- POST /restconf/operations/v1/cisco-resource-activation:run-cli-configuration
- samples/Run_CLI_Template/request.xml

Response
- samples/Run_CLI_Template/response.xml

1.43.1.1.4 Run CLI Template with retry

Request
- POST /restconf/operations/v1/cisco-resource-activation:run-cli-configuration
- samples/Run_cli_template_with_retry/request.xml
- samples/Run_cli_template_with_retry/request.json

Response
- samples/Run_cli_template_with_retry/response.xml
- samples/Run_cli_template_with_retry/response.json

1.43.1.1.5 Resource_Configuration-Create

Resource	Description
Modify Bearer Command (MBC)	Resource configuration create
HTTP Method	**Resource Path**
POST	https://<host>/restconf/operations/v1/cisco-resource-activation:create-config
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	The created **configuration** – see yang model for the data details. And result of modification on the feature.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TP.<number> are generated by this API. For example: TP.0029 for 'Set TerminationPoint Data Operation Failed: %s.' If error is from underlying framework/core modules error-app-tag format one of following

	• FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials

For OSPF with MBC service

Name	Type	Description
routingProcessId	String	Routing Process ID
routerId	String	The Router ID
cost	String	Cost to create
priority	String	Priority of service
maximumPaths	String	Maximum path value
distanceIP	String	Distance IP value
distanceExternal		Distance external value
node-ref	String (FDN)	FDN of the device where the cli from the template gets executed.
entity-name	String	OspfProcessSettings for OSPF

For BGP with MBC service

Name	Type	Description
localAs	String	Local as value
localIdentifier.address	String	Local identifier ip address
logNeighborChanges	String	Log neighbor changes
node-ref	String (FDN)	FDN of the device where the cli from the template gets executed.
feature-name	String	Feature name
entity-name	String	BgpProcessSettings for BGP service

Request
- POST /restconf/ operations/v1/cisco-resource-activation:create-config
- samples/Resource_Configuration_Create/request.xml
- samples/Resource_Configuration_Create/request.json

Response
- samples/Resource_Configuration_Create/response.xml

1.43.1.1.6 Resource_Configuration-Modify

Resource	Description
Modify Bearer Command (MBC)	Modify a service with MBC
HTTP Method	**Resource Path**
POST	https://\<host\>/restconf/operations/v1/cisco-resource-activation:modify-config
Authorization	One or more from following

Required	• Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	The modified **configuration** – see yang model for the data details. And result of modification on the feature.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TP.\<number\> are generated by this API. For example: TP.0029 for 'Set TerminationPoint Data Operation Failed: %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials

Request
- POST /restconf/operations/v1/cisco-resource-activation:modify-config
- samples/Resource_Configuration_Modify/request.xml
- samples/Resource_Configuration_Modify/request.json

Response
- samples/Resource_Configuration_Modify/response.xml

1.43.1.1.7 Resource_Configuration-Delete

Resource	Description
Modify Bearer Command (MBC)	Delete a service with MBC
HTTP Method	**Resource Path**
POST	https://\<host\>/restconf/operations/v1/cisco-resource-activation:delete-config
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	The delete **configuration** response – see yang model for the data details.

HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TP.<number> are generated by this API. For example: TP.0029 for 'Set TerminationPoint Data Operation Failed: %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials

Request
- POST /restconf/ operations/v1/cisco-resource-activation:delete-config
- samples/Resource_Configuration_Delete/request.xml
- samples/Resource_Configuration_Delete/request.json

Response
- samples/Resource_Configuration_Delete/response.xml

1.43.1.2   *CLI Configuration Run Status Retrieval*

Restconf NBI to get the status of the Templates based CLI Configuration which is scheduled to execute.

Operation	Description
get-cli-configuration-run-status	This operation can be used to check the status of the CLI template execution.
HTTP Method	**Resource Path**
GET	/restconf/operations/v1/cisco-resource-activation:get-cli-configuration-run-status/{job-name}
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request path parameter	job-name: of the CLI template execution
Authorization Required	One or more from following • Configure Templates • View Job
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Return response of type config-response that contains the details of the job executing the cli configuration which can be used to check the status.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors.

	• 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format RA.<number> are generated by this API. For example: RA.0003 for 'Please provide job name.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-resource-activation.yang

1.43.1.2.1 Response

Name	Type	Description
config-response	Container element	Holds the data for response.
job-status	Container element	Holds the job status of the CLI template execution.
job-name	String	Name of the job executing the template.
run-id	String	ID number of the job execution.
run-status	String	The job execution status which could be SCHEDULED, RUNNING, or COMPLETED.
status	String	The job execution result status which could be SUCCESS or FAILED.
duration	String	Time on CLI template job execution.
start-time	String	Time that the job started to run.
completion-time	String	Time that the job finished.
deploy-result-list	List	List of CLI template deploy result.
deploy-result	Container element	Holds the deploy result on each target device
node-ref	String (FDN)	FDN of the device where the cli from the template gets executed.
transcript	String	CLI config let commands executed on the device.
message	String	Exception message.

1.43.1.2.2 CLI Template Run Status

Request
- GET /restconf/operations/v1/cisco-resource-activation:get-cli-configuration-run-status/JobCliTemplateDeployIOSDevices08_18_56_526_PM_02_10_2017 HTTP/1.1

Response
- samples/CLI_Template_Run_Status/response.xml

1.43.1.2.3 GET CLI Template

Request

- GET /restconf/data/v1/cisco-resource-activation:cli-template HTTP/1.1

Response

- samples/Get_CLI_Template/response.xml

1.44 MPLS TE Explicit Path Create/ Modify/ Terminate

MPLS TE Explicit path create/ modify and terminate are supported through a set of operations defined as RESTCONF operations. Support for creating, modifying and deleting an Optical MPLS TE Explicit path is provided. The mpls-te-explicit-path-request type wrapper object is used for these operations.

Operation	Description
create-explicit-path modify-explicit-path terminate-explicit-path	This operation can be used to create/ modify/ terminate an MPLS TE Explicit Path.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:create-explicit-path /restconf/operations/v1/cisco-resource-activation:modify-explicit-path /restconf/operations/v1/cisco-resource-activation:terminate-explicit-path
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	mplste-explicit-path-type
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns if the MPLS TE Explicit path is created created/ modified/ terminated successfully.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format RA.<number> are generated by this API. For example: RA.0096 for 'MPLSTE explicit path service Provision failed -- "%s: %s' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB

	API Error Codes Reference.xlsx
Yang file name	cisco-mpls-te-extension.yang

MPLS TE Explicit Path Data

mplste-explicit-path-type	Data Type	Description
node-ref	String	On the node where the explicit path will be provisioned (4K device).
path-name	String	Explicit path name
path-hop	PathHop	Ordered list of Path Hop with constraints.

MPLS TE Explicit Path Entry Data

Each Path entry contains the fields described in the table below:

path-entries	Data Type	Description
node-ref	String	FDN of a device (eg: **MD=CISCO_EPNM!ND=NCS2006-239-20**) making up explicit path.
constraint-level-type	String	Path Constraint level Type, Possible Values: • strict • loose • none
constraint-type	String	Path Constraint Type; Possible Values: • next • include • exclude • srlg
tp-ref	String	FDN of PTP/CTP (ODU Controller) making up explicit path. (Eg: **MD=CISCO_EPNM!ND=NCS2006-239-20!FTP=name=PCHAN-2-34-RX;lr=lr-optical-channe**l) This fields is applicable only for Path Constraint type 'strict'.

MPLS TE Explicit Path Create

Request

- POST /restconf/operations/v1/cisco-resource-activation:create-explicit-path HTTP/1.1
- samples/MPLS_TE_Explicit_Path_Create/request.xml
- samples/MPLS_TE_Explicit_Path_Create/request.json

Response

- samples/MPLS_TE_Explicit_Path_Create/response.xml

MPLS TE Explicit Path Modify

Request

- POST /restconf/operations/v1/cisco-resource-activation:modify-explicit-path HTTP/1.1
- samples/MPLS_TE_Explicit_Path_Modify/request.xml
- samples/MPLS_TE_Explicit_Path_Modify/request.json

Response

- samples/MPLS_TE_Explicit_Path_Modify/response.xml

MPLS TE Explicit Path Terminate

Request

- POST /restconf/operations/v1/cisco-resource-activation:delete-explicit-path HTTP/1.1
- samples/MPLS_TE_Explicit_Path_Terminate/request.xml
- samples/MPLS_TE_Explicit_Path_Terminate/request.json

Response

- samples/MPLS_TE_Explicit_Path_Terminate/response.xml

1.45 MPLS TE Tunnel Computed Path via WAE PCE

This operation allows a user to compute a list of MPLS TE tunnel paths between two devices using a configured WAE server as the Path Compute Engine (PCE). A resulting computed path can be used for MPLS TE tunnel service provisioning.

Resource	Description	
Computed Path	Computes list of MPLS TE tunnel paths between the specified endpoints	
HTTP Method	**Resource Path**	
POST	/restconf/operations/v1/cisco-resource-network:computed-path	
Request Parameters		
Name	**Type**	**Description**
source-endpoint-ref	String	FDN of the source endpoint. Eg: `MD=CISCO_EPNM!ND=EPNCS4206-32`
destination-endpoint-ref	String	FDN of the destination endpoint. Eg: `MD=CISCO_EPNM!ND=EPNNCS4009-120-162`
vc-type	String	VC type allowed values: mpls-te-tunnel
vc-subtype	String	VC Subtype allowed values: uni-directional-te-tunnel bi-directional-te-tunnel layer3-link

Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Virtual connection Provisioning • Virtual connection Monitoring and Troubleshooting • Network Topology • Network Topology Edit • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	Returns list of computed paths if computed successfully, empty list if no paths are found, or error on failure
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format CP.\<number> are generated by this API. For example: CP.0001 for 'Source node name or destination node name is null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-computed-path.yang

Request

- POST /restconf/operations/v1/cisco-resource-network:computed-path HTTP/1.1
- samples/MPLS_TE_Wae_Computed_Path/request.xml
- samples/MPLS_TE_Wae_Computed_Path/request.json

Response

- samples/MPLS_TE_Wae_Computed_Path/response.xml
- samples/MPLS_TE_Wae_Computed_Path/response.json

1.46 Protection Profile Retrieval

Protection Profile can retrieve all the protection profile values, with the protection profile fdn a matching protection profile will be also be retrieved if available.

Resource	Description
protection-profile	Retrieves all Protection Profile in devices added to Cisco EPN Manager.

HTTP Method	Resource Path	
GET	/restconf/data/v1/cisco-resource-ems:protection-profile	
Query Parameters		
Name	**Type**	**Description**
fdn	String (FDN Format)	Fully Distinguished Name (FDN) of the Protection Profile. Given this, a corresponding single Protection Profile will be returned. FDN = MD=<CISCO_EPNM>!ND=<nd_name>!PPF=<profilename> Eg: MD=CISCO_EPNM!ND=cvg-scapa-229.cisco.com!PPF=123
Authorization Required	One or more from following • Chassis View Read, • Chassis View Read and Write, • Circuit or VC Monitoring and Troubleshooting • Circuit or VC Provisioning • Network Topology • Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more Protection Profile type **protection-profile**	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-protection-profile.yang	

Get All Protection Profile

Request

- GET /restconf/data/v1/cisco-resource-ems:protection-profile

Response

- samples/Get_All_Protection_Profile/response.xml

Get a Protection Profile

Request

- GET /restconf/data/v1/cisco-resource-ems:protection-profile?fdn=MD=CISCO_EPNM!ND=cvg-scapa-229.cisco.com!PPF=123

Response

- samples/Get_a_Protection_Profile/response.xml

1.47 Protection Profile Create/ Modify/ Terminate

Protection Profile create/ modify and terminate are supported through a set of operations defined as RESTCONF operations.

Operation	Description
create-protection-profile modify-protection-profile delete-protection-profile	This operation can be used to create/ modify/ terminate an Protection Profile.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:create-protection-profile /restconf/operations/v1/cisco-resource-activation:modify-protection-profile /restconf/operations/v1/cisco-resource-activation:delete-protection-profile
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	One or more from following - Chassis View Read and Write - MBC UI Framework Access - Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns if the MPLS TE Explicit path is created created/ modified/ terminated successfully.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format RA.\<number\> are generated by this API. For example: RA.0114 for 'protection-profile-ref is unavailable, please provide' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx

Yang file name	cisco-protection-profile.yang

Protection Profile request Data

Name	Data Type	Description
protection-profile-ref	String	FDN of a protection profile(eg: **MD=CISCO_EPNM!ND=cvg-scapa-221.cisco.com!PPF=Test_PPF_profile_name4**)
profile-name	String	Protection Profile name (optional)
protection-type	String	Protection Type; Possible Values: • ONE_PLUS_ONE_BDIR_APS • ONE_PLUS_ONE_UNIDIR_APS • ONE_PLUS_ONE_UNIDIR_NO_APS • ONE_PLUS_ONE_PLUS_R_BIDIR_APS • YCABLE • SPLITTER • PSM • NONE
protection-mode	String	Protection mode Type; Possible Values: • REVERTIVE • NON_REVERTIVE
vc-mode	String	vc mode Type; Possible Values: • VC_MODE_I • VC_MODE_N • VC_MODE_S
tcm-id	String	Tcm-id; Possible Values: • TCM1 • TCM2 • TCM3 • TCM4 • TCM5 • TCM6 • NONE
hold-of-timer	Integer	Hold of timer will accept the number
wait-to-restore-timer	Integer	Will accept numbers in multiples of 60

Protection Profile Create

Request

- POST /restconf/operations/v1/cisco-resource-activation:create-protection-profile
- samples/Protection_Profile_Create/request.xml
- samples/Protection_Profile_Create/request.json

Response

- samples/Protection_Profile_Create/response.xml

Protection Profile Modify

Request

- POST /restconf/operations/v1/cisco-resource-activation:modify-protection-profile
- samples/Protection_Profile_Modify/request.xml

- samples/Protection_Profile_Modify/request.json

  Response

- samples/Protection_Profile_Modify/response.xml

Protection Profile Terminate

Request

- POST /restconf/operations/v1/cisco-resource-activation:delete-protection-profile
- samples/Protection_Profile_Terminate/request.xml
- samples/Protection_Profile_Terminate/request.json

  Response

- samples/Protection_Profile_Terminate/response.xml

1.48 Patchcord Create/ Delete

Patch cord create/ modify and terminate are supported through a set of operations defined as RESTCONF operations.

The internal patchcord is treated as a topological link. The RDN type is "TL".

Operation	Description
create-patch-cord delete-patch-cord	This operation can be used to create/ delete internal Patchcords on NCS2K
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:create-patch-cord /restconf/operations/v1/cisco-resource-activation:delete-patch-cord
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns if the Patch cord is created created/ deleted successfully.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format RA.\<number\> are generated by this API. For example: RA.0023 for 'A End Node should match the Z End Node. Patch cord should be created on the same Node' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal

	errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

Patchcord Create Request Data

Name	Data Type	Description
node-ref	String	FDN of the node on which the patch cord is to be created.
a-end-tp-ref	String	FDN of the A End Termination point for the patchcord.
z-end-tp-ref	String	FDN of the Z End Termination point for the patchcord.
direction	String	Indicates the direction; Possible values: BIDIRECTIONAL UNIDIRECTIONAL
Wavelength	String	Wavelength; Possible values: NA

Patchcord Delete Request Data

Name	Data Type	Description
node-ref	String	FDN of the node on which the patch cord is to be created.
patch-cord-ref	String	FDN of the patchcord. Eg: MD=CISCO_EPNM!TL=10.58.234.141:PSLINE-1-14-10-TX--10.58.234.141:PSLINE-1-1-10-RX

Patch Cord Create

Request

- POST /restconf/operations/v1/cisco-resource-activation:create-patch-cord HTTP/1.1
- samples/Patch_Cord_Create/request.xml
- samples/Patch_Cord_Create/request.json

Response

- samples/Patch_Cord_Create/response.xml
- samples/Patch_Cord_Create/response.json

Patch Cord Delete

Request

- POST /restconf/operations/v1/cisco-resource-activation:delete-patch-cord HTTP/1.1
- samples/Patch_Cord_Delete/request.xml
- samples/Patch_Cord_Delete/request.json

Response

- samples/Patch_Cord_Delete/response.xml

- samples/Patch_Cord_Delete/response.json

Patch Cord Retrieval

Request

The Patch cord is treated as a Topological Link. An attribute in the topological Link response (link-type) indicates if the link is an internal patch cord. The value "internal-patch-cord" will indicate if the link is a patch cord.

- GET /restconf/data/v1/cisco-resource-network:topological-link?fdn=<value> HTTP/1.1

Response

- samples/Patch_Cord_Retrieval/response.xml
- samples/Patch_Cord_Retrieval/response.json

1.49 Shared Risk Resource Assign Link and Node

Shared Risk Resource Assign and Un-Assign Link and Node

Resource	Description	
Shared Risk Resource Group Attributes	Assigns a given Node /Link to an SRRG specified by the resource Pool Name .	
HTTP Method	**Resource Path**	
POST	/restconf/operations/v1/cisco-resource-activation:assign-shared-risk-resource-group	
Query Parameters		
Name	**Type**	**Description**
srrg-id	String	Unique SRRG ID. The SRRG ID is a unique field.
fdn	String	FDN of the SRRG. Eg: MD=CISCO_EPNM!SRRG=2222. Where SRRG is indicator. The value in this field is the same as present in srrg-id field.
user-label	String	The user defined name assigned to the SRRG. This field is not unique.
name	String	Name to be configured for the SRRG
resource-pool-ref	String	Resource pool reference, Eg : MD=CISCO_EPNM!SRRGPL=pool1
resource-fdn-list	List container	Contains list of resource-fdns
resource-fdn	String	Resource value as fdn, Eg: MD=CISCO_EPNM!ND=NCS2006-234-42
Authorization Required	One or more from following • Network Topology • Circuit or VC Provisioning	
Response Messae		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more SRRG resources of type **SRRG Attributes** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message.	

	• 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.\<number> are generated by this API. For example: TL.0005 - 'For SRRG Create, User-Label is mandatory and cannot be empty' If error is from underlying framework/core modules error-app-tag format one of following • TP.\<number> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid • FW.\<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-srrg.yang

Create a SRRG

- POST /restconf/operations/v1/cisco-resource-activation:create-shared-risk-resource-group HTTP/1.1

  Request

- samples/Create_a_SRRG_Link/request.xml

  Response

- samples/Create_a_SRRG_Link/response.xml

Assign SRRG to a Link

- POST /restconf/operations/v1/cisco-resource-activation:assign-shared-risk-resource-group HTTP/1.1

  Sample Request

  - samples/Assign_a_SRRG_to_a_Link/request.xml

  Sample Response

  - samples/Assign_a_SRRG_to_a_Link/response.xml

Assign SRRG to a Node

  Request

  - samples/Assign_a_SRRG_to_a_Node/request.xml

  Response

  - samples/Assign_a_SRRG_to_a_Node/response.xml

1.50 Shared Risk Resource UnAssign Node and Link

UnAssign SRRG to a Link

- POST /restconf/operations/v1/cisco-resource-activation:unassign-shared-risk-resource-group HTTP/1.1

Request

- samples/UnAssign_SRRG_to_a_Link/request.xml

Response

- samples/UnAssign_SRRG_to_a_Link/response.xml

UnAssign SRRG to a Node

Request

- samples/UnAssign_SRRG_to_a_Node/request.xml

Response

- samples/UnAssign_SRRG_to_a_Node/response.xml

1.51 Shared Risk Resource Group (SRRG) – Retrieval

The SRRGs are created on EPNM. The URL allows a user to retrieve the list of SRRGs, or a given SRRG by specifying the FDN of the SRRG

Shared Risk Resource Group Retrieval Data

Name	Type	Description
srrg-id	String	Unique SRRG ID. The SRRG ID is a unique field.
fdn	String	FDN of the SRRG. Eg: MD=CISCO_EPNM!SRRG=2222. Where SRRG is indicator. The value in this field is the same as present in srrg-id field.
user-label	String	The user defined name assigned to the SRRG. This field is not unique.
name	String	The display name configured for the SRRG

Shared Risk Resource Group Retrieval

Resource	Description	
Shared Risk Resource Group Attributes	SRRG Attributes will be retrieved.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-network:shared-risk-resource-group?fdn=<value>	
Query Parameters		
Name	Type	Description
Fdn	String	FDN of the SRRG. Eg: MD=CISCO_EPNM!SRRG=2222. Where SRRG is indicator. The value in this field is the same as present in srrg-id field.
Authorization Required	One or more from following - Network Topology	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-	

	data+json
Response Data	0 or more SRRG resources of type **SRRG Attributes** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL.0025 – 'Error: SRRG Configuration is required. ' If error is from underlying framework/core modules error-app-tag format one of following • TP.<number> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-srrg.yang

1.51.1.1   *GET SRRG Retrieval*

Request

- For All SRRGs: GET /restconf/data/v1/cisco-resource-network:shared-risk-resource-group HTTP/1.1
- For a given SRRG FDN: GET /restconf/data/v1/cisco-resource-network:shared-risk-resource-group?fdn=<value> HTTP/1.1

Response

- samples/GET_SRRG_Retrieval/response.xml

1.51.1.2   *GET SRRG Retrieval with tlFdn Filter*

Request

- GET /restconf/data/v1/cisco-resource-network:shared-risk-resource-group?tlFdn=MD=CISCO_EPNM!TL=10.10.1.84:[WDMSIDE-A]--10.10.1.85:[WDMSIDE-B]

Response

- samples/GET_SRRG_Retrieval_with_tlFdn_Filter/response.xml

1.51.1.3   *GET SRRG Pools List*

Resource	Description

Shared Risk Resource Group Attributes	SRRG Pool Attributes will be retrieved.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-network:srrg-pool	
Query Parameters		
Name	**Type**	**Description**
fdn	String(fdn)	FDN of the SRRG Pool. Eg: MD=CISCO_EPNM!SRRGPL=FUTURE_3 Where SRRGPL is indicator. The value in this field is the name of the srrg pool.
pool-type-ref	String(fdn)	FDN of the SRRG Pool type. Eg: MD=CISCO_EPNM!SRRGPT=FUTURE Where SRRGPT is indicator. The value in this field is the name of the srrg pool type ref.
Authorization Required	One or more from following • Network Topology	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more SRRG resources of type **SRRG Pool Attributes** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL.0034 – 'Resource pool name in FDN is not valid: FDN: %s. ' If error is from underlying framework/core modules error-app-tag format one of following • TP.<number> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-srrg.yang	

Shared Risk Resource Group Pool Retrieval Data

Name	**Type**	**Description**
fdn	String(fdn)	FDN of the SRRG Pool. Eg: MD=CISCO_EPNM!SRRGPL=FUTURE_3 Where SRRGPL is indicator. The value in this field is the name of the srrg pool.
name	String	Name of the SRRG Pool
range-start	String	The start range of the pool

range-end	String	The end range of the pool
type-id	String	Type of the srrg Pool
pool-type-ref	String(fdn)	FDN of the SRRG Pool type reference. Eg: MD=CISCO_EPNM!SRRGPT=FUTURE
resource-group-ref	String(fdn)	FDN of the group reference. Eg: MD=CISCO_EPNM!SRRGR=All Locations

Request

- */restconf/data/v1/cisco-resource-network:srrg-pool*

Response

- samples/GET_SRRG_Pool_List/response.xml

1.51.1.4 *GET SRRG Pools List by FDN*

Request

- */restconf/data/v1/cisco-resource-network:srrg-pool*?fdn=<fdn>

Response

- samples/GET_SRRG_Pool_List_by_FDN/response.xml

1.51.1.5 *GET SRRG Pools based on Pool Type*

Resource	Description	
Shared Risk Resource Group Attributes	SRRG Pool Types will be retrieved.	
HTTP Method	**Resource Path**	
GET	/restconf/data/v1/cisco-resource-network:srrg-pool-type	
Query Parameters		
Name	**Type**	**Description**
fdn	String(fdn)	FDN of the SRRG Pool Type. Eg: MD=CISCO_EPNM!SRRGPT=ROADM Degree
Authorization Required	One or more from following Network Topology	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more SRRG resources of type **SRRG Pool Type Attributes** – see yang model for the data details.	
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL.0042 – 'Invalid SRRG Pool Type Name in FDN %s' If error is from underlying framework/core modules error-app-tag format one of following	

	• TP.\<number\> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials • For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-srrg.yang

Shared Risk Resource Group Pool Retrieval Data

Name	Type	Description
fdn	String(fdn)	FDN of the SRRG Pool. Eg: MD=CISCO_EPNM!SRRGPT=ROADM Degree
name	String	Name of the SRRG Pool
range-start	String	The start range of the pool
range-end	String	The end range of the pool
type-id	String	Type of the srrg Pool

Request

• */restconf/data/v1/cisco-resource-network:srrg-pool-type*

Response

• samples/GET_SRRG_Pool_Type/response.xml

1.52 LAG Operations

The LAG operations supported are Create, Delete, Assign ports to LAG groups and Un-Assign ports from LAG groups.

LAG Create

This operation creates a LAG group identified by the user label and configuration provided.

Resource	Description	
LAG config attributes	Creat LAG groups .	
HTTP Method	Resource Path	
POST	/restconf/operations/v1/cisco-resource-activation:create-lag	
Input Parameters		
Name	Type	Description
user-label	String	Name of the LAG group to be created
channel-group-id	String	Indicates the unique identifier to be used for creating the LAG. The channel group id gets suffixed to the user-label upon successful creation of LAG
control-mode	String	Indicates if the LAG is either lacp or pagp. The allowed values are: ■ lacp ■ pagp
node-ref	String	The FDN of the node on which the LAG group has to be created.

Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Messae	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	The data indicating the name of the LAG, the status and raw configuration returned upon a successful creation of LAG.
Output Parameters	

Name	Type	Description
user-label	String	The user label provided for the LAG creation request
Status	String	SUCCESS or FAILURE
raw-config	String	The raw configuration applied on the device for creating the LAG.
HTTP Status Code		• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)		Response with error condition provides error tag in error-app-tag element. Error tag with format RA.<number> are generated by this API. For example: RA.0068 – 'Mandatory node-ref is missing ' If error is from underlying framework/core modules error-app-tag format one of following • TP.<number> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name		cisco-lag.yang

Request

- POST URL: https://{ServerIP}/restconf/operations/v1/cisco-resource-activation:create-lag
- samples/LAG_Create/request.xml

Response
- samples/LAG_Create/response.xml

LAG Delete

This operation deletes a LAG identified by the FDN provided as query parameter to the LAG deletion URL.

Resource	Description
LAG FDN	Deletes the LAG group identified by the LAG FDN. The LAG FDN follows the same naming convention as the termination point .
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:delete-lag
Query Parameters	

Name	Type	Description
Fdn	String	FDN of the LAG that has to be deleted. The LAG FDN is similar to termination point FDN. Eg: https://${server-ip}/restconf/operations/v1/cisco-resource-activation:delete-lag?fdn=MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-2.cisco.com!FTP=name=Bundle-Ether26;lr=lr-lag-fragment
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices	
Response Messae		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	The data indicating the name of the LAG, the status and raw configuration returned upon a successful creation of LAG.	
Output Parameters		

Name	Type	Description
user-label	String	The user label provided for the LAG deletion request
Status	String	SUCCESS or FAILURE
raw-config	String	The raw configuration applied on the device for deleting the LAG.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format RA.<number> are generated by this API. For example: RA.0068 – 'Mandatory node-ref is missing ' If error is from underlying framework/core modules error-app-tag format one of following • TP.<number> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials	

	• For complete list of error-app-tag and error message refer to [EPNM 7.1.1 NB API Error Codes Reference.xlsx](#)
Yang file name	cisco-lag.yang

Request

POST URL: [https://{ServerIP}/restconf/operations/v1/cisco-resource-activation:delete-lag?fdn= MD=CISCO_EPNM!ND=tmh-chn-mvso-asr9k-2.cisco.com!FTP=name=Bundle-Ether26;lr=lr-lag-fragment](#)

Response

• [samples/LAG_Delete/response.xml](#)

LAG Assign

This operation assigns member ports to a given LAG.

Resource	Description	
LAG config attributes	Assigns member ports to LAG groups .	
HTTP Method	**Resource Path**	
POST	/restconf/operations/v1/cisco-resource-activation:assign-lag-member	
Input Parameters		
Name	**Type**	**Description**
user-label	String	Name of the LAG group to which the member ports are to be assigned
channel-group-id	String	Indicates the channel group ID that gets suffixed to the user-label
control-mode	String	Indicates if the LAG is either lacp or pagp. The allowed values are: ▪ lacp ▪ pagp
lacp-mode	String	Identifies the modes based on the control-mode. The supported values are : -For control-mode lacp, the modes are - active and - passive.
pagp-mode	String	-For control-mode pagp, the modes are - auto - desirable and - on
node-ref	String	The FDN of the node to which the member ports have to be added
lag-member-list		Contains a list of member port FDNs to un-assign from the LAG group. Contains a list of "member" elements
member		Describes the member attributes, contains the mode of the member and the member-ref
member-ref	String	FDN of the termination point to be assigned to the LAG
lacp-mode	String	If the control mode is lacp, the lacp-mode s allowed.
pagp-mode	String	If the control mode is pagp, the pagp-mode is allowed.
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access	

	• Network Devices
Response Messae	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	The data indicating the name of the LAG, the status and raw configuration returned upon a successful creation of LAG.
Output Parameters		

Name	Type	Description
user-label	String	The user label provided for the LAG creation request
Status	String	SUCCESS or FAILURE
raw-config	String	The raw configuration applied on the device for un assigning the member ref from the LAG.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	

Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.
	
	Error tag with format RA.\<number\> are generated by this API. For example: RA.0068 – 'Mandatory node-ref is missing '
	
	If error is from underlying framework/core modules error-app-tag format one of following
	    • TP.\<number\> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid
	    • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
	    • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
	
	For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	

Yang file name	cisco-lag.yang	

Request
- POST URL: https://{ServerIP}/restconf/operations/v1/cisco-resource-activation:assign-lag-member
- samples/LAG_Assign/request.xml

Response
- samples/LAG_Assign/response.xml

LAG Un-Assign

This operation un-assigns member ports from the LAG.

Resource	Description
LAG config attributes	Un Assigns member ports from a LAG group
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:unassign-lag-member

Input Parameters		
Name	**Type**	**Description**
user-label	String	Name of the LAG group to be created
channel-group-id	String	Unique identifier that will be suffixed to the user label of the LAG
control-mode	String	Indicates if the LAG is either lacp or pagp. The allowed values are: ▪ lacp ▪ pagp
lacp-mode	String	Identifies the modes based on the control-mode. The supported values are : -For control-mode lacp, the modes are - active and - passive.
pagp-mode	String	-For control-mode pagp, the modes are - auto - desirable and - on
node-ref	String	The FDN of the node to which the member ports have to be added
lag-member-list		Contains a list of member port FDNs to un-assign from the LAG group. Contains a list of "member" elements
member		Describes the member attributes, contains the mode of the member and the member-ref
member-ref	String	FDN of the termination point to be un-assigned from the LAG
lacp-mode	String	If the control mode is lacp, the lacp-mode s allowed.
pagp-mode	String	If the control mode is pagp, the pagp-mode is allowed.
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Network Topology • MBC UI Framework Access • Network Devices	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	The data indicating the name of the LAG, the status and raw configuration returned upon a successful creation of LAG.	
Output Parameters		
Name	**Type**	**Description**
user-label	String	The user label provided for the LAG creation request
Status	String	SUCCESS or FAILURE
raw-config	String	The raw configuration applied on the device for un assigning the member ref from the LAG.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.	

	Error tag with format RA.<number> are generated by this API. For example: RA.0068 – 'Mandatory node-ref is missing ' If error is from underlying framework/core modules error-app-tag format one of following • TP.<number> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-lag.yang

Request
- POST URL: https://{ServerIP}/restconf/operations/v1/cisco-resource-activation:unassign-lag-member
- samples/LAG_UnAssign/request.xml

Response
- samples/LAG_UnAssign/response.xml

1.53 Performance Metrics Retrieval on Topological Link– Optical Span Loss

Resource	Description
Topological Link metrics	Performance Metrics for the given topological Link.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-resource-network:perf-metrics?tlFdn=<value>
Query Parameters	

Name	Type	Description
tlFdn	String	FDN of the Topological Link on which the Performance Metrics has to be retrieved. Eg: /restconf/data/v1/cisco-resource-network:perf-metrics?tlFdn=MD=CISCO_EPNM!TL=10.58.234.42:[WDM SIDE-B]--10.58.234.55:[WDMSIDE-A]
Authorization Required	One or more from following • Network Topology • Network Topology Edit	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	The Performance metrics for the given Topological Link.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.	

	Error tag with format PREF.<number> are generated by this API. For example: PREF.0001 – 'Missing input. Topological Link is mandatory for performance metrics' If error is from underlying framework/core modules error-app-tag format one of following - TP.<number> - any tag starting with "TP." prefix for any internal errors like TP.0002=Given LayerRate Value is Invalid - FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. - CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-performance-analytics.yang

Performance Metrics for Topological Link Retrieval Data

The Performance metrics is retrieved for a given topological Link. The current support is for retrieving the Span Loss associated with the end points of a given topological Link. The Link FDN is given as filter parameter for the URL.

Name	Type	Description
topological-link-metrics	Complex Object	Container Object
span-loss-direction	String	Indicates the direction of the Span; Possible values: **A to Z** **Z to A**
span-loss-value	Float	The span loss value
span-loss-type	String	Indicates the span loss type. Possible values: **OSC**, **Channel**
max-threshold	String	Max Threshold
min-threshold	String	Min Threshold
resolution	String	Indicates span-loss resolution
span-loss-in-range	Boolean	Is span loss in range

Request

- GET /restconf/data/v1/cisco-resource-network:perf-metrics?tlFdn=<value> HTTP/1.1

Response

- samples/Performance_Metrics_for_Topological_Link_Retrieval/response.xml

1.54 Alarm Retrieval

Alarm Retrieval through Restconf with various filters.

Resource	Description
Alarm	Alarm resource which will retrieves all the alarms and retrieves alarms based on filters.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-rtm:alarm?{filter}
Query Parameters	

Name	Type	Description
tp-ref	String	Alarms with the matching termination point reference will be retrieved MD=<CISCO_EPNM>!ND=<nodenmae>!CTP=name=OTU2 0/6/0/7;lr=lr-och-transport-unit-2
nd-ref	String	Alarms with the matching node reference will be retrieved MD=<CISCO_EPNM>!ND=<nodename>
eq-ref	String	Alarms with the matching equipment reference will be retrieved MD=<CISCO_EPNM>!ND=<nodename>!EQ=<name=PWR-B;partnumber=15454-M6-DC>
perceived-severity	String	Alarms with the matching perceived severity will be retrieved, possible severity values consist of (critical, major, minor, warning, cleared, intermittent
Authorization Required	One or more from following • View Alerts and Events	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more alarm resources of type **alarm** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.<number> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-alarms.yang	

Alarm data type

alarm -type	Data Type	Description
alarm	**Container element**	Container element holds the information about Alarm
alarm-identifier	**Container element**	Holds event, resource and cause associated to the alarm
description	String	Description of the Alarm
category	String	Category of alarm like Optical

alarm -type	Data Type	Description
source-object-ref	Fdn String	FDN for the Source device assocciated with Alarm (Eg: MD=CISCO_EPNM!ND=ncs2006-239-72 or MD=CISCO_EPNM!ND=NCS4009-Automation!CTP=name=OTU20/6/0/7;lr=lr-och-transport-unit-2 or MD=CISCO_EPNM!ND=ncs2006-239-72!EQ=name=PWR-B;partnumber=15454-M6-DC)
source-object-id	String	Internal id for the source object if applicable
business-key	String	Optional opaque field containing info for alarm correlation business logic
source-object-name	String	Source device name associated with the Alarm
node-ref	String	Device name associated wth the Alarm
cause-type	String	Cause Type will have possible values • root-cause • symptom • cause-unknown
ack-state	String	Acknowledge state of the Alarm will contain possible values • acknowledged • unacknowledged
remote-interface-ip-address	String	Device ip address associated with Alarm
perceived-severity	String	Alarm severity with the following possible values • cleared • indeterminate • minor • major • critical • warning multiple values can also be provided with separator ","
system-received-time	String	Alarm occurred time
system-received-time-iso8601	String	Application or system time stamp when the alarm is first processed
system-update-time	String	Last updated time of the alarm
system-update-time-iso8601	String	last update in the application system
node-event-time	String	Device timestamp of the alarm
node-event-time-iso8601	String	Node or device time stamp when the alarm is generated using ISO 8601 format yyyy-MM-dd'T'HH:mm:ss.SSSXXX
probable-cause	String	Probable cause of the alarm
service-affecting	String	Indicates if the alarm is service affecting coming directly from NCS 2K devices. Possible values • service-affecting • non-service-affecting • service-affecting-unknown

alarm -type	Data Type	Description
service-impacting	String	Indicates if the alarm is service impacting through EPNM Service Impact Analysis. Possible values • service-impacting • non-service-impacting • service-impacting-unknown
event-type	String	The event type as defined in X.733/X.736.
has-clear	String	Indicates if the alarm has a potential clear notification
owner	String	Alarm owner
Note	**container**	Note details related to the Alarm
action-performed	String	Action performed on the alarm with the following possible values • alarm-clear • alarm-acknowledge • alarm-unacknowledge • alarm-delete • alarm-anotate • alarm-action-unknown
impacted-objects	fdn - String	List of impacted services related to alarm Eg: MD=CISCO_EPNM!CFS=OCHNC_Passive_2
root-cause-objects	Fdn - String	Fully Distinguished Name of the Objects that are candidates for causing the alarm
root-cause-alarm-identifier	Container	Root cause event identifier
user-defined-fields	Container	User defined fields associated with alarm

Alarm Identifier type

Alarm-identifier	Data Type	Description
event-identifier	String	Alarm id of the Alarm
resource-object-ref	Fdn String	FDN for the Resource object reference device associated with Alarm (Eg: MD=CISCO_EPNM!ND=ncs2006-239-72 or MD=CISCO_EPNM!ND=NCS4009-Automation!CTP=name=OTU20/6/0/7;lr=lr-och-transport-unit-2 or MD=CISCO_EPNM!ND=ncs2006-239-72!EQ=name=PWR-B;partnumber=15454-M6-DC)
probable-cause	String	Probable cause of the alarm

Note type

Note	Data Type	Description
creator-id	String	Note creator possibly username
text	String	Note text
note-time	String	time stamp when note created

Root-cause-alarm-identifier

Type	Data Type	Description
event-identifier	String	Alarm id of the Alarm

User-Defined-Fields

Type	Data Type	Description
user-defined-field	Container	Container will hold user defined field's label and value related to alarm
label	String	Label of User defined field associated with alarm
value	String	value of User defined field associated with alarm

Get All Alarms

Request

- GET /restconf/data/v1/cisco-rtm:alarm

Response

- samples/Get_All_Alarm/response.xml

Get All Alarms with User Defined Fields

Alarm retrieval will expose User defined fields associated with respective alarms in the get All alarm API

Request

- GET /restconf/data/v1/cisco-rtm:alarm

Response

- samples/Alarms_With_UDF_Product_id_product_name/response.xml
- samples/Alarms_With_UDF_Product_id_product_name/response.json

Get All Alarm by Tp-Ref

Request

- GET /restconf/data/v1/cisco-rtm:alarm?tp-ref=MD=CISCO_EPNM!ND=232!CTP=name=Optics0/4/0/11;lr=lr-optical-section

Response

- samples/Get_All_Alarm_By_TP_Ref/response.xml

Get All Alarm by Nd-Ref

Request

- GET /restconf/data/v1/cisco-rtm:alarm?nd-ref=MD=CISCO_EPNM!ND=ONS15454-4

Response

- samples/Get_All_Alarm_By_Nd_Ref/response.xml

Get All Alarm by Eq-Ref

Request

- GET   /restconf/data/v1/cisco-rtm:alarm?eq-ref=MD=CISCO_EPNM!ND=ONS15454-44!EQ=name=SLOT-1-5

Response

- samples/Get_All_Alarm_By_Eq_Ref/response.xml

Get All Alarm by Perceived Severity

Request

- GET /restconf/data/v1/cisco-rtm:alarm?perceived-severity=major

Response

- samples/Get_All_Alarm_By_Perceived_Severity/response.xml

Get All Alarm by More than one Perceived Severity

Request

- GET /restconf/data/v1/cisco-rtm:alarm?perceived-severity=major,minor

Response

- samples/Get_All_Alarm_By_More_than_one_Perceived_Severity/response.xml

Get All Alarm by Scope

Alarm retrieval can be done with a scope, scope implies creating a new virtual domain or even with a existing domain creating a new user and assign a single or multiple Network Element to the same user in EPNM GUI. Use the newly created username/password in the rest-client and retireve alarm with following rest url:
GET /restconf/data/v1/cisco-rtm:alarm?nd-ref=MD=CISCO_EPNM!ND=NCS4k-A

Request

- GET /restconf/data/v1/cisco-rtm:alarm

Response

- samples/Get_All_Alarm_By_Scope/response.xml

Get All Alarm by System-Update Time

Alarms can retrieved using system-update-time. The alarms with system-update-time greater than or equal the time will be retrieved.
Request

- GET/restconf/data/v1/cisco-rtm:alarm?system-update-time=2018-06-19 08:47:17.641

Response

- samples/Get_All_Alarm_By_System_Update_Time/response.xml

Get Alarm by Iterator Id

Request

- GET/restconf/data/v1/cisco-rtm:alarm?.iteratorId=5685737

Response

- samples/Get_All_Alarm_By_Iterator_Id/response.xml

Alarm Handling

Alarm Handling capability allows to Acknowledge/ UnAcknowledge/ Clear and Delete alarms
Host: <epnm-host>
Accept: application/yang-data+xml

<p:action-performed>alarm-acknowledge</p:action-performed>
<p:action-performed>alarm-unacknowledge</p:action-performed>
<p:action-performed>alarm-clear</p:action-performed>
<p:action-performed>alarm-delete</p:action-performed>

Optionally probable-cause can take specific alarm-id to update the alarm status.
<p:probable-cause>alarm-id</p:probable-cause>

Request

- PUT /restconf/data/v1/cisco-alarm:handle-alarm
- samples/Alarm_Handling/request.xml

Response

- samples/Alarm_Handling/response.xml

Alarm to Service Association

Alarms related to a service can be retrieved by the CFS-Ref

Request

- GET /restconf/data/v1/cisco-rtm:impacting-alarms-by-service?cfs-ref=<value>

Response

- samples/Alarm_to_Service_Association/response.xml

Get All Alarms with root-cause

To retrieve all alarms with cause-type as root-cause in the system.

Resource	Description
Alarm	Alarm resource which will retrieves all the alarms and retrieves alarms based on filters.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-rtm:alarm-with-root-cause
Authorization Required	One or more from following • View Alerts and Events
Response Message	

Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more alarm resources of type **alarm** – see yang model for the data details.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.<number> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-alarms.yang

Host: <epnm-host>
Accept: application/yang-data+xml

Request

- GET /restconf/data/v1/cisco-rtm:alarm-with-root-cause

Response

- samples/Alarms_With_Root_Cause/response.xml

Get All symptom alarms with root-cause

To retrieve all symptom alarms associated with a single root cause alarm.

Resource	Description	
Alarm	Alarm resource which will retrieves all the alarms with root-cause.	
HTTP Method	**Resource Path**	
POST	/restconf/data/v1/cisco-rtm:alarm-with-root-cause	
Input Parameters		
Name	**Type**	**Description**
alarm-request		Alarm request container which takes alarm-list as input
alarm-identifier		
event-identifier	String	Alarm id of the Alarm
resource-object-ref	Fdn String	FDN for the Resource object reference device associocated with Alarm (Eg: MD=CISCO_EPNM!ND=ncs2006-239-72)

probable-cause	String	Probable cause of the alarm
Authorization Required	One or more from following • View Alerts and Events	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	0 or more alarm resources of type **alarm** – see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.<number> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-alarms.yang	

Host: <epnm-host>
Accept: application/yang-data+xml

Request

- POST /restconf/data/v1/cisco-rtm:alarm-with-root-cause
- samples/Alarm_Symptom_Alarms_With_Root_Cause/request.xml

Response

samples/Alarm_Symptom_Alarms_With_Root_Cause/response.xml

Get All Alarms with symptom

To retrieve all alarms with cause-type as symptom in the system.

Resource	Description
Alarm	Alarm resource which will retrieves all the alrams and retrieves alarms based on filters.
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-rtm:alarm-with-symptom
Authorization Required	One or more from following • View Alerts and Events
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json

Response Data	0 or more alarm resources of type **alarm** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.<number> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-alarms.yang

Host: <epnm-host>
Accept: application/yang-data+xml

Request

- GET /restconf/data/v1/cisco-rtm:alarm-with-symptom

Response

- samples/Alarms_With_Symptom/response.xml

Get root-cause alarm with symptom alarm

To retrieve the root-cause alarm associated with a single symptom alarm.

Resource	Description	
Alarm	Alarm resource which will retrieves all the alarms with symptom.	
HTTP Method	**Resource Path**	
POST	/restconf/data/v1/cisco-rtm:alarm-with-symptom	
Input Parameters		
Name	**Type**	**Description**
alarm-request		Alarm request container which takes alarm-list as input
alarm-identifier		
event-identifier	String	Alarm id of the Alarm
resource-object-ref	Fdn String	FDN for the Resource object reference device associacted with Alarm (Eg: MD=CISCO_EPNM!ND=ncs2006-239-72)
probable-cause	String	Probable cause of the alarm
Authorization Required	One or more from following • View Alerts and Events	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	

Response Data	0 or more alarm resources of type **alarm** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.\<number\> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-alarms.yang

Host: <epnm-host>
Accept: application/yang-data+xml

Request

- POST /restconf/data/v1/cisco-rtm:alarm-with-symptom
- samples/Alarm_Root_Cause_Alarms_With_Symptom/request.xml

Response

samples/Alarm_Root_Cause_Alarms_With_Symptom/response.xml

1.55 Controller Port

Controller Port resource path to retrieve and update media type controller mode.

Retrieve ControllerPort

Resource	Description	
ControllerPort	Retrieves the Controller Port.	
HTTP Method	**Resource Path**	
GET	/restconf**/**data/v1/cisco-nrf-controller:controller-port	
Query Parameters		
Name	**Type**	**Description**
fdn	String (FDN Format)	Fully Distinguished Name (FDN) of the. Given this, a corresponding single Controller Port will be returned. FDN = MD=\<CISCO_EPNM\>!ND=\<nd_name\>!CTRLP =\<name\> Eg: MD=CISCO_EPNM!ND=NCS4206-146.4!CTRLP=MediaType 0/4/0
ndFdn	String (FDN Format)	Fully Distinguished Name (FDN) of the device. Given this, all the controller ports of this device are returned

Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more controller port resources of type controller-port – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Response Data	No response if the operation succeeds. Error message is displayed if the operation fails.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format CTRL.\<number> are generated by this API. For example: CTRL.0005 for 'Requires controller port fdn.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang File Name	cisco-nrf-controller.yang

Get Controller Port

Request

• GET https://{{host}}/restconf/data/v1/cisco-nrf-controller:controller-port

Response

• samples/Get_Controller_Port/response.xml

Update ControllerPort – MediaType Controller Mode

Resource	Description
ControllerPort	Update the controller port – controller-port, specifically the MediaType Controller's mode can be updated

HTTP Method	Resource Path
PUT	/restconf/data/v1/cisco-nrf-controller:controller-port
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **controller-port** that contains the details of the controller-port – see yang model for the data details. NOTE: only "mode" of the MediaType controller can be updated. See example request/response sections for api invocation and data
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	No response if the operation succeeds. Error messages is returned if the operation fails.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format CTRL.\<number\> are generated by this API. For example: CTRL.0006 for 'Controller port not found with fdn: %s' If error is from underlying framework/core modules error-app-tag format one of following •　　　FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. •　　　CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang File Name	cisco-nrf-controller.yang

Update Controller Port – MediaType Controller Mode

Request

- PUT /restconf/data/v1/cisco-nrf-controller:controller-port
- samples/Update_Controller_Port/request.xml

1.56 Virtual Trunk

This interface provides the services to create, modify, delete and get the Virtual Trunk.
Virtual Trunk will be a mandatory pre-requisite for the LMP creation, so we have this interface to manage Virtual Trunks.

Input Parameters		
Name	**Type**	**Description**
virtual-trunk-request		Virtual Trunk request container
add-drop-port-fdn	String	Add drop port fdn, fdn information for virtual trunk, more than

		1 and maximum of 2 add-drop-port-fdn can be provided for Virtual Trunk operations Eg : MD=CISCO_EPNM!ND=NCS2K Node-C!ADP=PSLINE-2-1-10-RX<![CDATA[&]]>PSLINE-2-1-10-TX
description	String	Description of Virtual Trunk
alien-wavelength	Enum	Possible values are: • MR MM TXP • MR MM TXP (w/splitter) • MR SM TXP • MR SM TXP (w/splitter) • 2.5-Gbps Aggregation • 2.5-Gbps Aggregation (w/splitter) • OC192LR • OC48ELR • 10-Gbps Aggregation • 10-Gbps Aggregation (w/splitter) • GE DWDM GBIC • DWDM-XENPAK • Data Muxponder • Data Muxponder (w/splitter) • 40G DWDM ITU-T TXP • CRS-1 40G ITU-T LC • 2.5G DWDM ITU-T SFP • 40G DWDM ITU-T MXP • 4OC192-ITU • 4-10GE-ITU • 10GE-ITU • DWDM ITU-T SFP • DWDM-XFP • DWDM-X2 • ONS-XC-10G-EP • ONS-XC-10G-C • ONS-XC-10G • ONS-SC-2G • ONS-SC-4G • ONS-SC+-10G • 100G-LC-C • 100G-ME-C • MXP_2.5G_10G • MXP_MR_2.5G • MXPP_MR_2.5G • TXPP_MR_2.5G • TXP_MR_2.5G • TXP_MR_10E • TXP_MR_10G • MXP_2.5G_10E, • MXP_MR_10DME • 40G-TXP-C • 40G-MXP-C

		• 40E-TXP-C • 40E-MXP-C • 100G-CK-C • 100G-CK-ME-C • 100GS-CK-LC • 200G-CK-LC
trunk	Enum	Possible values are: • TRUNK_DEFAULT_MODE • TRUNK_100G_MODE • TRUNK_150G_MODE • TRUNK_350G_MODE • TRUNK_450G_MODE • TRUNK_550G_MODE • TRUNK_200G_MODE • TRUNK_250G_MODE • TRUNK_300G_MODE • TRUNK_400G_MODE • TRUNK_500G_MODE • TRUNK_600G_MODE • TRUNK_300G_3_BPS_MODE • TRUNK_300G_3_4375_BPS_MODE • TRK_200G_2_3125BPS_MODE • TRK_400G_4_4375BPS_MODE • TRK_300G_3_4375BPS_MODE
fec	Enum	Possible values are: • NONE • STANDARD • ENHANCED_HG20 • ENHANCED_HG7 • ENHANCED_I_4 • ENHANCED_I_7 • ENHANCED_SWIZZLE • ENHANCED • SD_20 • ENHANCED_SD_20 • ENHANCED_SD_7 • LONG_HAUL_SD • HIGH_GAIN_SD • HIGH_GAIN_HD • HIGH_GAIN_HD_MULTIVENDOR • SD_15_DE_OFF • SD_15_DE_ON • SD_25_DE_OFF • SD_25_DE_ON • SD_7 • OTU_7_STAIRCASE • SD_15 • SD_25

		• LONG_HAUL_HD • HIGH_GAIN_CI_BCH_FEC • SD_EVEREST • SD_DENALI • ENHANCED_SD_27 • ENHANCED_SD_15 • SD_27_DE_OFF • SD_27_DE_ON • OFF
txp-control-mode	String	Allowed values are: NONE, LOCAL Default: NONE To provision local LMP, value to be used: LOCAL

Virtual Trunk Creation

Virtual Trunk creation service request accepts the request payload with add drop port fdn, description, fec, alien wavelength and trunk and the following table gives the details about the request:

Operation	Description
Virtual Trunk Creation	This operation can be used to create new Virtual Trunk.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:virtual-trunk
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data contains the details of add drop port fdn, description, fec, alien wavelength and trunk.
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	Result: Indicating the creation as SUCCESS / FAILED Message: Command pushed to CLI or Failure message when Result is Failed.
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	Virtual Trunk response – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.

	Error tag with format AL.<number> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

Request

- POST /restconf/operations/v1/cisco-resource-activation:virtual-trunk
- samples/Virtual_Trunk_Create/request.xml
- samples/Virtual_Trunk_Create/response.xml

Virtual Trunk Modification

Virtual Trunk Modification service request accepts the request payload with add drop port fdn, description, fec, alien wavelength and trunk and the following table gives the details about the request:

Operation	Description
Virtual Trunk Modification	This operation can be used for modifying existing Virtual Trunk.
HTTP Method	**Resource Path**
PUT	/restconf/operations/v1/cisco-resource-activation:virtual-trunk
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data contains the details of add drop port fdn, description, fec, alien wavelength and trunk.
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	Result: Indicating the creation as SUCCESS / FAILED Message: Command pushed to CLI or Failure message when Result is Failed.
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	Virtual Trunk response – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body

	• 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.<number> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

Request

- PUT /restconf/operations/v1/cisco-resource-activation:virtual-trunk
- samples/Virtual_Trunk_Modify/request.xml
- samples/Virtual_Trunk_Modify/response.xml

Virtual Trunk Deletion

Virtual Trunk Deletion service request accepts the request payload with add drop port fdn, description, fec, alien wavelength and trunk and the following table gives the details about the request:

Operation	Description
Virtual Trunk Deletion	This operation can be used for deletion of existing Virtual Trunk.
HTTP Method	**Resource Path**
DELETE	/restconf/operations/v1/cisco-resource-activation:virtual-trunk
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data contains the details of add drop port fdn, description, fec, alien wavelength and trunk.
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json

Response Data	Result: Indicating the creation as SUCCESS / FAILED Message: Command pushed to CLI or Failure message when Result is Failed.
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	Virtual Trunk response – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.\<number\> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

Request

- DELETE /restconf/operations/v1/cisco-resource-activation:virtual-trunk
- samples/Virtual_Trunk_Delete/request.xml
- samples/Virtual_Trunk_Delete/response.xml

Virtual Trunk Retrieval

- Virtual Trunks can be retrieved through the GET api
- GET api retrieves all the Virtual Trunks
- ndRef filter is available to list all the Virtual Trunks under a specific device

Resource	Description	
Virtual Trunk Deletion	This operation can be used for retrieving existing Virtual Trunks.	
HTTP Method	**Resource Path**	
GET	/restconf/operations/v1/cisco-resource-activation:virtual-trunk?ndRef={}	
Query Parameters		
Name	**Type**	**Description**
ndRef	String	Fdn to retrieve list of Virtual Trunks associated with device MD=\<CISCO_EPNM\>!ND=\<nodenmae\>
Authorization Required	One or more from following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning	

	• Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more Virtual Trunks – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format AL.\<number\> are generated by this API. For example: AL.0003 for 'ME RDN cannot be null.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

Request

- GET /restconf/operations/v1/cisco-resource-activation:virtual-trunk?ndRef={}
- samples/Virtual_Trunk_Get/response.xml

1.57 LMP Link

LMP Link creation and deletion are done via., POST operations. LMP Links can be created between:
- NCS2K → NCS4K
- NCS4K → NCS4K
- NCS2k → NCS1K

➢ LMP Link creation requires the source and destination endpoints (Termination point FDN) or Optical static LMP container fields to be specified.
➢ LMP Link deletion requires the LMP Link FDN or ADP FDN to be passed as a query parameter to the DELETE URL.
➢ LMP Link retrieval is like regular topological link retrieval. The Topological Link retrieval URL is provided with the LMP Link FDN as query parameter.
➢ Optical Static LMP Retrieval is done based on source Node FDN or specific Add Drop Virtual Trunk Port FDN.

LMP Link Create

Resource	Description
LMP Attributes	Creates an LMP Link between the specified endpoints
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:lmp-link-resource

Input Parameters		
Name	**Type**	**Description**
topo-link-create-request		LMP Link Creation request container
source-endpoint		Source Endpoint container
endpoint-ref	String	FDN of the source endpoint of the LMP. Eg: `MD=CISCO_EPNM!ND=NCS2KE-235-159!PTP=name=PSLINE-5-1-11-RX;lr=LR_PHYSICAL_OPTICAL`
dest-endpoint		Destination Endpoint container
endpoint-ref	String	FDN of the destination endpoint of the LMP Eg: `MD=CISCO_EPNM!ND=NCS2KE-235-159!PTP=name=PSLINE-5-1-11-RX;lr=LR_PHYSICAL_OPTICAL`
optical-static-lmp		Optical Static LMP Container
add-drop-port-fdn	Fdn	Virtual trunk endpoint FDN of the device.
lmp-type	Enum	LMP Type. Possible values are: • Signaled • Not Signaled • Signaled(NCS1004) • Signaled(NCS4k)
is-numbered	Boolean	Indicates whether local interface is required or not. true when local interface IP is required else will default to "0.0.0.0"
local-interface-ip	ip-address	IP address provided/considered only when is-numbered is true
is-remote-managed	Boolean	Indicates whether destination device is remotely managed or not
dest-endpoint-ref	Fdn	End-point FDN of the remote managed device
Authorization Required	One or more from following • Network Topology • Network Topology Edit	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Result: Indicating the creation as CREATED / FAILED Message:	
	Type	**Description**
Result	String	CREATED / FAILED
message	String	**For success case**: LMP Link is created Successfully **For error condition** (Internal Error on Server): Preconditions not met **For API call error**: LMP Link creation failed
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message.	

	• 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL.0045 - 'LMP Link creation failed: <value>' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

LMP Link Modify

Resource	Description
LMP Attributes	Modify Optical Static LMP Link between the specified endpoints
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-resource-activation:modify-lmp-link-resource
Input Parameters		

Name	Type	Description
topo-link-modify-request		LMP Link Modify request container
optical-static-lmp		Optical Static LMP Container
add-drop-port-fdn	Fdn	Virtual trunk endpoint FDN of the device.
is-remote-managed	Boolean	Indicates whether destination device is remotely managed or not
dest-endpoint-ref	Fdn	End-point FDN of the remote managed device
peering	String	lmp ID of neighbour lmp on same source node. Provide 'NA' to remove peering. This is applicable for NCS1K devices, for NCS2K or NCS4K it is not applicable
Authorization Required	One or more from following • Network Topology • Network Topology Edit	
Response Message		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Result: Indicating the creation as SUCCESS / FAILED Message: Command pushed to CLI or Failure message when Result is Failed.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed.	

	Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example: TL.0045 - 'LMP Link creation failed: <value>' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

LMP Link Delete

Resource	Description	
LMP Attributes	Deletes an LMP Link specified as an URL parameter	
HTTP Method	**Resource Path**	
DELETE	/restconf/operations/v1/cisco-resource-activation:lmp-link-resource	
Query Parameters		
Name	**Type**	**Description**
Fdn	String	FDN of the LMP link to be deleted. Link FDN or ADP FDN
Authorization Required	One or more from following • Network Topology • Network Topology Edit	
Response Messae		
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json	
Response Data	Result : Indicating the creation as CREATED / FAILED Message:	
	Type	**Description**
Result	String	DELETED / FAILED
Message	String	**For success case**: LMP Link is deleted Successfully **For error condition** (Internal Error on Server) : Preconditions not met **For API call error** : LMP Link deletion failed
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TL.<number> are generated by this API. For example:	

	TL.0046 - 'LMP Link deletion failed: <value>' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-topology.yang

LMP Link Create Request / Response

- POST /restconf/operations/v1/cisco-resource-activation:lmp-link-resource

Request

- samples/LMP_Link_Create/request.xml

Response

- samples/LMP_Link_Create/response.xml

Request(Optical Static LMP)

- samples/LMP_Link_Create/Static_LMP/request.xml

Response(Optical Static LMP)

- samples/LMP_Link_Create/Static_LMP/response.xml

LMP Link Modify Request / Response

Request(Optical Static LMP)

- samples/LMP_Link_Modify/request.xml

Response(Optical Static LMP)

- samples/LMP_Link_Modify/response.xml

LMP Link Delete Request / Response

Request

- DELETE /restconf/operations/v1/cisco-resource-activation:lmp-link-resource?fdn=MD=CISCO_EPNM!TL=10.58.235.85:49--10.58.235.159:2130706710

Response

- samples/LMP_Link_Delete/response.xml

Request(Optical Static LMP)

- DELETE /restconf/operations/v1/cisco-resource-activation:lmp-link-resource?fdn=MD=CISCO_EPNM!ND=NCS2006-234-143!ADP=PSLINE-1-1-6-RX%26PSLINE-1-1-6-TX

Response(Optical Static LMP)

- samples/LMP_Link_Delete/Static_LMP/response.xml

LMP Link Retrieval

LMP Link is treated like a Topological Link. The Link can be retrieved by specifying the FDN of the Topological Link with the topological link retrieval URL.

Request

- GET URL : https://{server_IP}/restconf/data/v1/cisco-resource-network:topological-link?fdn=MD=CISCO_EPNM!TL=10.58.235.159:2130706714--10.58.235.221:505

Reponse

- samples/LMP_Link_Retrieval/response.xml

Optical Static LMP Retrieval

Optical Static LMP Retrieval is done based on source Node FDN or specific Add Drop Virtual Trunk Port FDN.

Request Node FDN

- GET URL : https://{server_IP}/restconf/operations/v1/cisco-resource-activation:lmp-link-resource?ndFdn=MD=CISCO_EPNM!ND=NCS2006-234-143

Reponse

- samples/LMP_Link_Retrieval/Static_LMP/response_adpFdn.xml

Request ADP FDN

- GET URL : https://{server_IP}/restconf/operations/v1/cisco-resource-activation:lmp-link-resource?fdn=MD=CISCO_EPNM!ND=NCS2006-234-143!ADP=PSLINE-1-1-6-RX%26PSLINE-1-1-6-TX

Reponse

- samples/LMP_Link_Retrieval/Static_LMP/response_ndFdn.xml

1.58 PCE Computation Path

This interface returns optical paths computed between two NCS 2K optical trunk ports, over which an OCH-CC or OCH-NC circuit can be created.

Request

- GET /restconf/data/v1/cisco-resource-network:vc-path?src-tp-fdn=<Source TP FDN>&dest-tp-fdn=<Destination TP FDN>

Response

- samples/PCE_Computation_Path/response.xml
- samples/PCE_Computation_Path/response.json

1.59 OTDR Link Scan

Optical Time Domain Reflectometry is used to provide information about basic characteristic of the Optical fiber among Optical nodes, like Insertion Loss and concentrate point of reflection.

OTDR Scan will be performed on a given topological link. The API is asynchronous in nature. This will initiate a onetime OTDR scan on the OTDR equipment associated with the topological link. The test id associated with the scan will be returned to the user.

The user can download the OTDR SOR file by sending request on the file download URL (e.g., GET /restconf/operations/v1/cisco-network-resource-oam:network-resource-oam-config/otdr-scan-test-sor-file/{test-id}?check-ready=true) with the test id associated to the last scan. The SOR file contain details of the last scan. The User will require a third party SOR file reader to read the SOR file.

NOTE: The default scan mode supported is 'Hybrid'

Sl.no	Name	Type	Description
1	network-resource-oam-request	Container	Holds input request parameters
2	tl-ref	String	FDN of the topological Link
3	scan-direction	QName	Indicates the scan direction to use: Allowed values: a-tx-to-z-rx – Translates to TX a-rx-to-z-tx – Translates to RX z-tx-to-a-rx – Translates to TX z-rx-toa-tx – Translates to RX
4	distance-profile	QName	Indicates the allowed distance profile parameters: Allowed values: scan-auto-mode scan-expert-mode scan-event scan-zone-one (0-1 Km) scan-zone-two (0-25 Km) scan-zone-three (0-80 Km) scan-zone-four (full span)

Request

- POST /restconf/operations/v1/cisco-network-resource-oam:network-resource-oam-config
- samples/OTDR_Link_Scan/request.xml

Response

- samples/OTDR_Link_Scan/response.json

Getting SOR file

URL to Download SOR file:

- GET /restconf/operations/v1/cisco-network-resource-oam:network-resource-oam-config/otdr-scan-test-sor-file/1001?check-ready=true

When Not Ready

- samples/Getting_SOR_File/not_ready.json

When Ready

- samples/Getting_SOR_File/when_ready.txt

NOTE: The OTDR file retrieved via., RESTCONF API will be in .zip format, user needs to unzip the file to get OTDR SOR file.

Getting Scan Results

This request can be used to fetch historical scans performed on EPNM. Below is the list of attributes used to filter the scan.

S.No.	Name	Type	Description
1	network-resource-oam-request	Container	Holds input request parameters
2	resource-ref	FDN	FDN of the Device Controller.
3	scan-type	QName	Indicates the scan type to use: Allowed values: BASELINE LASTSCAN IMPORTED
4	direction	QName	Indicates the allowed direction parameters: Allowed values: TX RX TX_RX

Request

URL to Get Scan Results based on the input parameters passed in the request.

- POST /restconf/operations/v1/cisco-network-resource-oam:network-resource-oam-config/otdr-scan-result
- samples/OTDR_Link_Scan/Get_Scan_Result/request.xml

Response

- samples/OTDR_Link_Scan/Get_Scan_Result/response.xml

Getting Scan Event

This request is used to fetch the Scan Event attributes per OTDR Scan Result.

Request

URL to Get Scan Event based on the scan-result-id passed as a query param in the request.

- GET /restconf/operations/v1/cisco-network-resource-oam:network-resource-oam-config/otdr-scan-result/<scan-result-id>

Response

- samples/OTDR_Link_Scan/Get_Scan_Event/response.xml

1.60 AINS - Automatic In-Service

NCS42xx and ASR9xx platforms shall support to manage equipment and port state model in two modes in default, namely Transport mode and router mode.

In "Transport mode" system shall support subset of generic state requirements for Network Elements (NEs) as per GR1093. In "Router mode" system shall support Cisco standard representation for Equipment and port model.

"Transport mode" is super set of "Router mode".

Operation	Description
Automatic In-Service	This operation to support managing equipment and port state
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-nrf-physical:reserve-equipment
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	provision-equipment-request
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns provision-equipment-response.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.

	Error tag with format PRE.<number> are generated by this API. For example: PRE.0019 for 'Error, found null payload.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-nrf-physical.yang

Below table gives details about input request arguments:

Provision Equipment Request

Sl.no	Name	Type	Description
1	reserve-equipment-request	Container	Holds input request parameters
2	nd-ref	String	FDN of the network device
3	parent-resource-name	String	Slot Names for the AINS
4	product-id	String	Product Id for the AINS

Provision Equipment Response

Sl.no	Name	Type	Description
1	reserve-equipment-respone	Container	Holds response parameters
2	Result	Container	Result container
3	Staus	String	Status of the operation

Request

- POST /restconf/data/v1/cisco-nrf-physical:reserve-equipment
- samples/AINS_Automatic_In_Service/request.xml

Response

- samples/AINS_Automatic_In_Service/response.xml

1.61 Equipment Operations – Reserve, Reload, Provision

NCS2K platforms shall support the ability to reserve/pre-provision a card slot. For cards that already exist, users will have the ability to set the card mode by provisioning the card. Finally, a user may also choose to reload the card.

Operation	Description
Equipment Operation	This operation is to support managing equipment reserve/unreserve.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-nrf-physical:reserve-equipment
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json

Request Data	reserve-equipment-request
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns reserve-equipment-response.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format PRE.<number> are generated by this API. For example: PRE.0019 for 'Error, found null payload.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-nrf-physical.yang

Reserve Equipment

Below is the required inputs to reserve/pre-provision a NCS2K device.

Sl.no	Name	Type	Description
1	reserve-equipment-request	Container	Holds input request parameters
2	nd-ref	String	FDN of the network device
3	parent-resource-name	String	Slot location of the card
4	product-id	String	Product Id for the card
5	resource-type	String	MODULE

Reserve Equipment Response

Sl.no	Name	Type	Description
1	reserve-equipment-response	Container	Holds reserve equipment response parameters
2	nd-ref	String	FDN of the network device
3	parent-resource-name	String	Slot location of the card
4	product-id	String	Product Id for the card
5	resource-type	String	MODULE

6	resource-ref	String(fdn)	Resource reference FDN Eg: MD=CISCO_EPNM!ND=NCS2006-239-56!EQ=name=SLOT-2-8

Request

- POST /restconf/data/v1/cisco-nrf-physical:reserve-equipment
- samples/Reserve_Equipment/request.xml

Response

- samples/Reserve_Equipment/response.xml

Unreserve Equipment

The payload is exactly the same as Reserve Equipment. For response, you will receive a 200 message on success. The only difference is that you must change the payload to be:
`<p:unreserve-equipment-request>`

Reload Equipment

This api allows a user to reload an already provisioned card on an NCS2K device.

Request

- POST /restconf/data/v1/cisco-nrf-physical: reload-equipment
- samples/Unreserve_Equipment/request.xml

Response

- 200 Response on success.

Provision Equipment (Card Mode)

Allows a user to set the card operating mode for a card. For available card operating modes, see the yang file.

Request

- POST /restconf/data/v1/cisco-nrf-physical:provision-equipment
- samples/Provision_Equipment_Card_Mode/request.xml

Response

- samples/Provision_Equipment_Card_Mode/response.xml

Unprovision Equipment (Card Mode)

Allows a user to delete the card mode for a specific card. Request and response are essentially the same. Main difference being change from provision to unprovision:
`<p: unprovision-equipment-response />`
and operation from "create" to "delete"

Request

- POST /restconf/data/v1/cisco-nrf-physical:unprovision-equipment
- samples/UnProvision_Equipment_Card_Mode/request.xml

Response

- samples/UnProvision_Equipment_Card_Mode/response.xml

Provision Card Configuration(Create)

Allows a user to set the setting trunk bit , client bit rate on different card mode. For available card modes, see the yang file.

Resource	Description			
Card Configuration	Card Configuration Create			
HTTP Method	**CREATE**			
POST	/restconf/operations/v1/cisco-nrf-physical:provision-card-configuration?{fdn}			
Input Parameters				
Name	**Type**	**Allowed Values**	**Description**	
resource-ref	String(FDN)		Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS4206-120.19	
card-mode	String	MUXPONDER SLICE REGEN	Muxponder - In this mode, both trunk ports are configured with the same trunk rate. The client-to-trunk mapping is in a sequence. Muxponder slice - In this mode, each trunk port is configured independent of the other with different trunk rates. The client-to-trunk mapping is fixed. For Trunk 0, the client ports are 2 through 7. For Trunk 1, the client ports are 8 through 13. Regeneration Mode - In Regeneration (Regen) mode, the OTN signal is received on a trunk port and the regenerated OTN signal is sent on the other trunk port of the line card and the other way round.	
slice-number	Integer	Skinny BO card - 0 to 5 Other cards - 0,1	Indicates slice to which card mode is to be configured. Mandatory for Slice card mode	
client-bit-rate	String	100GE OTU4 400GE	Client data rate to be supported. Mandatory for Slice & Muxponder. Not supported for RegenMode	
trunk-bit-rate	String	SliceMode - 100G,200G,300G, 400G,500G,600G MuxponderMode-50G,100G,150G,2 00G,250G,300G,4 50G,500G,550G,6 00G RegenMode - 100G,200G,300G, 400G,500G,600G	Trunk data rate to be supported. Mandatory for all card modes	

lldp-drop	String	true / false	For NCS1004 Bellatrix 2x400G LC Card mode **MUXPONDER** : LLDP-DROP Port Supported **SLICE** : LLDP-DROP Port supported except client-bit-rate as OTU4 **REGEN** : Not Supported
Response Message			
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json		
Response Data	The `provision-card-configuration-response–` see yang model for the data details. And result of modification on the feature.		
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.		

Request

- POST /restconf/data/v1/cisco-nrf-physical:provision-card-configuration
- samples\Card_Mode_Configuratioin_Create\request.xml

Response

samples\Card_Mode_Configuratioin_Create\response.xml

Provision Card Configuration(Delete)

Allows a user to set the setting trunk bit , client bit rate on different card mode. For available card modes, see the yang file.

Resource	Description
Card Configuration	Card Configuration Delete
HTTP Method	**DELETE**
DELETE	/restconf/operations/v1/cisco-nrf-physical:provision-card-configuration?{fdn}
Response Message	
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json
Response Data	The `provision-card-configuration-response–` see yang model for the data details. And result of modification on the feature.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.

Request

- `DELETE /restconf/data/v1/cisco-nrf-physical:provision-card-configuration`
- `samples\Card_Mode_Configuratioin_Delete\request.xml`

Response

- samples\Card_Mode_Configuratioin_Delete\response.xml

Provision Card Configuration(Retrieval)

Allows a user to Retrieve Card Configuration by resource FDN. For available card modes, see the yang file.

Resource	Description
Card Configuration	Card Configuration Retrieval
HTTP Method	**GET**
GET	/restconf/operations/v1/cisco-nrf-physical:provision-card-configuration?{fdn}
Response Message	
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json
Response Data	The `provision-card-configuration-response`– see yang model for the data details. And result of modification on the feature.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.

Response

- samples\Card_Mode_Configuratioin_Retrieve\response.xml

Provision Line Card Configuration (Create)

Allows a user to set the Line Card mode configuration. For available Line card modes, see the yang file.

Configuration of new LC mode follows below steps:
1.Action: CONFIGURE - To configure new LC Mode. Once configured, status would be set as RUNNING in get call.
2.Action: DELETE - To delete Existing LC Mode. Once deleted, status would be set as DELETED in get call.
3.Action: RELOAD - To reload the card. Once card is reloaded, status would be set as NOT_SET in get call.

Resource	Description
Line Card Mode Configuration	Line Card Mode Configuration POST. Action: CONFIGURE/RELOAD

HTTP Method	CREATE
POST	\<server-ip\>/restconf/operations/v1/cisco-nrf-physical: provision-line-card-mode-configuration?(fdn)

Input Parameters

Name	Type	Description
Line Card Mode Configuration		Line Card Mode Configuration POST. Action: CONFIGURE/RELOAD
resource-ref	FDN	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-23!EQ=name=0-1
line-card-mode	String	Supported Line Card Modes: 4x100G-MXP-400G-TXP, 40x10G-4x100G-MXP, 4x100GE-MXP-DD, OTUCn-REGEN, FC-MXP, 2x100GE-TXP-MXP, 10G-GREY-MXP, 400GE-TXP-DD. This field is **Mandatory**
line-card-mode-action-type	Enum	Indicates what action to perform. Action Types: CONFIGURE - Configuring LC mode on the card so that status is set as RUNNING. DELETE - Delete the existing LC mode on the card so that Status is set as DELETED. RELOAD - Reload the card to make status as NOT_SET This field is **Mandatory**

Response Message

Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json
Response Data	The `provision-line-card-mode-configuration-response` – see yang model for the data details. And result of modification on the feature.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB

	API Error Codes Reference.xlsx
Yang file name	cisco-nrf-physical.yang

Request

- POST /restconf/operations/v1/cisco-nrf-physical: provision-line-card-mode-configuration?(fdn)
- /samples/Provision_Create_LC_Mode/Request.xml

Response

- /samples/Provision_Create_LC_Mode/response.xml

Provision Line Card Configuration (Delete)

Allows a user to delete existing Line Card mode Configuration.

Resource	Description
Line Card Mode Configuration	Line Card Mode Configuration POST. Action: DELETE
HTTP Method	**DELETE**
DELETE	\<server-ip\>/restconf/operations/v1/cisco-nrf-physical: provision-line-card-mode-configuration?(fdn)
Input Parameters	

Name	Type	Description
Line Card Mode Configuration		Line Card Mode Configuration POST. Action: DELETE
resource-ref	FDN	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-23!EQ=name=0-1
line-card-mode	String	Supported Line Card Modes: 4x100G-MXP-400G-TXP, 40x10G-4x100G-MXP, 4x100GE-MXP-DD, OTUCn-REGEN, FC-MXP, 2x100GE-TXP-MXP, 10G-GREY-MXP, 400GE-TXP-DD. Mandatory.
line-card-mode-action-type	Enum	Indicates what action to perform. Supported Action Type: DELETE - Delete the existing LC mode on the card so that Status is set as DELETED. Mandatory.
Response Message		
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json	
Response Data	The `provision-line-card-mode-configuration-response` – see yang model for the data details. And result of modification on the feature.	

HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-nrf-physical.yang

Request

- DELETE /restconf/operations/v1/cisco-nrf-physical:provision-line-card-mode-configuration?(fdn)
- /samples/Delete_LC_Mode/Request.xml

Response

- /samples/Delete_LC_Mode/response.xml

Provision Line Card Mode Configuration (Retrieval)

Allows a user to Retrieve Card Configuration by resource FDN. For available card modes, see the yang file.

Resource	Description
Line Card Mode Configuration	Fetch Line Card Mode Configuration on card.
HTTP Method	**Resource Path**
GET	/restconf/operations/v1/cisco-nrf-physical: provision-line-card-mode-configuration?{fdn}
Response Message	
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json
Response Data	The provision-line-card-mode-configuration-response– see yang model for the data details. And result of modification on the feature.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.
Application Error Codes	Response with error condition provides error tag in error-app-tag element.

(error-app-tag)	
	If error is from underlying framework/core modules error-app-tag format one of following
• FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
• CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials

For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx |
| Yang file | cisco-nrf-physical.yang |

*Note: Above API support is applicable only for BO card

Response

- /samples/Provision_Create_LC_Mode/Request.xml

1.62 Protection Switch Action

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

Operation	Description
protection-switch	This operation can be used to apply protection switch to service.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-service-action:protection-switch
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	protection-switch-service-action-request
Authorization Required	One or more from following
• Chassis View Read and Write
• MBC UI Framework Access
• Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns protection-switch-service-action-response.
HTTP Status Code	• 200 OK - Success with response message-body
• 401, 403 – Authentication and Authorization errors.
• 400 Bad Request - Invalid request message.
• 500 Internal Server Error - operation-failed.
Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.

Error tag with format CFS.<number> are generated by this API. For example: CFS.0003 for 'Error in calling Optical Protection Switch Service: %s'

If error is from underlying framework/core modules error-app-tag format one of |

	following
	• FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
	• CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
	For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	Cisco-service-action.yang

Protection-switch-service-action-request

attribute	Data Type	Description
vc-ref	String(fdn)	Fdn of the service Eg: MD=CISCO_EPNM!CFS=AGELMO_OCHNC-PSM-PROTECTED_CTC
action-type	Enum	Accepts following values • force-switch • manual-switch • clear • lockout • clearlockout
protection-role	Enum	Accepts following values • working-path • protect-path • restore-path

Protection-switch-service-action-response

attribute	Data Type	Description
vc-ref	String(fdn)	Fdn of the service Eg: MD=CISCO_EPNM!CFS=AGELMO_OCHNC-PSM-PROTECTED_CTC
status	String	Status of the operation with following values COMPLETED ACTION_FAILED
result	String	Result of the operation
node-ref	String(fdn)	Fdn of the node Eg: MD=CISCO_EPNM!ND=454A-234-50
device-configuration	String	Actual device configuration when the operation is applied to the device

Force Switch on Working Path

Request
```
POST /restconf/data/v1/cisco-service-action:protection-switch
```
• samples/Force_Switch_on_Working_Path/request.xml

Response
• samples/Force_Switch_on_Working_Path/response.xml

Force switch on Protected Path

Request

- POST [/restconf/data/v1/cisco-service-action:protection-switch](#)
- [samples/Force_Switch_on_Protected_Path/request.xml](#)

Response

- [samples/Force_Switch_on_Protected_Path/response.xml](#)

Lockout on Working Path

1.62.1.1   *Request*

POST [/restconf/data/v1/cisco-service-action:protection-switch](#)
- [samples/Lockout_on_Working_Path/request.xml](#)

1.62.1.2   *Response*

- [samples/Lockout_on_Working_Path/response.xml](#)

Manual switch on working path

Request

- POST [/restconf/data/v1/cisco-service-action:protection-switch](#)
- [samples/Manual_Switch_on_Working_Path/request.xml](#)

Response

- [samples/Manual_Switch_on_Working_Path/response.xml](#)

Manual switch on Protected path

Request

- POST [/restconf/data/v1/cisco-service-action:protection-switch](#)
- [samples/Manual_Switch_on_Protected_Path/request.xml](#)

Response

- [samples/Manual_Switch_on_Protected_Path/response.xml](#)

Clear Action –Protection Switch

Request

- POST [/restconf/data/v1/cisco-service-action:protection-switch](#)
- [samples/Clear_Action_Protection_Switch/request.xml](#)

Response

- [samples/Clear_Action_Protection_Switch/response.xml](#)

1.63 Service Action

The set of operations defined under service action can be used to perform revert, upgrade restore and re-route an optical service. The Operation type supported is PUT. The user has to provide the VC FDN as an argument to the service action URL.

Resource	Description
Virtual Connection	The service action specified by the URL is performed on the VC provided as a query parameter to the URL. The

HTTP Method	Resource Path
PUT	/restconf/operations/v1/cisco-service-action:restore-revert /restconf/operations/v1/cisco-service-action:restore-upgrade /restconf/operations/v1/cisco-service-action:restore-reroute

Query Parameters		
Name	**Type**	**Description**
vcFdn	String	The Virtual Connection FDN on which the service action has to be performed MD=<CISCO_EPNM>!VC=Trail-OCH-Test Eg: /restconf/operations/v1/cisco-service-action:restore-revert ?vcFdn= MD=<CISCO_EPNM>!VC=Trail-OCH-Test

Authorization Required	One or more from following • Circuit or VC Provisioning

Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	The service action result with the configuration command will be returned on a successful operation, else a result indicating the failure of service action will be returned. The response will be of type **service-action-response**– see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format CFS.<number> are generated by this API. For example: CFS.0016 for 'Error when executing restore revert operation: %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang File Name	cisco-service-action.yang

Service Action Restore-Revert

This operation allows a user to perform a manual revert of a service. The query parameter input should be a valid VC FDN.

- **Pre-Condition**: The restoration status of the service should be RESTORED & REVERTIBLE for the manual revert operation to succeed.

- **Post-Condition**: On successful completion of the switchRoute (manual Revert), the service will go back to its original path. The restoration status will change to NONE.

Request

- PUT /restconf/operations/v1/cisco-service-action:restore-revert?vcFdn=MD=CISCO_EPNM!VC=TRAIL-100G_final

Response

- samples/Service_Action_Restore_Revert/response.xml

Service Action Restore-Upgrade

This operation allows a user to perform an upgrade and restore a service. The query parameter input should be a valid VC FDN.

- **Pre-Condition:** The restoration status of the service should be RESTORED or RESTORED & REVERTIBLE.
- **Post-Condition:** On successful completion of setIntentedRoute (upgradeRestore), the current restoration path will be set as the working path. Restoration Status will be set to NONE.

Request

- PUT /restconf/operations/v1/cisco-service-action:restore-upgrade?vcFdn=MD=CISCO_EPNM!VC=TRAIL-100G_final

Response

- samples/Service_Action_Restore_Upgrade/response.xml

Service Action Restore-Reroute

This operation allows a user to perform a re-route of the Virtual connection if there is an alternate path existing. The query parameter input should be a valid VC FDN. There is no pre-condition required for this operation.

- **Post-Condition:** On successful completion of alternate path will be set as the working path. Restoration Status will be set to NONE.

Request

- PUT /restconf/operations/v1/cisco-service-action:restore-reroute?vcFdn=MD=CISCO_EPNM!VC=TRAIL-c-e_new_2

1.64 Client Port

OTN-XP under NCS1004 platform shall support to manage equipment and client ports.

OTN-XP supports different client ports based on the Card Mode and Line Card Operating Mode configured, and the supported clint and other details are as follows,

LC MODE	Config Type	Card Mode	Trunk Rate	Client Port Rate	Slice	Client Port	Trunk Port	Lane ID
4x100G-MXP-400G-	400G MXP	MUXPONDER SLICE	400G	100GE, OTU4	0	1, 6, 7, 10	12	NA
					1	0, 4, 5, 8	13	
	400G	MUXPONDER	400G	400GE	0	10	12	NA

TXP	Type	Slice	Rate	Modes	Idx	Lanes	No.	Lane Mapping
TXP	TXP	SLICE				8	13	
	200G MXP	MUXPONDER SLICE	200G	100GE, OTU4	0	7, 10	12	NA
					1	5, 8	13	
	300G MXP	MUXPONDER SLICE	300G	100GE, OTU4	0	6, 7, 10	12	NA
					1	4, 5, 8	13	
40x10G-4x100G-MXP	10x10G + 3 x 100G	MUXPONDER SLICE	400G	10GE, 100GE, OTU4, OTU2, OTU2e	0	100G - 0, 1, 6	12	NA
						10G – 2, 4, 5		Lane 1, 2 – Port 2 Lane ALL – 4, 5
	40x10G	MUXPONDER SLICE	400G	10GE, OTU2, OTU2e	0	0, 1, 2, 3, 4, 5, 6, 7, 9, 11	12	1, 2, 3, 4
	30x10G + 1 x 100G	MUXPONDER SLICE	400G	10GE, 100GE, OTU2, OTU2e, OTU4	0	100G – 6	12	NA
						10G – 0, 1, 2, 3, 4, 5, 9, 11		Lane ALL – Port 0, 1, 2, 3, 4, 5, 9 Lane 1, 2 – Port 11
	30x10G	MUXPONDER SLICE	300G	OTU2E, 10GE, OTU2	0	10G - 0, 1, 2, 3, 4, 5, 9, 11	12	Lane ALL - 0, 1, 2, 3, 4, 5, and 9 Lane 1, 2 - 11
	20x10G + 1 x 100G	MUXPONDER SLICE	300G	100GE, 10GE, OTU2, OTU2E	0	100G - 0	12	NA
						10G - 1, 2, 4,5, 9, 11		Lane ALL – 1, 4, 5, 9 Lane 3, 4- 2 Lane 1, 2 – 11
	20x10G + 2 x 100G	MUXPONDER SLICE	400G	100GE, OTU4, OTU2E, 10GE, OTU2	0	100G – 0, 1	12	NA
						10G – 2, 4, 5, 6, 7, 11		Lane ALL- 4, 5, 6, 7 Lane ALL – 3, 4 – 2, 11
	10x10G + 2 x 100G	MUXPONDER SLICE	300G	100GE, OTU2E, OTU2, 10GE	0	100G – 0, 1	12	NA
						10G – 2, 4, 5		Lane ALL - 4, 5 Lane 3, 4 - 2
	10x10G + 1x100G	MUXPONDER SLICE	200G	100GE, 10GE	0	10G – 2, 4, 5 100G - 0	12	Lane ALL - 4, 5 Lane 3, 4 - 2
					1	10G – 6, 7, 11 100G - 1	13	Lane ALL – 6, 7 Lane 3, 4 - 11

4x100GE-MXP-DD	4x400G-MXP-DD	MUXPONDER SLICE	400G	100GE	0	1, 6, 7, 10	11	NA
					1	0, 4, 5, 8	9	
	400G-TXP-DD	MUXPONDER SLICE	400G	400GE	0	10	11	NA
					1	8	9	
	3x100GE-MXP-DD	MUXPONDER SLICE	300G	100GE	0	1, 7, 10	11	NA
					1	4, 5, 8	9	
	2x200G MXP-DD	MUXPONDER SLICE	200G	100GE	0	7, 10	11	NA
FC-MXP	16G FC-MXP	MUXPONDER SLICE	400G	16GFC	0	1, 6, 7, 9, 10, 11	12	Lane All – All Ports
					1	0, 2, 3, 4, 5, 8	13	
	32G FC-MXP	MUXPONDER SLICE	400G	32GFC	0	9, 10, 11	12	Lane All – All Ports
OTUCn REGEN	NA	REGEN MODE	400G	NA	NA	NA	NA	NA

Below table gives details about input request arguments:

Provision Client Port Request

Operation	Description
Client/Pluggable Port	This operation to support managing equipment and port state
HTTP Method	POST
Resource Path	/restconf/operations/v1/cisco-nrf-physical:pluggable-port
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	provision-equipment-request
Authorization Required	One or more from following. - Chassis View Read and Write - MBC UI Framework Access - Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns provision-pluggable-port-response
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format PRE.\<number> are generated by this API. For example: PRE.0019 for 'Error, found null payload.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number> - any tag starting with "FW." prefix for any internal

			errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
Yang file name			cisco-nrf-physical.yang

Sl.no	Name	Type	Description
1	provision-pluggable-port-request	Container	Holds input request parameters
2	resource-ref	String	FDN of the Equipment
3	port-number	String	Port number
4	client-bitrate	String	Client bit rate for selected port
5	lane-id	Integer	Lane ID for the selected port and it is supported for a particular client bit rate for a specific configuration. **Not Mandatory** field
6	slice-number	Integer	Slice number to configure client port. **Mandatory** field

Request

- `POST /restconf/data/v1/cisco-nrf-physical:pluggable-port`
- samples/Pluggable_Port_Create/1.request.xml

Provision Client Port Response

Sl.no	Name	Type	Description
1	provision-pluggable-port-response	Container	Holds response parameters
2	Result	Container	Result container
3	Status	String	Status of the operation

Response

- samples/Pluggable_Port_Create/1.response.xml

Delete Client Port Request

Operation	Description
Client/Pluggable Port	This operation to support managing equipment and port state
HTTP Method	DELETE
Resource Path	/restconf/operations/v1/cisco-nrf-physical:pluggable-port
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	provision-pluggable-port-request
Authorization Required	One or more from following. • Chassis View Read and Write • MBC UI Framework Access

	• Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns provision-pluggable-port-response
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format PRE.<number> are generated by this API. For example: PRE.0019 for 'Error, found null payload.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
Yang file name	cisco-nrf-physical.yang

Sl.no	Name	Type	Description
1	provision-pluggable-port-request	Container	Holds input request parameters
2	resource-ref	String	FDN of the Equipment
3	port-number	String	Port number
4	client-bitrate	String	Client bit rate for selected port
5	lane-id	Integer	Lane ID for the selected port and it is supported for a particular client bit rate for a specific configuration. **Not Mandatory** field
6	slice-number	Integer	Slice number to configure client port. **Mandatory** field

Request

- DELETE /restconf/data/v1/cisco-nrf-physical:pluggable-port
- samples/Pluggable_Port_Delete/1.request.xml

Delete Pluggable Port Response

Sl.no	Name	Type	Description
1	provision-pluggable-port-response	Container	Holds response parameters

2	Result	Container	Result container
3	Status	String	Status of the operation

Response

- samples/Pluggable_Port_Delete/1.response.xml

Client Port Retrieval

Operation	Description
Client/Pluggable Port	This operation to support managing equipment and port state
HTTP Method	GET
Resource Path	/restconf/operations/v1/cisco-nrf-physical:pluggable-port?fdn=<Equipment FDN>
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	One or more from following. • Chassis View Read and Write • MBC UI Framework Access • Network Devices
Response Message	
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Response Data	Returns provision-pluggable-port-response
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format PRE.<number> are generated by this API. For example: PRE.0019 for 'Error, found null payload.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
Yang file name	cisco-nrf-physical.yang

Request

- GET URL : https://{server_IP}/restconf/operations/v1/cisco-nrf-physical:pluggable-port?fdn=MD=CISCO_EPNM!ND=EPNNCS1004-124-24.cisco-lab.com!EQ=name=0/0

Response

S.No.	Name	Type	Description
1	provision-pluggable-port-response	Container	Holds list of pluggable ports Response
2	provision-pluggable-ports	Container	Contains list of pluggable ports
3	resource-ref	FDN	FDN of the Device Equipment Controller.
4	port-number	String	Port number
5	slice-number	String	Slice number to configure client port
6	client-bitrate	String	Client bit rate for selected port
7	lane-id	String	Lane ID for the selected port and it is supported for a particular client bit rate for a specific configuration

- samples/Pluggable_Port_Retrieve/1.response.xml

1.65 Provision 5G slot mode to EOWYN Line card

This API helps operator to provision 5G slot mode in Eowyn line card. Details about input request argument are explained in the table below:

Sl.no	Name	Type	Description
1	node-ref	String(FDN)	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS4206-120.19
2	operating-mode	Container	Container for the possible modes
3	Mode	String	Indicates mode to be used. Allowed values are: EQ_MODE_10G EQ_MODE_5G EQ_MODE_TXPP_10G EQ_MODE_TXP_10G EQ_MODE_TXP_100G EQ_MODE_RGN_10G EQ_MODE_RGN_100G EQ_MODE_MXP_10_10G EQ_MODE_MXP_2x40G EQ_MODE_LOW_LATENCY EQ_MODE_FANOUT_10_10G EQ_MODE_OC3 EQ_MODE_OC12 EQ_MODE_T1 EQ_MODE_E1 EQ_MODE_NONE EQ_MODE_8G

			EQ_MODE_8G_1G
			EQ_MODE_8G_10G
			EQ_MODE_8G_2G
			EQ_MODE_ONE_10G
			EQ_MODE_16G_10G
			EQ_MODE_16G_10G_OS
			EQ_MODE_18G
			EQ_MODE_18G_OS
			EQ_MODE_16G
			EQ_MODE_16G_OS
			EQ_MODE_17G
			EQ_MODE_17G_OS
			EQ_MODE_4_PORTS_ONLY
4	resource-name	String	Slot to be used e.g. slot0/3
Yang file name		cisco-nrf-physical.yang	

Request

- POST /restconf/data/v1/cisco-nrf-physical:provision-equipment
- samples/Provision_5G_Slot_Mode_to_EOWYN_Line_Card/request.xml

Response

HTTP/1.1 201 Created
Server: <epnm-host>
Content-Type: application/yang.operation+xml

- samples/Provision_5G_Slot_Mode_to_EOWYN_Line_Card/response.xml

1.66 Device Synchronization

This API synchronize the device managed by EPNM to the device on the network.

Resource	Description
Node	Synchronize the node in EPNM to the device on the network.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-nrf-physical:synchronize-node
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **synchronize-node-request** – see yang model for the data details.
Authorization Required	One or more from following • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more response of type **synchronize-node-response** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed.

	Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format SYNC.\<number\> are generated by this API. For example: SYNC.0003 for 'Errors encountered synchronizing nodes' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-nrf-physical.yang

Device Synchronization Request/Response

Request

- samples/Device_Synchronization/request.xml
- samples/Device_Synchronization/request.json

Response

- samples/Device_Synchronization/response.xml
- samples/Device_Synchronization/response.json

1.67 Node Configuration - Set Admin State

This API allows to set admin state of the multiple devices managed by EPNM to the devices on the network. The request payload must be correct, otherwise it results in failure. It shows error message which needs to be corrected before sending the request. It does not allow partial execution. It results in success or failure.

Resource	Description
Node	Configure the node in EPNM to the device on the network.
HTTP Method	**Resource Path**
POST	/restconf/operations/v1/cisco-nrf-physical:set-node-configuration
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Request Data	Request data of type **node-configuration-request** – see yang model for the data details.
Authorization Required	One or more from following • Network Devices
Response Message	
Response Content Type	application/xml, application/yang-data+xml, application/json, application/yang-data+json
Response Data	0 or more response of type **node-configuration-response** – see yang model for the data details.
HTTP Status Code	• 200 OK - Success with response message-body

	• 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.
Yang file name	cisco-nrf-physical.yang

Node Configuration – Admin State Request/Response

Request

- samples/Set_Admin_State/request.xml
- samples/Set_Admin_State/request.json

Response

- samples/Set_Admin_State/response.xml
- samples/Set_Admin_State/response.json

Troubleshooting

The table below provides some issues you might encounter when setting up the OSS integration layer. It also describes the steps to troubleshoot each issue.

Problem Description	Indication	Probable Cause	Troubleshooting Procedure
No response to HTTP GET request	Client reports it could not get any response to the query (server is not listening at port).	Server is down. SSL certificate not installed.	Verify that server is up by logging through GUI. Install SSL certificate on server. Then examine logs/console.log for errors.
401 or 403	Server returns 404 Not Found and "No service was found."	The credentials are incorrect.	Verify that a basic Authorization header with valid user/password is included in the request.
Module not found	Server returns 500 Internal Server Error and an error message stating that the module was not found.	The URL is incorrect.	Issue a ../restconf/vi/modules request to get a list of supported URLs and correct the URL in the request.
Invalid column	Server returns 500 Internal Server Error and an error message stating that "x is not a valid column in the database".	The query arguments contain an invalid column name, pagination directive, or sorting directive.	Correct the column or directive in the query parameters.
No content	Server returns 204 No Content and no message body.	The query arguments or the URL do not match any objects.	Alter the URL or the query parameters to match one or more objects.
Data are returned in the wrong format	Expected XML format and retrieved JSON. Expected JSON format and retrieved XML.	Accept header missing or incorrect in the request.	Specify application/<desired format> in the Accept header.
Server error with no error message	Sent a valid URL and server returns a 500 Internal Server Error with no error message field.	Unsupported format in Accept header.	Specify supported format in the Accept header.
Server returns an array with no records	Server returns 200 OK and a body with an empty of the requested object type.	No objects of the requested type in the database.	Verify that services that generate this type of object are provisioned in Cisco EPN Manager.

Duplicate Circuit Name Limitation

*NOTE: Circuit Name Duplication can be allowed if service created from UI or CTC with different optical ports. But NBI has validation which will not allow for duplication for the same endpoints or different interface. If duplicate service created from UI or CTC, then from NBI side getCFS (https://<IP>/restconf/data/v1/cisco-service-network:customer-facing-service) or getVC call (https://<IP>/restconf/data/v1/cisco-service-network:virtual-connection) will fetch any one of the services. That is the limitation NBI has.

YANG Schema for Cisco EPN Manager RESTCONF NBI Data Modules

Download Yang and XSD Schema files.

1.68 Yang Modules

List Supported Yang Modules

Request

GET /restconf/data/ietf-yang-library:modules-state HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

Response
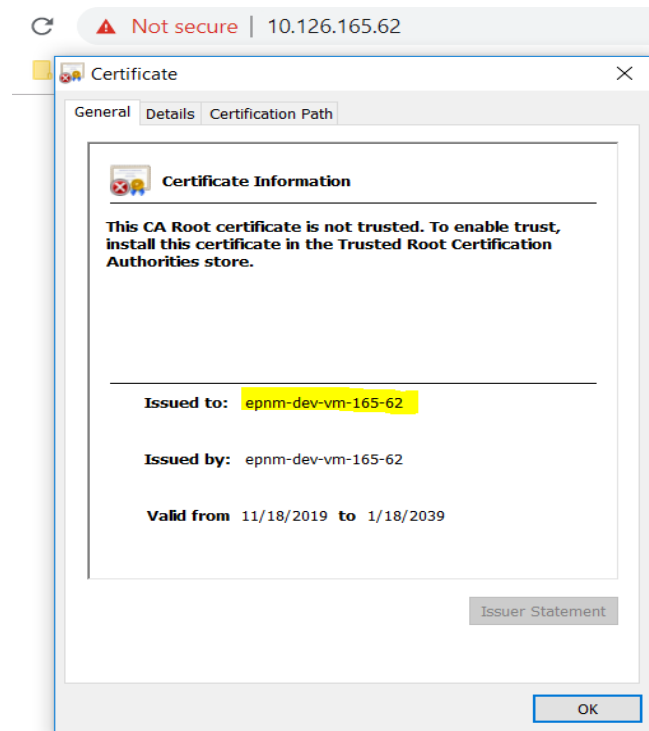
- samples/List_Supported_Yang_Modules/response.xml

Notifications

Currently, notifications are supported using two different mechanisms:
- Connection-oriented notifications, using websockets
- Connectionless notifications

Note : While subscribing for notification, use same host name as configured in the certificate of that particular EPNM server. Please refer below screen shot for more clarity.

Note : When notification clients are running and user needs to import devices, make sure that import of devices should not be greater than 500 devices at a time. The next set of 500 devices to be imported only when previous 500 devices are in managed and synchronized state. Under load notification can be received with some delay which is noted between 2 to 6 minutes.

1.69 Supported notification types

- Inventory notifications - supported via both connection-oriented and connectionless mechanisms. This is disabled by default.
- Alarm notifications - supported via both connection-oriented and connectionless mechanisms. This is disabled by default.
- Service Activation notifications - supported via both connection-oriented and connectionless mechanisms
- Template-execution notifications – supported via both connection-oriented and connectionless mechanisms
- High-Availability (HA) notifications - supported only via connectionless notifications since a persistent connection cannot be expected during the course of a failover or failback.
- "all" – you may provide the value "all" to listen for all notifications listed above

All the above notifications share the same schema.

1.70 Enabling Inventory and Alarm Notifications

By default, inventory and alarm notifications are disabled. To enable them, open the file located at:

- /opt/CSCOlumos/conf/restconf/restconf-config.properties

To enable inventory notifications, set the property below to 'true':

- epnm.restconf.inventory.notifications.enabled=true

To enable alarm notifications, set the property below to 'true':

- epnm.restconf.alarm.notifications.enabled=true

1.71 Notification Subscription Count Limits

These values are configurable from the server at:

- /opt/CSCOlumos/conf/restconf/restconf-config.properties
  - You will then need to restart EPNM for these changes to take effect.

Configurable Limits and their default Values:

- epnm.restconf.notification.subscription.limit=250
  - Represents the total number of allowed subscriptions regardless of topics
- epnm.restconf.notification.inventory.subscription.limit=50
  - Represents the total number of allowed inventory subscriptions
- epnm.restconf.notification.alarm.subscription.limit=50
  - Represents the total number of allowed alarm subscriptions
- epnm.restconf.notification.service.activation.subscription.limit=50
  - Represents the total number of allowed service activation subscriptions
- epnm.restconf.notification.template.execution.subscription.limit=50
  - Represents the total number of allowed template execution subscriptions
- epnm.restconf.notification.all.subscription.limit=50
  - Represents the total number of allowed subscriptions with the topic "all"

1.72 Notification URLs

Connection-Less

/restconf/data/v1/cisco-notifications:subscriptions/

Connection-Oriented (Websocket)

- /restconf/streams/v1/inventory
- /restconf/streams/v1/alarm
- /restconf/streams/v1/service-activation
- /restconf/streams/v1/template-execution
- /restconf/streams/v1/all

1.73 Connection-oriented Notifications

The following is the workflow in the case of "connection-oriented" inventory notifications:

- The client subscribes to a predefined URL using a websocket client using basic authentication through a secure HTTPS channel.

- URL: https://<epnm-server-fully-qualified-domain-name>/restconf/streams/v1/**{notification-type}{.xml | .json}**
  - where {notification-type} can be either "inventory" or "service-activation" or "alarm"or "template-execution"
  - and appending the url with ".xml" will result in notifications serialized to xml format and ".json" will result in notifications serialized to json
  - Filters are optional and may be provided as a query parameter:
    - /restconf/streams/v1/{notification-type}{.xml | .json}**?{filterType1}={filterValue1}&{filterType2}={filterValue2}**
      - filter values should be URI encoded
      - productType=Cisco ASR 4000 should be encoded as: productType=Cisco%20ASR%204000
  - **Authentication**: Basic auth
- If the client has provided all required information and if the provided user passes the authorization phase, a secure connection channel is established between the Cisco EPN Manager server and the client.
- Once the connection is established, the same connection will be kept alive throughout the lifecycle of the application.
  - the lifecycle here is governed by the following cases:
    - until the client disconnects from the server
    - until the server goes down either for maintenance or during a failover.
- As long as the connection is kept alive, a notification of type push-change-update is sent from the Cisco EPN Manager server to all clients that are listening for notifications.
- The yang schema for the cisco-yang-push has been included above.

A sample client for subscribing and listening to connection-oriented notifications is provided in the next section. Connectionless notifications can be received by any REST service accepting an XML or JSON payload via a POST request.

1.74 Connectionless Notifications

The following is the workflow in the case of "connectionless" notifications:
- The user is expected to a REST webservice that is capable of accepting XML and/ or JSON payloads as a POST request. This REST service is the endpoint to which the Cisco EPN Manager restconf notifications framework publishes notifications to.
- User subscribes to notifications by providing the REST service endpoint along with the topic to subscribe to. In this case, the topic will be "inventory"
  - **URL**: https://{server}/restconf/data/v1/cisco-notifications:subscription
  - **Method**: POST
  - **Authentication**: Basic Authentication
  - **Example Payload**:
  - samples/notifications/connection_less_request.xml
  - samples/notifications/connection_less_request.json
    where,
    - the endpoint-url is a REST service capable of accepting XML or JSON payloads as a POST request deployed in {server} at {port} using {context}. The notifications are then sent as POST payload to this endpoint-url. The REST service can then handle the notifications from the incoming POST message in any way that is desired.
    - {topic} can be either "inventory", "service-activation", "alarm", "template-execution" or "ha"
- There can be any number of subscriptions to the same type of notification.
- To get the list of notifications that the current user has access to, the following request can be used:
  - **URL**: https:// {server}/restconf/data/v1/cisco-notifications:subscription

- o **Method**: GET
- o **Authentication**: Basic Authentication
- o **NOTE**: "root" user can see subscriptions made by any user while any non-root user can see only notification details that they subscribed to.
- o samples/notifications/subscription_retrieval.xml
- To get details of a single subscription:
  - o **URL**: /restconf/data/v1/cisco-notifications:subscription/{subscription-id}
  - o **Method**: GET
  - o **Authentication**: Basic Authentication
- To delete a subscription:
  - o **URL**: /restconf/data/v1/cisco-notifications:subscription/{subscription-id}
  - o **Method:** DELETE
  - o **Authentication:** Basic Authentication

1.75 Notification Filters

Filter Support

Filters are supported for the following notification types:
- Inventory
- Alarms

Filter Notes

These are some things to look out for when using notifications:
- When using connection-oriented filters, the filter value should be properly URI encoded when using filter values with spaces
- Example: productType=Cisco ASR 4000 should be encoded as: productType=Cisco%20ASR%204000
- For connection-less, since the value is read as a string, it is ok to provide the space: "push.value":"Cisco ASR 4000"

Virtual Domain Filters

Notifications are filtered based on virtual domain users. This will happen automatically when you specify the user/password information when subscribing.
- **NOTE**: "root" user can see subscriptions made by any user while any non-root user can see only notification details that they subscribed to.

elementType Filters

Notifications of the provided elementType will only be sent when this filter is provided. The filter value will correspond to the yang container element name.
The following are the current supported elementTypes filter values:
- o customer
- o customer-facing-service
- o equipment
- o ipsla-profile-details
- o link-aggregation-group
- o ni
- o node
- o physical-connector
- o qos-profile
- o shared-risk-resource-group
- o shared-risk-resource-group-pool

- o shared-risk-resource-group-pool-type
- o termination-point
- o topological-link
- o virtual-connection
- o virtual-connection-multi-layer-route-list
- o RC_Node

Subscribing with multiple elementType filters is supported. A subscription with the filters below will receive both RC_Node notifications AND Equipment notifications.
- o elementType=RC_Node&elementType=Equipment

```
Sample Connection-less subscription
samples/notifications/subscription payload.json
```
Sample Connection-oriented subscription
/restconf/streams/v1/inventory.json?elementType=physical-connector
/restconf/streams/v1/inventory.json?elementType=node&elementType=physical-connector

Device Level Filters

Device level filters are applicable for the following notification types
- inventory
- alarms

The following filters may be used when looking for notifications that match a certain device property
- productType
- productFamily
- productSeries
- group
- ndFdn

A list of all supported product type/series/family may be found by accessing the "Supported Devices" page in EPNM. This page may be accessed with the URL:
- https://{server}/webacs/welcomeAction.do?commandType=abridgedShell#href=applications/swim/supported_devices/supportedDevices.html

Filters of the same key will be treated as an OR operation while filters with different keys will be treated as an AND operation when.
- productType=Cisco ASR 9000&productType=Cisco ASR 4000&productFamily=Routers
  - o A subscription with the above filters will only send notifications that have a productFamily value of Routers AND a productType of either Cisco ASR 9000 OR Cisco ASR 4000

```
Sample Connection-less subscription
samples/notifications/subscription payload producttype.json
Sample Connection-oriented subscription
https://{server}/restconf/streams/v1/inventory.json?productType=Cisco%2
0ASR%204000&productFamily=Routers
```

Device Level Filters and ElementType combinational support

Following device level filters and elementType can be used together to have more granular filters.

Device filter
- productType
- productFamily
- productSeries
- group
- ndFdn

ElementType Filters
- o equipment
- o node
- o physical-connector
- o RC_Node

Inverse Filters

Inverse filters are a way of applying the NOT operation on a specified filter. This lets you say you want notifications for everything that is NOT a specific topic. Inverse filters apply to all available filters.

```
Sample Inverse Filters – This will give you all notifications that are
NOT Cisco ASR 4000 notifications.
{
    "push.endpoint-url":"http://10.155.124.143:7081/notifications",
    "push.topic":"inventory",
    "push.format": "json",
    "push.filters": [
     {
            "push.key":"productType",
            "push.value": "!Cisco ASR 4000"
     }
    ]
}
```

Alarm Forwarding Filters

If the notification policies are enabled from EPNM and notification policies are configured with destination set as restconf in the EPNM, then each alarm generated and forwarded to NBI notification is checked against notification policies. If the user group set in the notification policies match with user group of the subscribed client to notification.

1.76 Inventory Notifications

Inventory notifications in Cisco EPN Manager restconf is supported for three types of operations:
- CREATE
  - o when a device is added to Cisco EPN Manager
  - o when a service was provisioned on one or more devices that created an object in the system.
  - o In this case, the entire object that was created is sent as part of the notification.
- MODIFY/ UPDATE/ AVC (Attribute Value Change)
  - o when a device or object that exists in the system is updated.
  - o In this case, the object identified by its FDN (fully distinguished name) along with the properties that were changed are sent as part of the notification.
- DELETE
  - o when a device or object is deleted from the system.
  - o Only the FDN (fully distinguished name) of the object that was deleted is sent as part of the notification.

HTTP Method	Resource Path
POST	/restconf/data/v1/cisco-notifications:subscription
Websocket	/restconf/streams/v1/inventory [.xml	.json]
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json

	One or more from following for /restconf/streams/v1/template-execution[.xml|.json]
Authorization Required	- Chassis View Read - Chassis View Read and Write - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting - Network Topology - Network Devices All of the following for /restconf/data/v1/cisco-notifications:subscription - Chassis View Read - Chassis View Read and Write - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting - Network Topology - Network Devices - View Alerts and Events Configure Templates One or more from following

Inventory Notification - Examples

1.76.1.1 *Create notification*

- samples/notifications/create_notification.xml

1.76.1.2 *Update Notification*

- samples/notifications/update_notification.xml

1.76.1.3 *Delete Notification*

For Delete, need to send the Subscription Id in the URL and HTTP Method as DELTE

- /restconf/data/v1/cisco-notifications:subscription/{SubscriptionId}

1.77 Service-Activation Notifications

When a call to provision a service is made, it is not possible to guarantee a timely response - this may be dependent on the load on the system currently among other factors. Due to this uncertainty, the Cisco EPN Manager server, upon receiving a request to provision a service, sends out a response to the user immediately after submitting the task for provisioning. The actual completion/ failure status of the provisioning task is sent out as a notification to the subscribed clients.

The response obtained by the client is expected to contain the following information:

- The Service ID - a unique ID that was created for that particular request. Audit trails for this task can be done using this ID.
- The name of the service that was submitted
- The type of deploy-action (Preview or Deploy)
- The type of the operation (Provision, Modify, Terminate)
- The status of the operation (SUBMITTED if successfully submitted, the status is updated based on operation status and moved SUBMITTED -> PENDING -> SUCCESS | FAILED.
- A generic notification URL (for connection-oriented notifications only) - to receive notifications on the status of any provisioning task. This URL is predefined and can be subscribed to even before submitting the provisioning task
  - **URL**: https://<epnm-server-fully-qualified-domain-name>/restconf/streams/v1/service-activation[.xml | .json]

- where appending the url with .xml will result in notifications serialized to xml and .json will result in notifications serialized to json
  - **Authentication**: Basic auth

For connectionless notifications, the workflow of subscribing and receiving notifications is the same as that of inventory notifications, except the "topic" has to be "service-activation". The same endpoint that receives inventory notifications may be used to receive service-activation notifications.

A sample client for subscribing and listening to connection-oriented notifications is provided in the next section. Connectionless notifications can be received by any REST service accepting an XML or JSON payload via a POST request.

HTTP Method	Resource Path
POST	/restconf/data/v1/cisco-notifications:subscription
Websocket	/restconf/streams/v1/service-activation[.xml | .json]
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	One or more from following for /restconf/streams/v1/template-execution[.xml|.json] • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting All of the following for /restconf/data/v1/cisco-notifications:subscription • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices • View Alerts and Events • Configure Templates

1.78 Alarm Notifications

Alarm notifications are sent out for the following events:
1. When an alarm is created.
2. When an alarm is assigned to a user.
3. When an alarm is acknowledged.
4. When a user adds notes to the alarm

For connectionless notifications, the workflow of subscribing and receiving notifications is the same as that of inventory notifications, except the "topic" has to be "alarm". The same endpoint that receives inventory notifications may be used to receive service-activation notifications.

A sample client for subscribing and listening to connection-oriented notifications is provided in the next section. Connectionless notifications can be received by any REST service accepting an XML or JSON payload via a POST request.

Alarms may be filtered by device properties as specified in section 8.5.3. You may specify filters in an alarm subscription the same way you would with an inventory subscription.

Sample Alarm Connection-less subscription with filters
samples/notifications/subscription_alarm_filters.json
Sample Alarm Connection-Oriented Subscription
`https://{server}/restconf/streams/v1/alarm.json?productType=Cisco%20ASR`
`%204000&productFamily=Routers`

Alarm Specific Filters

Alarms also have 2 filters exclusively available to them:
- category
- severity
- probable-cause
- cause-type
  - symptom
  - root-cause
  - cause-unknown

This filters are applied the same as device level filters.

1.78.1.1 *Severity Filter Notes*

- When specifying a filter like critical, you will also received the corresponding clear alarm when that critical alarm is cleared.
- **Sample Alarm Connection-less subscription with Filters**
  - samples/notifications/subscription_alarm_filters.json

HTTP Method	Resource Path
POST	/restconf/data/v1/cisco-notifications:subscription
Websocket	/restconf/streams/v1/alarm [.xml | .json]
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	One or more from following for /restconf/streams/v1/template-execution[.xml|.json] - View Alerts and Events All of the following for /restconf/data/v1/cisco-notifications:subscription - Chassis View Read - Chassis View Read and Write - Circuit or VC Provisioning - Circuit or VC Monitoring and Troubleshooting - Network Topology - Network Devices - View Alerts and Events - Configure Templates

1.79 Template Execution Notifications

Notifications are also sent out to subscribed clients when a job that was executed through the Restconf NBI completes execution. Due to the asynchronous nature of these jobs, an immediate response is not guaranteed and users are encouraged to subscribe to template-execution notifications.

For connectionless notifications, the workflow of subscribing and receiving notifications is the same as that of inventory notifications, except the "topic" has to be "template-execution". The same endpoint that receives inventory notifications may be used to receive service-activation notifications.

HTTP Method	Resource Path
POST	/restconf/data/v1/cisco-notifications:subscription
Websocket	/restconf/streams/v1/template-execution[.xml | .json]
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	One or more from following for /restconf/streams/v1/template-execution[.xml|.json]

	• Configure Templates All of the following for /restconf/data/v1/cisco-notifications:subscription • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices • View Alerts and Events • Configure Templates

1.80 All Notifications

It is possible to subscribe to receive all notifications. Please note that this will generate a lot of notifications.

HTTP Method	Resource Path
POST	/restconf/data/v1/cisco-notifications:subscription
Websocket	/restconf/streams/v1/all[.xml	.json]
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	All of the following • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Network Devices • View Alerts and Events • Configure Templates

1.81 High-Availability Notifications

HA notifications are sent for:
- Failover: when the secondary becomes active
- Failback: when the primary becomes active again.

Sample HA Notifications

1.81.1.1 *Failover*

- samples/notifications/ha.failover.xml

1.81.1.2 *Failback*

- samples/notifications/ha.failback.xml

HTTP Method	Resource Path
POST	/restconf/data/v1/cisco-notifications:subscription
Request Message	
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json
Authorization Required	All of the following • Chassis View Read

	• Chassis View Read and Write
	• Circuit or VC Provisioning
	• Circuit or VC Monitoring and Troubleshooting
	• Network Topology
	• Network Devices
	• View Alerts and Events
	• Configure Templates

1.82 Notifications Client

The notifications client that is supported by Cisco EPN Manager restconf should ideally be supporting web-sockets. The recommendation is to use a client that works with "Atmosphere framework".

Sample client code

- samples/notifications/notification_client_code.txt

1.83 Notifications Schema

- samples/notifications/notification_schema.yang

Software Image Management (SWIM)

1.84 Job Details

Operations

The following sub-sections provide the details of the operations that can be used for retrieving the job details for swim jobs.

Service

Operation	Description
Job Details by Id	This operation is used to retrieve the job details.
HTTP Method	**Resource Path**
GET	/webacs/api/v1/op/swim/image/jobDetailsById/{jobId}
Request Message	
Request Content Type	
Request Data	Request data of type **Long** that contains the job Id.
Response Message	
Response Content Type	application/json
Response Data	Return a data of type **SwimDashboardJobDetailsDTO** that contains the details of job for given job Id.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.

1.84.1.1   *Service Request*

Name	Type	Description
jobId	Long	The Job Id

1.84.1.2   *Service Response*

Name	Type	Description
SwimDashboardJobDetailsDTO	Container element	Holds the data for swim job details

1.85 Collection Service

Operations

The following sub-sections provide the details of the operations that can be used for importing images to EPNM.

Service

Operation	Description
Image collection Service	This operation can be used to import image to EPNM.
HTTP Method	**Resource Path**
POST	/webacs/api/v1/op/swim/image/collect
Request Message	
Request Content Type	application/json
Request Data	Request data of type **CollectionJobDTO** that contains the details of the job scheduler, job specification, job type, job name, username and description.

Response Message	
Response Content Type	application/json
Response Data	Return a provisioning response of **SwimJobResultDTO** that contains job Id and job status.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.

1.85.1.1 *Service Request*

Name	Type	Description
CollectionJobDTO	Container element	Holds data for the details of the job scheduler, job specification, job type, job name, username and description.

1.85.1.2 *Service Response*

Name	Type	Description
SwimJobResultDTO	Container element	Holds the data for job schedule result.

1.86 Commit Service

Operations

The following sub-sections provide the details of the operations that can be used to commit change in the device.

Service

Operation	Description
Commit Service	This operation can be used to commit the changes on IOS-XR device
HTTP Method	**Resource Path**
POST	/webacs/api/v1/op/swim/image/commit
Request Message	
Request Content Type	application/json
Request Data	Request data of type **SwimCommitJobDTO** that contains the details of the job scheduler, job specification, job type, job name, username and description.
Response Message	
Response Content Type	application/json
Response Data	Return a provisioning response of **SwimJobResultDTO** that contains job Id and job status.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.

1.86.1.1 *Service Request*

Name	Type	Description
SwimCommitJobDTO	Container element	Holds data for the details of the job scheduler, job specification, job type, job name, username and description.

1.86.1.2 *Service Response*

Name	Type	Description
SwimJobResultDTO	Container element	Holds the data for job schedule result.

1.87 Distribution Service

Operations

The following sub-sections provide the details of the operations that can be used to copy image to cisco device.

Service

Operation	Description
Distribution Service	This operation can be used to copy image to cisco devices.
HTTP Method	**Resource Path**
POST	/webacs/api/v1/op/swim/image/distribute
Request Message	
Request Content Type	application/json
Request Data	Request data of type **SoftwareImageDistributionDTO** contains the details of the job scheduler, job specification, job type, job name, username and description.
Response Message	
Response Content Type	application/json
Response Data	Return a provisioning response of **SwimJobResultDTO** that contains job Id and job status.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.

1.87.1.1 *Service Request*

Name	Type	Description
SoftwareImageDistributionDTO	Container element	Holds data for the details of the job scheduler, job specification, job type, job name, username and description.

1.87.1.2 *Service Response*

Name	Type	Description
SwimJobResultDTO	Container element	Holds the data for job schedule result.

1.88 Activation Service

Operations

The following sub-sections provide the details of the operations that can be used to install or activate image.

Service

Operation	Description
Operation	Description
Activation Service	This operation can be used to add/install/remove image.
HTTP Method	**Resource Path**

POST	/webacs/api/v1/op/swim/image/activate
Request Message	
Request Content Type	application/json
Request Data	Request data of type **SoftwareImageDistributionDTO** contains the details of the job scheduler, job specification, job type, job name, username and description.
Response Message	
Response Content Type	application/json
Response Data	Return a provisioning response of **SwimJobResultDTO** that contains job Id and job status.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.

1.88.1.1   *Service Request*

Name	Type	Description
SoftwareImageDistributionDTO	Container element	Holds data for the details of the job scheduler, job specification, job type, job name, username and description.

1.88.1.2   *Service Response*

Name	Type	Description
SwimJobResultDTO	Container element	Holds the data for job schedule result.

1.89 Port Details Retrieval

This interface provides the operations required to retrieve port details.

Resource	Description
Device details	Retrieves port's details available on the given device (NdFdn pass as query param).
HTTP Method	**Resource Path**
GET	/restconf/data/v1/cisco-resource-ems:odu-slice
Query Parameters	

Name	Type	Description
ndFdn	String	Fully Distinguished Name (FDN) of the Node. FDN = 'MD=<CISCO_EPNM>!ND=<nodename>
serviceType	String	Possible Values: SONET_OPU2_BMP, SDH_OPU2_BMP, ETHERNET_OPU2E_BMP, OTN_OPU2E, ETHERNET_OPU4_GMP, OTN_OPU4
protection	String	Possible Values: NONE, ONE_PLUS_ONE

Get All Port details for Device Request/Response

Request

GET /restconf/data/v1/cisco-resource-ems:odu-slice?protection=NONE&serviceType=OTN_OPU2E
&ndFdn=MD=CISCO_EPNM!ND=<Device Name>

Response

- samples/Get_PortDetails/response.xml

1.90 Odu Card Protection Group

NCS1K4 platforms shall support the ability to configure odu protection group. For Bo cards that already exist with CFP2D pluggables, users will have the ability to set the odu protection group on trunk level. A user can also update or delete the protection group.

Odu Card Protection Group(Create)

Allows a user to create new odu protection group for Muxponder card mode. All the input params are mandatory.

Resource	Description	
Card protection group	Card protection group create	
HTTP Method	**CREATE**	
POST	/restconf/operations/v1/cisco-nrf-protection:odu-card-protection	
Input Parameters		
Name	**Type**	**Description**
odu-card-protection-request		Odu card protection request container
resource-ref	FDN	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-23!EQ=name=0-1
odu-group-name	Integer	Indicates protection group number Allowed range: 0 to 65535
connection-mode	String	Mode of connection Allowed value: SNC_N, NONE
hold-off-timer	Integer	Wait time between link fault detection & link switch to protected path Allowed range: 0 to 10000 (In multiples of 100)
reversion-time	Integer	Wait time before link traffic returns to primary path Allowed range: 300 to 720
protection-mode	String	Allowed values: REVERTIVE,NONREVERTIVE
protection-type	String	Allowed values: APSbidi
protect-tp-ref	FDN	Termination point reference for protecting controller e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-23!CTP=name=ODUC40/1/0/13;lr=lr-och-data-unit-c4
working-tp-ref	FDN	Termination point reference for working controller
Response Message		
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json	
Response Data	The `odu-card-protection-response`– see yang model for the data details. And result of modification on the feature.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response	

	data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.
	If error is from underlying framework/core modules error-app-tag format one of following
	• FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
	• CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
	For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-nrf-protection.yang

Request

- /samples/Create_Odu_Protection_Group/request.xml

Response

- samples/Create_Odu_Protection_Group/response.xml

Odu Card Protection Group(Update)

Allows a user to modify the hold-off-timer and reversion-time for existing protection group. All the input params are mandatory.

Resource	Description	
Card protection group	Card protection group update	
HTTP Method	**UPDATE**	
PUT	/restconf/operations/v1/cisco-nrf-protection:odu-card-protection	
Input Parameters		
Name	**Type**	**Description**
odu-card-protection-request		Odu card protection request container
resource-ref	FDN	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-23!EQ=name=0-1
protection-group-id	Integer	Unique identifier for protection group
hold-off-timer	Integer	Wait time between link fault detection & link switch to protected path. Allowed range: 0 to 10000 (In multiples of 100)
reversion-time	Integer	Wait time before link traffic returns to primary path Allowed range: 300 to 720
Response Message		
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json	
Response Data	The odu-card-protection-response– see yang model for the data details. And result of modification on the feature.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed.	

	Please refer to RESTCONF standard status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element.
	If error is from underlying framework/core modules error-app-tag format one of following
	• FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found.
	• CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials
	For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-nrf-protection.yang

Request

- /samples/Update_Odu_Protection_Settings/request.xml

Response

- /samples/Update_Odu_Protection_Settings/response.xml

Odu Card Protection Group(Delete)

Allows a user to delete the hold-off-timer and reversion-time for existing protection group. All the input params are mandatory.

Resource	Description	
Card protection group	Card protection group delete	
HTTP Method	**DELETE**	
DELETE	/restconf/operations/v1/cisco-nrf-protection:odu-card-protection	
Input Parameters		
Name	**Type**	**Description**
odu-card-protection-request		Odu card protection modification request container
resource-ref	FDN	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-23!EQ=name=0-1
protection-group-id	Integer	Unique identifier for protection group
Response Message		
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json	
Response Data	The odu-card-protection-response– see yang model for the data details.	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.	

Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to [EPNM 7.1.1 NB API Error Codes Reference.xlsx](#)
Yang file name	cisco-nrf-protection.yang

Request

- [/samples/Delete_Odu_Protection_Group/request.xml](#)

Response

- [/samples/Delete_Odu_Protection_Group/response.xml](#)

Odu Card Protection Group (Retrieval)

Allows a user to Retrieve protection group by resource FDN.

Resource	Description
Card Configuration	Card Configuration Delete
HTTP Method	**GET**
GET	/restconf/operations/v1/cisco-nrf-protection:odu-card-protection?{fdn}
Query Parameters	
Name	**Description**
fdn (String)	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-23!EQ=name=0-1
Response Message	
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json
Response Data	The `odu-card-protection-response`– see yang model for the data details. And result of modification on the feature.
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.
Yang file name	cisco-nrf-protection.yang

Response

- [/samples/Get_Odu_Protection_Group/response.xml](#)

ODU Group Protection Switch Action(Post)

Allows a user to perform switch action on created ODU-Group Protection Action. All the input params are mandatory.

Resource	Description
ODU Group Protection Switch Action	To perform odu group protection switch action on the mentioned odu group
HTTP Method	**Post**
POST	/restconf/operations/v1/cisco-protection-action:protection-action
Input Parameters	

Name	Type	Description
protection-switch-action-request		Protection Switch Action request container
resource-ref	FDN	Node ref of the node being used. e.g. MD=CISCO_EPNM!ND=EPNNCS1004-124-22!EQ=name=0-0
protection-group-id	Integer	Indicates protection group instance id
action-type	String	Type of Action Allowed values : manual,force,lockout,clear,resync

Response Message	
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json
Response Data	The protection-switch-action-response– see yang model for the data details. And result of modification on the feature.
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF standard status codes and standard error response data for more details.
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	`cisco-protection-action`.yang

Request

- /samples/ODUG_Manual_Switch/request.xml

Response

- samples/ODUG_Manual_Switch/response.xml

1.91 Get ANS

To retrieve information about node setup – automatic node setup amplifier & non-amplifier attributes.

Resource	Description	
cisco-resource-ems	Retrieve ANS attributes	
HTTP Method	GET	
Resource Path	/restconf/data/v1/cisco-resource-ems:automatic-node-setup?tpFdn={fdn}	
Query Parameters		
Name	**Type**	**Description**
tpFdn	FDN	Termination point FDN e.g. MD=CISCO_EPNM!ND=NCS2K-N-21!PTP=name=LINE-1-2-3-RX;lr=lr-optical-physical
ndFdn	FDN	Node FDN e.g.MD=CISCO_EPNM!ND=NCS2K-19
ans-type	String	e.g. channel-power
Request Message		
Request Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json	
Authorization Required	One or more from following. - Chassis View Read and Write - MBC UI Framework Access - Network Devices	
Response Message		
Response Content Type	application/xml, application/yang.operation +xml, application/json, application/yang.operation+json	
Response Data	Returns automatic-node-setup-response	
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format PRE.<number> are generated by this API. For example: PRE.0019 for 'Error, found null payload.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0081=Service name %s is not found. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials	
Yang file name	cisco-termination-point.yang	

Automatic-node-setup-response format:

Name	Type	Description
automatic-node-setup-response	Container	Automatic Node Setup Response Container
node-ref	String	FDN of the Node
tp-data-list	Container	Contains list of tp-data
tp-data	Container	termination point data
tp-ref	FDN	tp-ref from the list
ans-node-data-list	Container	Contains list of ans-node-data
ans-node-data	<ans-param,ans-param-value>	Pair of ANS param name & ANS param value

Get ANS for termination-point

Response

- /samples/Get_ANS_Amplifier_Attributes/response.xml

1.92 Set ANS

To configure automatic-node-setup attributes for a termination point

Set ANS Amplifier Attributes

To set ANS amplifier attributes.

Resource	Description	
cisco-resource-ems	This resource is used to set or unset ANS attributes for port.	
HTTP Method	**Resource Path**	
PUT	/restconf/operations/v1/cisco-resource-ems:configure-termination-point	
Authorization	One or more from following - Chassis View Read and Write - MBC UI Framework Access - Network Devices	
Input Parameters		
Name	**Type**	**Description**
configure-termination-point-request	Container	Configure termination point request container
node-ref	FDN	node reference that the TP configuration can be applied
tp-parameter-list	Container	Contains list of tp-parameter
tp-parameter	Container	
tp-ref	FDN	Termination point reference for subsequent modify
layer-rate	String	technology layer rate of the termination point. E.g. lr-optical-transmission-section
ans-attributes	Container	Contains ANS configurations
amplifier	Container	Contains attributes applicable to amplifier functions
channel-power	Decimal (upto 4 decimal places)	in dBm unit
working-mode		Amplifier Working Mode
tilt	Decimal (upto 4 decimal places)	in dB unit

tilt-calibration	Decimal (upto 4 decimal places)	in dB unit
gain-range	String	amplifier gain range
gain	Decimal (upto 4 decimal places)	East Side Rx Amplifier Gain
is-logo-enabled	True/false	is logo parameters enabled
Response Message		
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json	
Response Data	Returns configure-termination-point-response	
HTTP Status Code	200 OK - Success with response message-body 401, 403 – Authentication and Authorization errors. 400 Bad Request - Invalid request message. 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TP.\<number\> are generated by this API. For example: TP.0050 for 'Invalid value for generic-admin-state, valid values are %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.\<number\> - any tag starting with "FW." prefix for any internal errors like FW.0039=TerminationPoint with FDN - %s and Layer Rate - %s does not exist or is not associated with a Node in the current user'€™s virtual domain. • CORE.\<number\> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials • RA.\<number\> - any tag starting with "RA." prefix for any internal errors like RA.0001=Operation is not supported. For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx	
Yang file name	cisco-termination-point.yang	

Request

- PUT /restconf/operations/v1/cisco-resource-ems:configure-termination-point
- /samples/Set_ANS_Amplifier_Attributes/request.xml

Response

- /samples/Set_ANS_Amplifier_Attributes/response.xml

Set ANS Non-Amplifier Attributes

To set ANS non-amplifier attributes for a termination point.

Resource	Description
cisco-resource-ems	This resource is used to set or unset ANS attributes for port.
HTTP Method	**Resource Path**
PUT	/restconf/operations/v1/cisco-resource-ems:configure-termination-point
Authorization	One or more from following

	• Chassis View Read and Write	
	• MBC UI Framework Access	
	• Network Devices	

Input Parameters		
Name	**Type**	**Description**
configure-termination-point-request	Container	Configure termination point request container
node-ref	FDN	node reference that the TP configuration can be applied
tp-parameter-list	Container	Contains list of tp-parameter
tp-parameter	Container	
tp-ref	FDN	Termination point reference for subsequent modify
layer-rate	String	technology layer rate of the termination point. ex. lr-optical-transmission-section
ans-attributes	Container	Contains ANS configurations
osc-los-threshold	Decimal (upto 4 decimal places)	in dBm unit
channel-los-threshold	Decimal (upto 4 decimal places)	in dBm unit
min-expected-span-loss	Decimal (upto 4 decimal places)	in dB unit. Min Expected Span Loss
max-expected-span-loss	Decimal (upto 4 decimal places)	in dB unit. Max Expected Span Loss
add-drop-output-power	Decimal (upto 4 decimal places)	in dBm unit. Add and Drop port output power
drop-power-channel	Decimal (upto 4 decimal places)	in dBm unit. East side Rx amplifier channel Power
Response Message		
Response Content Type	application/xml, application/yang.data+xml, application/json, application/yang.data+json	
Response Data	Returns configure-termination-point-response	
HTTP Status Code	• 200 OK - Success with response message-body • 401, 403 – Authentication and Authorization errors. • 400 Bad Request - Invalid request message. • 500 Internal Server Error - operation-failed. Please refer to RESTCONF RFC 8040 for status codes and standard error response data for more details.	
Application Error Codes (error-app-tag)	Response with error condition provides error tag in error-app-tag element. Error tag with format TP.<number> are generated by this API. For example: TP.0050 for 'Invalid value for generic-admin-state, valid values are %s.' If error is from underlying framework/core modules error-app-tag format one of following • FW.<number> - any tag starting with "FW." prefix for any internal errors like FW.0039=TerminationPoint with FDN - %s and Layer Rate - %s	

	does not exist or is not associated with a Node in the current user'€™s virtual domain. • CORE.<number> - any tag starting with "Core." prefix for any internal errors like CORE.0009=Bad credentials • RA.<number> - any tag starting with "RA." prefix for any internal errors like RA.0001=Operation is not supported. For complete list of error-app-tag and error message refer to EPNM 7.1.1 NB API Error Codes Reference.xlsx
Yang file name	cisco-termination-point.yang

Request

- PUT /restconf/operations/v1/cisco-resource-ems:configure-termination-point
- /samples/Set_ANS_Non_Amplifier_Attributes/request.xml

Response

- /samples/Set_ANS_Non_Amplifier_Attributes/response.xml

References

RESTCONF Specification
YANG Specification