Cisco Evolved Programmable Network Manager 3.0 RESTCONF API Guide

First Draft Published: Feb 21, 2019
EDCS-1570360

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

Abstract

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

Cisco Evolved Programmable Network Manager 3.0 RESTCONF API Guide

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. This includes:

- Managed Elements and Equipment Inventory
- Termination Point and Topological Link Inventory
- Virtual Connection (RFS) Resource Inventory
- Service (CFS) Inventory
- Service Provisioning
- Inventory Object Create, Delete and Attribute Value Change (AVC) Notifications

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

1.6.1 Default Batch Size

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

1.6.2 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.

1.7.1 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-megabit-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_EthPwLink #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=MyAccessEplEnni
Customer Facing Service	MD=CISCO_EPNM!CFS=<cfs.name>	MD=CISCO_EPNM!CFS=MyEPLService1
Customer	MD=CISCO_EPNM!CUSTOMER=<customer.name>	MD=CISCO_EPNM!CUSTOMER=MyGoldCustomer
QOS Policy	MD=CISCO_EPNM!POLICY_QOS=<name>	MD=CISCO_EPNM!POLICY_QOS=MyDeviceQoS
QOS Profile	MD=CISCO_EPNM!PROFILE_QOS=<name>	MD=CISCO_EPNM!PROFILE_QOS=MyUserDefineQoS
Service Profile	MD=CISCO_EPNM!PROFILE_SERVICE=<name>	MD=CISCO_EPNM!PROFILE_SERVICE=GoldEplServiceProfile1
Path	MD=CISCO_EPNM!PATH=<name>	MD=CISCO_EPNM!PATH=123_exp_path
Controller Port	MD=CISCO_EPNM!ND=<node.name>!CTRLP=<name>	MD=CISCO_EPNM!ND=NCS4206-146.4!CTRLP=MediaType 0/4/0

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.

1.10.1 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.

1.11.1 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.

1.11.2 Configuration

Rate and size limiting is configured with properties defined in the table below. These properties can only be changed by a systems administrator and require a platform restart to take effect.

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	10	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	45	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.	5	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 for total requests.	20	This is the number of total request 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

1.12.1 Overview

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

1.12.2 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 a platform 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 resource path.

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

Layer	layer=<value>
Retrieve Virtual Connection Resource	
Get All Virtual Connections	/data/v1/cisco-service-network:virtual-connection
Get All Virtual Connections for a specific type	/data/v1/cisco-service-network:virtual-connection?type=<value>
Get a Virtual Connection given its FDN (Fully Distinguished Name)	/data/v1/cisco-service-network:virtual-connection?fdn=<value>
Get All Virtual Connection referencing a given Termination point	/data/v1/cisco-service-network:virtual-connection?tpFdn=<value>
Multi Layer Trace	
Get Multi Layer Trace for a given vcFDN	/data/v1/cisco-resource-network:virtual-connection-multi-layer-route?vcFdn=<value>
MPLSTE Explicit Path	
Get All MPLS TE Explicit Paths	/data/v1/cisco-resource-ems:mpls-te-explicit-path
Get an MPLS TE Explicit Path	/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	/data/v1/cisco-service-network:customer-facing-service?type=<value>
Get All Customer Facing Services of a given type and sub-type	/data/v1/cisco-service-network:customer-facing-service?type=<type value>&subtype=<sub-type value>
Get Customer Facing Services given its FDN	/data/v1/cisco-service-network:customer-facing-service?fdn=<value>
QoS Policy Retrieval	
Get All QoS Policies in a batch	/data/v1/cisco-qos:qos-policy
Get QoS Policy for a given FDN	/data/v1/cisco-qos:qos-policy?fdn=<value>
Get All QoS Policies for a given device	/data/v1/cisco-qos:qos-policy?ndFdn=<value>
QoS Profile Retrieval	
Get All QoS Profiles in a batch	/data/v1/cisco-qos:qos-profile
Get QoS Profile for an given FDN	/data/v1/cisco-qos:qos-profile?fdn=<value>
CLI Template Retrieval	
Get All CLI Template in a batch	/data/v1/cisco-resource-activation:cli-template
Get CLI Template for a given template name	/data/v1/cisco-resource-activation:cli-template?name=<cli-template-name>
Set Termination Point	
Set attributes on a Termination Point	/operations/v1/cisco-resource-activation:set-termination-point
Service Activation	
Provision a Service	/operations/v1/cisco-service-activation:provision-service
Modify a Service	/operations/v1/cisco-service-activation:modify-service
Terminate a Service	/operations/v1/cisco-service-activation:terminate-service
Roll a Service	/operations/v1/cisco-service-activation:roll-service
Customer CRUD	/data/v1/cisco-customer:customer
Standalone OAM Performance Test	
Execute Performance Test	/operations/v1/cisco-service-oam:service-oam-config
Get Performance Test Result	/operations/v1/cisco-service-oam:service-oam-config/{request-id}
Resource Activation	
Run CLI Configuration Template – TBC (Template Based Configuration)	/operations/v1/cisco-resource-activation:run-cli-configuration
CLI Configuration Template Run Status	/operations/v1/cisco-resource-activation:get-cli-configuration-run-status/{job-name}
MPLS TE explicit path - Create	/operations/v1/cisco-resource-activation:create-explicit-path

MPLS TE explicit path - Modify	/operations/v1/cisco-resource-activation:modify-explicit-path
MPLS TE explicit path - Terminate	/operations/v1/cisco-resource-activation:terminate-explicit-path
Performance Metrics	
Optical Power And Span Loss for Links	/data/v1/cisco-resource-network:perf-metrics
Alarm Retrieval	
Get All Alarms in a batch	/data/v1/cisco-rtm:alarm
Get All Alarms by given Node reference	/data/v1/cisco-rtm:alarm?nd-ref=<value>
Get All Alarms by given Termination point reference	/data/v1/cisco-rtm:alarm?tp-ref=<value>
Get All Alarms by given Equipment reference	/data/v1/cisco-rtm:alarm?eq-ref=<value>
Get All Alarms by given precieved severity	/data/v1/cisco-rtm:alarm?precieved-severity=<value>
Get All Alarms by given System Update Time	/data/v1/cisco-rtm:alarm?system-update-time=<value>
Get All Alarms by given IteratorId	/data/v1/cisco-rtm:alarm?.iteratorId=<value>
Alarm Handling	
Alarm Ack/UnAck/Clear/Delete	/data/v1/cisco-alarm:handle-alarm
Alarm to Service association	
Get All Alarms by Service name	data/v1/cisco-rtm:impacting-alarms-by-service?cfs-ref=<value>
Patch cord	
Create Patchcord	/operations/v1/cisco-resource-activation:create-patch-cord
Delete Patchcord	/operations/v1/cisco-resource-activation:delete-patch-cord
SRRG	
Get All SRRGs present in EPNM	/data/v1/cisco-resource-network:shared-risk-resource-group
Get SRRG by FDN	/data/v1/cisco-resource-network:shared-risk-resource-group?fdn=<value>
GetAll SRRG Pool	data/v1/cisco-resource-network:srrg-pool
Get SRRG Pool by fdn	data/v1/cisco-resource-network:srrg-pool?fdn=<value>
Get SRRG Pool by pool type reference	data/v1/cisco-resource-network:srrg-pool?pool-type-ref=<value>
Get All SRRG Pool Type	data/v1/cisco-resource-network:srrg-pool-type
Get SRRG Pool type by fdn	data/v1/cisco-resource-network:srrg-pool-type?fdn=<value>
Performance Metrics for Topological Link	
Get Performance metrics for a given Topological Link	/data/v1/cisco-resource-network:perf-metrics?tlFdn=<value>
MediaType Controller	
Get/Update MediaType Controller	/data/v1/cisco-nrf-controller:controller-port
LMP Link	
Create LMP Link	/operations/v1/cisco-resource-activation:lmp-link-resource
Delete LMP Link	/operations/v1/cisco-resource-activation:lmp-link-resource?fdn=<lmpFdn>
Retrieve LMP Link	/ data/v1/cisco-resource-network:topological-link?fdn=< lmpFdn>
AINS – Automatic In-Service	
Create LMP Link	/operations/v1/cisco-nrf-physical:reserve-equipment
Device Synchronization	
Device Synchronization	/operations/v1/cisco-nrf-physical:synchronize-node

Supported layer rates for optical interfaces

Below are the list of legacy and currently supported layer rates for optical interfaces.
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>

Legacy layer rates	**Currently supported layer rate**
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

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.

1.14.1 Yang Module Data

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

1.14.2 Request/Response

Request

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

Response

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.

1.15.1 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.

1.16.1 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	/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.	
Yang file name	cisco-physical-node.yang	

1.17.1 Group Data

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

1.17.2 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

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	/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 • Device WorkCenter	
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.	
Yang file name	cisco-physical-node.yang	

1.18.1 Node Data

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

1.18.2 Get All Nodes Request/Response

1.18.2.1 *Request*

GET /restconf/data/v1/cisco-resource-physical:node?.startIndex=4&.maxCount=2 HTTP/1.1
Host: <epnm-host>
Accept: application/yang-data+xml
Authorization: Basic …

1.18.2.2 *Response*

HTTP/1.1 200 OK
Server: <epnm-host>
Content-Type: application/yang-data+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	/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 • Device WorkCenter	
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.
Yang file name	cisco-physical-equipment.yang

1.19.1 Equipment Data

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

1.19.2 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

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	/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 • Device WorkCenter	

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.
Yang file name	cisco-physical-equipment.yang

1.20.1 Chassis Data

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

1.20.2 Get All Chassis 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
```

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	/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	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 Device WorkCenter
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.
Yang file name	cisco-physical-equipment.yang

1.21.1 Module Data

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

1.21.2 Get All Modules Request/Response

Request

GET /restconf/data/v1/cisco-resource-physical:module?.startIndex=4&.maxCount=2 HTTP/1.1

Response

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	/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 • Device WorkCenter
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.
Yang file name	cisco-physical-equipment.yang

1.22.1 PhysicalConnector Data

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

1.22.2 Get All Physical Connectors Request/Response

Request

GET /restconf/data/v1/cisco-resource-physical:physicalconnector?.startIndex=900&.maxCount=5 HTTP/1.1

Response

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	/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 • Device WorkCenter
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.
Yang file name	cisco-resource-optical.yang

1.23.1 Optical Network Element Settings Data

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

1.23.2 Get All Optical Network Element Settings Request/Response

Request

GET /restconf/data/v1/restconf/data/v1/cisco-resource-optical:optical-nesettings?.depth=1&.maxCount=7 HTTP/1.1

Response

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	/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/fal	Enables you to return Contained In Use Connection

	se)	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 • Device WorkCenter	
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.	
Yang file name	cisco-termination-point.yang	

1.24.1 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.

1.24.2 Get All Physical Termination Points Request/Response

Request

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

Response

1.24.3 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

1.24.4 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

1.24.5 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

1.24.6 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

1.24.7 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

1.24.8 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

1.24.9 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

1.24.10 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

1.24.11 Get FiberType and FiberLength for All Termination Points Request/Response

Request

- `https://<server-ip>/restconf/data/v1/cisco-resource-ems:termination-point?ndFdn=MD=CISCO_EPNM!ND=tcc40&.startIndex600&.batchSize=100`

Response

- samples/Get_FiberType_and_FiberLength_for_All_Termination_Points/response.xml

1.24.12 Get FiberType and FiberLength for Single Termination Point Request/Response

Request

GET /restconf/data/v1/cisco-resource-ems:termination-point?fdn=MD=CISCO_EPNM!ND=<device-name>!CTP=name=<CTP-name>;lr=<layer-rate

Response

- samples/Get_FiberType_and_FiberLength_for_Single_Termination_Point/response.xml

1.24.13 Get Termination Points for Patch Cord A END Request/Response

Request

- GET /restconf/data/v1/cisco-resource-ems:termination-point?fdn=MD=CISCO_EPNM!ND=<device-name>!CTP=name=<CTP-name>;lr=<layer-rate> / 1.1
- Host: <epnm-host>
- Accept: application/yang-data+xml

Response

- samples/Get_Termination_Points_for_Patch_Cord_A_END/response.xml

1.24.14 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

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	/operations/v1/cisco-resource-activation:set-termination-point
Authorization Required	One or more from following • Chassis View Read and Write • MBC UI Framework Access • Device WorkCenter
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.
Yang file name	cisco-termination-point.yang

1.25.1 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	Indicates the portMode for the TP.

		OTN	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 INTERNAL RECOVERED FREE_RUNNING ENHANCED	Specifies the clock source 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	
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	-	
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 TCM_CONTROL_PORT_CONFIG			
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 2.0 to 100.0.	
alsRecoveryPulseWidth	Float	Value Ranging from 60 to 100.	
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.	
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	

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

1.25.2 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

1.25.3 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

1.25.4 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

1.25.5 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

1.25.6 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

1.25.7 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

Response

- samples/Set_Termination_Point_ODU_PORT_CONFIG/response.xml

1.25.8 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

1.25.9 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

Response

- samples/Set_Termination_Point_OTN_PORT_CONFIG/response.xml

1.25.10 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

1.25.11 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

1.25.12 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

1.25.13 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

1.25.14 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

1.25.15 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

1.25.16 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

1.26 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	/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.
.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 filter skips a call to the device to get fiber attributes data thus improving 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.	
Yang file name	Cisco-topology.yang	

1.26.1 Topological Link Data

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

1.26.1.1 *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.
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.

1.26.2 Get All Topology

Request

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

Response

- samples/Get_All_Topology/response.xml

1.26.3 Get a Topology

Request

- GET /restconf/data/v1/cisco-resource-network:topological-link?fdn=MD=CISCO_EPNM!TL=LINK PW

Response

- samples/Get_a_Topology/response.xml

1.26.4 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

1.27 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	/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>
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 • Device WorkCenter	
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.	
Yang file name	cisco-mpls-te-extension.yang	

1.27.1 MPLS TE Explicit Path Data

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

1.27.2 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

1.27.3 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

1.28 Virtual Connection Retrieval

This interface provides the operations required to retrieve virtual connection details which include the CEM and MPLS-TE RFS details.

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	/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, and mpls-l3-vpn.
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.
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.
Yang file name	cisco-virtualconnection.yang

1.28.1 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	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-resynch, 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		
protection-type	String		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			Virtual Connection termination point list.
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	Uni-direction/bi-direction	Base identity for VC for direction.
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		
untagged-default	String		
sv-id-list	String		
cv-id-list	String		
vid-rewrite-oper	String		
rewrite-is-symmetric	String		
mtu	String		
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		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.
sr-te-policy			Segment Routing Policy with SR-TE Paths
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
sids-list			for each candidate path, there's a segement ids list 1 and 0-m (SIDs list)
sids			Segment IDs
name	String		segment IDs name
type	String		dynamic, explict 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			DWDM OCH NC circuit specific attributes.
restoration-type	String		
Restoration-status	String		
Activation-state	String		
regeneration-allowed	Boolean		
upstream-power-offset	String		
downstream-power-offset	String		
path-policy	String		
ignore-path-alarms	String		
circuit-diversity	String		
revert	String		
soak-time	String		
frequency	String		
width	String		
priority	String		
optical-path-settings	String		
is-uni	Boolean		
is-wson	Boolean		
is-mandatory-freq	Boolean		
frequency-preference	String		
frequency-protected	String		

frequency-protected-preference	String		
is-mandatory-frequency-protected	Boolean		
failure-reason	String		
Och-trail			DWDM OCH Trail circuit specific attributes.
restoration-type	String		
Restoration-status	String		
activation-state	String		
regeneration-allowed	Boolean		
upstream-power-offset	String		
downstream-power-offset	String		
path-policy	String		
ignore-path-alarms	String		
circuit-diversity	String		
revert	String		
soak-time	String		
frequency	String		
width	String		
priority	String		
optical-path-settings	String		
is-uni	Boolean		
is-wson	Boolean		
is-mandatory-freq	Boolean		
frequency-preference	String		
frequency-protected	String		
frequency-protected-preference	String		
is-mandatory-frequency-protected	Boolean		
failure-reason	String		
Och-cc			DWDM OCH CC circuit specific attributes.
restoration-type	String		restoration type, none, restore, revert
restoration-status	String		restoration type, none, failed, restored, restoring, revertible, reverting
working-och-trail	String		Reference to the working OCH Trail.
protected-och-trail	String		Reference to the protecting OCH Trail.
is-wson	Boolean		WSON indicator. Circuit is routed automatically or manually.
failure-reason	String		Indicates the failure reason for DWDM OCH Client Connection if any error exists during circuit provisioning.
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		
manage-constraints	Boolean		
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 attributes.
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		Associated tunnel-id
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		
bandwidth	String		
protection-profile	String		
diverse-attribute-name	String		
failure-reason	String		
	String		
te-tunnel-path-option-list	String		
path-preference	String		
protection-role	String	Working/protected	
path-type	String		
lock-down	String		
protected-by	String		

explicit-path-name	String		

1.28.2 Get All Virtual Connection Request/Response

Request

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

Response

- samples/Get_All_Virtual_Connections/response.xml

1.28.3 Get All Virtual Connection L3VPN Request/Response

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

1.28.4 Get a Single Virtual Connection Request/Response

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

1.28.5 Get a Virtual Connection – L3VPN Request/Response

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

1.28.6 Get All Virtual Connections - CE Request/Response

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

1.28.7 Get a Virtual Connections - CE Request/Response

Request

- GET /restconf/data/v1/cisco-service-network:virtual-connection? fdn= MD=CISCO_EPNM!VC=EVPTree-NBI-03

Response

- samples/Get_a_Virtual_Connection_CE/response.xml

1.28.8 Get All Virtual Connections - CEM Request/Response

Request

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

Response

- samples/Get_All_Virtual_Connections_CEM/response.xml

1.28.9 Get a Virtual Connections - CEM Request/Response

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

1.28.10 Get ALL Virtural Connections – OPTICAL Request/Response

Request

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

Response

- samples/Get_All_Virtual_Connections_OPTICAL/response.xml

1.28.11 Get a Virtual Connections – Optical (OCH 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_Optical_OCH_Service/response.xml

1.28.12 Get All Virtual Connections – With ServiceInfo Resynch 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_Resynch_State/response.xml

1.28.13 Get a Virtual Connection for MCH Services

Request

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

Response

- samples/Get_a_Virtual_Connection_for_MCH_Services/response.xml

1.29 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.

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	/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.
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.	
Yang file name	Cisco-topology.yang	

1.29.1 Virtual Connection Multi-Layer Route 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 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.

1.29.2 Get a Virtual Connection Multi-Layer Route – OCHTRAIL_UNI

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

1.29.3 Get a Virtual Connection Multi-Layer Trace – MCHGroup

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

1.29.4 Get MLT Request for OCHTrail UNI

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

1.29.5 Get MLT Request for OPU over ODU

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

1.29.6 Get MLT Request for ODUUNI Hairpin

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

1.30 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 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	/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.
Yang file name	cisco-customer-facing-service.yang

1.31 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	/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.	
Yang file name	cisco-network-interface.yang	

1.32 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.	
Yang file name	cisco-qos.yang	

Request

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

Response

- samples/Get_All_QoS_Policy_Retrieval/response.xml

1.33 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.
Yang file name	cisco-qos.yang

1.34 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	/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.	
Yang file name	cisco-resource-activation.yang	

1.35 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.
Yang file name	cisco-ipsla-profile.yang

1.35.1 Get IPSLA Profile

Request

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

Response

- samples/Get_IPSLA_Profile/response.xml

1.36 Service Activation

1.36.1 Operations

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

1.36.1.1 *Provision Service*

Operation	**Description**
Provision a Service	This operation can be used to provision a service.
HTTP Method	**Resource Path**
POST	/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.
Yang file name	• cisco-service-activation.yang

1.36.1.1.1 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.

1.36.1.1.2 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.
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.

1.36.1.2 *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

1.36.1.2.1 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

1.36.1.2.2 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

1.36.1.2.3 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

1.36.1.2.4 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

1.36.1.2.5 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

1.36.1.2.6 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

1.36.1.2.7 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

1.36.1.2.8 Provision CEM STM1 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_STM1_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_STM1_Service_over_SDH_Controller/response.xml

1.36.1.2.9 Provision CEM STM4 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_STM4_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_STM4_Service_over_SDH_Controller/response.xml

1.36.1.2.10 Provision CEM STM16 Service over SDH Controller

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Provision_CEM_STM16_Service_over_SDH_Controller/request.xml

Response

- samples/Provision_CEM_STM16_Service_over_SDH_Controller/response.xml

1.36.1.2.11 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

1.36.1.2.12 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

1.36.1.2.13 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

1.36.1.2.14 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

1.36.1.2.15 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

1.36.1.2.16 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

1.36.1.2.17 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

1.36.1.2.18 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

Response

- samples/Provision_CEM_SDH_MSP_VC12/response.xml

1.36.1.2.19 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

1.36.1.2.20 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

1.36.1.2.21 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

1.36.1.2.22 Provision MPLS-TE Unidirectional 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

1.36.1.2.23 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

1.36.1.2.24 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

1.36.1.2.25 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>
```

1.36.1.2.26 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

1.36.1.2.27 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

1.36.1.2.28 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

1.36.1.2.29 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

1.36.1.2.30 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

1.36.1.2.31 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

1.36.1.2.32 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

1.36.1.2.33 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

1.36.1.2.34 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

1.36.1.2.35 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

1.36.1.2.36 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

1.36.1.2.37 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

1.36.1.2.38 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

1.36.1.2.39 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

1.36.1.2.40 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

1.36.1.2.41 Provision QoS Profile Service

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

1.36.1.2.42 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

1.36.1.2.43 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

1.36.1.2.44 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

1.36.1.2.45 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

1.36.1.2.46 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

1.36.1.2.47 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

1.36.1.2.48 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

1.36.1.2.49 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

1.36.1.2.50 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

1.36.1.2.51 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

1.36.1.2.52 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

1.36.1.2.53 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

1.36.1.2.54 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

1.36.1.2.55 Provision Optical Service

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

1.36.1.2.56 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

1.36.1.2.57 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

1.36.1.2.58 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

1.36.1.2.59 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

1.36.1.2.60 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

1.36.1.2.61 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

1.36.1.2.62 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

1.36.1.2.63 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

1.36.1.2.64 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

1.36.1.2.65 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

1.36.1.2.66 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

1.36.1.2.67 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

1.36.1.2.68 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

1.36.1.3 *Modify Service*

Operation	**Description**
Modify existing service	This operation can be used to modify existing service.
HTTP Method	**Resource Path**
POST	/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

1.36.1.3.1 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.

1.36.1.3.2 Modify Service Response

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

1.36.1.3.3 Modify CEM Service Example

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

1.36.1.3.4 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

1.36.1.3.5 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

1.36.1.3.6 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

1.36.1.3.7 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

1.36.1.3.8 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

1.36.1.3.9 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

1.36.1.3.10 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

1.36.1.3.11 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

1.36.1.3.12 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

1.36.1.3.13 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

1.36.1.3.14 Modify Optical Service

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

1.36.1.3.15 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

1.36.1.3.16 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

1.36.1.3.17 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

1.36.1.3.18 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

1.36.1.3.19 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

1.36.1.3.20 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

1.36.1.3.21 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

1.36.1.3.22 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

1.36.1.3.23 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

1.36.1.3.24 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

1.36.1.3.25 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

1.36.1.3.26 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

1.36.1.4 *Terminate Service*

Operation	**Description**
Terminate existing Service	This operation can be used to terminate existing service.
HTTP Method	**Resource Path**
POST	/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

1.36.1.4.1 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.

1.36.1.4.2 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,VT2,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

1.36.1.4.3 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

1.36.1.4.4 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

1.36.1.4.5 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

1.36.1.4.6 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

1.36.1.4.7 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

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

Request

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

1.36.1.4.9 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

1.36.1.4.10 Terminate Optical Service

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

1.36.1.4.11 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

1.36.1.4.12 Terminate OCHNC Service

Request

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

Response

- samples/Terminate_OCHNC_Service/response.xml

1.36.1.4.13 Terminate OCHCC Service

Request

- POST /restconf/operations/v1/cisco-service-activation:terminate-service
- samples/Terminate_OCHCC_Service/request.xmlC:\Users\vgangadh\AppData\Local\Temp\samples\Terminate_OCHNC_Service\response.xml

Response

- samples/Terminate_OCHCC_Service/response.xml

1.36.1.4.14 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

1.36.1.4.15 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

1.36.1.4.16 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

1.36.1.4.17 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

1.36.1.4.18 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

1.36.1.4.19 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

1.36.1.4.20 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

1.36.1.4.21 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

1.36.1.4.22 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

1.36.1.5 *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	/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

1.36.1.5.1 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.

1.36.1.5.2 Roll Service Response

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

1.36.1.5.3 Roll Service Request/Response

Request

- samples/Roll_Service/request.xml

Response

- samples/Roll_Service/response.json

Notification

- samples/Roll_Service/notification.json

1.36.1.6 *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	/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

1.36.1.6.1 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.

1.36.1.6.2 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
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,VT2,OC1,OC3, OC12,OC48
MPLS-TE	mpls-te-tunnel	Bidirectional, Unidirectional, TE Tunnel, Layer 3 Link
L3VPN	mpls-l3-vpn	L3VPN

Force Terminate Sample Response:

- samples/Force_Terminate_Service/response.xml

1.36.1.7 *Schedule service deployment*

NBI supports service deployment to be scheduled to a specified time for all supported services except optical . It is applicable for provide, amend and terminate operations. For scheduling a service use “deploy-schedule-time” tag along with “deploy-action” as “Scheduled” in the NBI input payload.

1.36.1.7.1 Schedule service deployment for provide operation

Request

- POST /restconf/operations/v1/cisco-service-activation:provision-service
- samples/Schedule_Deployment/Evpl-DeploySchedule-Provide-Request.xml

- samples/Schedule_Deployment /EPTree-DeploySchedule-Provide-Request.xml

Response

- samples/Schedule_Deployment/Evpl-DeploySchedule-Provide-Response.xml
- samples/Schedule_Deployment/EPTree-DeploySchedule-Provide-Response.xml

1.36.2 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.

1.36.2.1 *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).

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 except optical services	This is the tag to specify deploy action in the payload. Default value : Deploy Possible Values : Preview , Deploy , Scheduled
deploy-schedule-time	Date	No	No	All except 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

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
termination-point-list	List container	Yes	N/A	All	List of connection termination point configurations.
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=GigabitEthernet0/4;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

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.
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>

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
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
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.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
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.
operator-ref	String (FDN)	No	No	Access EPL, Access EVPL	FDN of the customer object – set of RDN types with MD, CUSTOMER.

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
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
match-exact	Boolean	No	Yes	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Mentions do exact match 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
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.
pop-operation	Container	No	N/A	EVPL, Access EVPL, EVP-LAN, EVP-Tree	Pop action configuration container element.

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
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
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
protection-type	Enum (Working, Working+Protected)	Yes	Yes	EPL, EVPL	Type of MPLS Tunnel Path Protection.
enable-autoroute	Boolean	No	Yes	EPL, EVPL	Enable Auto Route True/False, Default is True
enable-frr	Boolean	No	Yes	EVPL	Enable Fast Re-route. Applicable for uni-directional tunnel only

Carrier Ethernet Service Order Data	Data Type	Mandatory	Modifiable	Applicable to Service Type	Description
enable-auto-bandwidth	Boolean	No	Yes	EVPL	Enable Auto Bandwidth. Applicable for uni-directional tunnel only Default value : true
enable-autoroute	Boolean	No	Yes	EVPL	This attribute specifies whether to enable autoroute option
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.

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_26551659
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_26551659
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

1.36.2.2 *Service Order Data – CEM*

CEM Service Order Data	Data Type	Mandatory	Modifiable	Description
service-type	String (CEM)	Yes	No	The type of service.
service-subtype	String (t1,t3,e1,e3,vt1.5,vt2,sts1, sts3,sts48,sts192, DS0)	Yes	No	Service subtypes
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-description	String	No	Yes	A unique description about the service.

service-activate	Boolean	No	Yes	Turn service on/off.
frame-type	Enum (CEP, SATOP, CESoPSN)	No	No	CEM Framing Type.
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
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 STM1 :** AU-4 1, AU-4 2,…,AU-4 48 **For STM4 :** AU-4 1-4, AU-4 5-8,…,AU-4 45-48 **For STM16 :** 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: STS1, STS3C, STM1, STS12C, STM4, STS48C, STM16, STS192C, STM64, T3,E3, VT15, VT2, T1, E1, STS3C_VCAT, CT3, CT3_E1, VC11_T1, VC12_E1, UNFRAMED. **STM1 over SDH controllers :** VC4 **STM4 over SDH controllers :** VC4_4C **STM 16 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
ds0-time-	String	No	No	Comma separated ds0 time slot numbers.

slots				
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
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
protection-type	Enum	Yes	Yes	Type of MPLS Tunnel Path Protection. Working, Working+Protected Default value = Working
enable-autoroute	Boolean	No	Yes	Enable Auto Route true/false. Default 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

1.36.2.3 *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.

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
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.

UNI 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 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>
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.

UNI 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 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

1.36.2.4 *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.

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

ENNI Service Order Data	Data Type	Mandatory	Modifiable	Description
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.
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.

ENNI Service Order Data	Data Type	Mandatory	Modifiable	Description
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.
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.

ENNI Service Order Data	Data Type	Mandatory	Modifiable	Description
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

1.36.2.5 *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.

1.36.2.6 *Partial service support*

- One of the "<termination-point-config>" in a 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:

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

  - <device-name> is mandatory. Use a string as a third party device name.
  - <directionality> is mandatory. Allowed values are source, sink and bidirectional
  - <new-device> is boolean and is used to indicate a new or existing device.
    - If it is true, you also need to provide a <device-ip-address> which should not exist in Cisco EPN Manager.
    - 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.
  - <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.
  - <device-ldp-address> is the LDP IP address on the third party LDP configuration.
  - <vc-id> is an integer for vc.

1.36.2.7 *Service Order Data - MPLS Layer3 Link*

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-point-list	**List container**	**Yes**	**No**	**List of termination point configurations.**
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.
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 ,Level-1, Level-2-only, Level-1-2 Default value: NONE
level1-metric	String	No	Yes	Level1 metric , it will be used only when value of "circuit-type" is Level-1 or Level-1-2 Value within 1-65535 range.
level2-metric	String	No	Yes	Level2 metric , it will be used only when value of "circuit-type" is Level-2-only or Level-1-2 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.

1.36.2.8 *Service Order Data - MPLS-TE*

	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.
	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),	ID used with association ID and source address to form bidirectional tunnel uniqueness.

		No (for uni-directional-tunnel)	
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: 7)	No	Tunnel Hold Priority
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
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.
min-auto-bandwidth	String	No	This attribute specifies the minimum auto bandwidth.
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.
	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.

1.36.2.9 *Service Order Data - MPLS L3VPN*

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

	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 referece 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-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 Excernal 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.

1.36.2.10 *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 and ODU_UNI).

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

Services can use MediaChannels, 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).

Optical Service Order Data	Data Type	Applicable to Service Type	Description
service-name	String	All	Unique name to identify the circuit/VC.
service-description	String	All	Description of the VC that will help to identify the VC.
service-type	String		Service Type. Possible value: **optical** – for Optical Services **explicit-path** – for MPLS TE Explicit Path
service-subtype	String		Service SubType. Possible Values: **OCHNC, OCHCC, OCHTrail, OCHTRAIL_UNI, ODU_TUNNEL and ODU_UNI** – for Optical Services **mplste-explicit-path** – for MPLS TE Explicit Path
customer-ref	String		Customer FDN.
mutual-diverse	Boolean	**OCHTRAIL_UNI**	For mutual Diverse from one another.
diverse-from-name	String	**OCHTRAIL_UNI**	Diverse from Service name.
diverse-from-cfs-ref	FDN	**OCHTRAIL_UNI and ODU UNI**	Diversing current Service from the service which have the same AEND owning Entity value.
service-activate	Boolean		Activate Service.
direction	String		Service/Circuit direction. Possible Values: BIDIRECTIONAL.

Optical Service Order Data	Data Type	Applicable to Service Type	Description
optical-data	ce-data-service-type		Container for OPTICAL service configuration.
termination-point-list	List container	All	List of connection termination point configurations.
path-diversity	container	OCHNC, OCHCC and OCHTrail	This conatainer is applicable only for the services of type OCHNC, OCHCC and OCHTrail.
constraints	container	All OCH and MCH service	Constraints container will holds list of constraint values to be applied for a particular service.
constraint	container	All OCH and MCH 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	Description
optical-data		All	Optical data for service provisioning.
uni	Boolean	All	UNI Allows Bundling. Allows the use of multiple VLANs for this UNI.
label	String	All	Label for service provisioning.
protection	String	All	Protection Mechanism for service provisioning.
validation	Boolean	OCHNC, OCHCC, OCHTrail and OCHTRAIL_UNI	True or false.
optical-threshold	String	OCHNC, OCHCC, OCHTrail and OCHTRAIL_UNI	Optical Threshold for service provisioning.
optical-threshold-protected	String	OCHNC, OCHCC and OCHTrail.	Optical Threshold Protected for service provisioning.
up-stream-channel-power-offset	String	OCHNC, OCHCC and OCHTrail.	Up Stream Channel Power Offset for service provisioning.
down-stream-channel-power-offset	String	OCHNC, OCHCC and OCHTrail.	Down Stream Channel Power Offset for service provisioning.
ignore-path-alarm	Boolean	OCHNC, OCHCC and OCHTrail.	True or false.
allow-regeneration	Boolean	OCHNC, OCHCC, OCHTrail and OCHTRAIL_UNI	True or false.
restoration	String	OCHNC, OCHCC, OCHTrail and OCHTRAIL_UNI	Restoration for service provisioning.
revert	String	OCHNC, OCHCC and OCHTrail.	Revert for service provisioning.
soak-time	String	OCHNC and OCHTrail.	Soak Time for service provisioning.
priority	String	OCHNC, OCHCC, OCHTrail and OCHTRAIL_UNI	Priority for service provisioning.

validation-restoration	String	OCHNC, OCHCC and OCHTrail.	Validation Restoration for service provisioning.
optical-threshold-restoration	String	OCHNC, OCHCC and OCHTrail.	Optical Threshold Restoration for service provisioning.
optical-threshold-restoration-protected	String	OCHNC, OCHCC and OCHTrail.	Optical Threshold Restoration Protected for service provisioning.
frequency	String	OCHNC and OCHTrail.	Frequency for service provisioning.
width	String	OCHNC and OCHTrail.	Width for service provisioning.
frequency-required	Boolean	OCHNC and OCHTrail.	True or false.
frequency-protected	String	OCHNC and OCHTrail.	Frequency Protected for service provisioning.
width-protected	String	OCHNC and OCHTrail.	Width Protected for service provisioning.
frequency-protected-required	Boolean	OCHNC and OCHTrail.	True or false.
open-end	Boolean	OCHTrail, ODU_TUNNEL and ODU_UNI	True or false.
record-route	Boolean	ODU_TUNNEL and ODU_UNI	True or false.
otn-service-type	String	ODU_TUNNEL and ODU_UNI	OTN Service Type for service provisioning.
bandwidth	String	ODU_TUNNEL and ODU_UNI	Bandwidth for service provisioning.
framing-type	String	ODU_TUNNEL and ODU_UNI	Framing Type for service provisioning.
bit-rate	String	ODU_TUNNEL and ODU_UNI	Bit Rate for service provisioning.
protection-profile	String	ODU_TUNNEL and ODU_UNI	Protection Profile for service provisioning.
client-port-status	Enum	OCHCC and MCHCC	Applicable values Ex : UP and DOWN. 1. UP for create/provision a service 2. DOWN for delete/terminate a servcie

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	Description
termination-point-list	Termination point-list container	All	Yes	termination point list
termination-point-config	container	All	Yes	termination point config

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	Description
tp-ref	String (FDN)	All	Yes	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"
directionality	Identity	All	Yes	Source, Sink, and Bi-directional.
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	OCHNC service container
ochcc-data	container	OCHCC	Yes	OCHCC service container
och-trail-data	container	OCHTrail	Yes	OCHTrail service container
och-trail-uni-data	container	OCHTRAIL_UNI	Yes	OCHTRAIL_UNI service container
odu-tunnel-data	container	ODU_TUNNEL	Yes	ODU_TUNNEL service container
odu-uni-data	container	ODU_UNI	Yes	ODU_UNI service container
drop-port-ref	String	OCHNC	Yes	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	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	Possible Values: LOOSE and STRICT
diversity-type	Enum	OCHNC, OCHCC and OCHTrail	Yes, if 'path-diversity' is provided in payload	Possible Values: NE, LINK and SRRG
constraint	String	All OCH and MCH services	no	Name of the constraint
link-fdn	String	All OCH and MCH services	Yes, if constraint-type is LINK	FDN of TL , Ex : MD=CISCO_EPNM!TL=10.225.120.39:[WDMSIDE-B]--10.225.120.41:[WDMSIDE-A]
nd-ref	String	All OCH and MCH services	Yes, if constraint-type is NODE	FDN of Node, Ex : MD=CISCO_EPNM!ND=tcc200

Optical Service Order Data	Data Type	Applicable to Service Type	Is Mandatory	Description
constraint-type	Enum	All OCH and MCH services	Yes, if Constranints are part of payload	LINK, NODE
as	Enum	All OCH and MCH services	Yes, if Constranints are part of payload	INCLUDE and EXCLUDE
route	Enum	All OCH and MCH services	Yes, if Constranints are part of payload	Possible values are 'WORK', 'PROTECTED' and 'WORK_AND_PROTECTED'
Media Channels - spectrum switched optical network (SSON)				
mch-group-data	container	MCHG	Yes, for MCHGroup	Holdsl List of mchgroup service attributes
mchcc-data	container	MCHCC	Yes, for MCHCC	Holdsl List of mchcc service attributes
mchnc-data	container	MCHNC	Yes, for MCHNC	Holdsl List of mchnc service attributes
mch-trail-data	container	MCHTrail	Yes, for MCHTrail	Holdsl List of mchtrail service attributes
width	float	All MCH services	Yes	Default value is 50.0
auto-provisioning	Enum	All MCH services	Yes, for all MCH services	TRUE/FALSE
central-wavelength-required	Enum	All MCH services	Yes, only if "auto-provisioning" set FALSE.	TRUE/FALSE
central-wavelength	Float	All MCH services	Yes, only if "auto-provisioning" set FALSE.	Values range: 1528.773 To :1566.723
containing-mchg	String	All MCH services	No	MCH Group service name, this will taken as group for the currently creating MCH service

1.36.3 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.

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

1.36.3.1 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

1.36.4 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.

1.36.4.1 *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	/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

1.36.4.1.1 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

1.36.4.1.2 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 CIR/EIR or Custom rates
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

1.36.4.1.3 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

1.36.4.1.4 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

1.36.4.1.5 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

1.36.4.1.6 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

Response

- samples/Standalone_Y1564_Test/response.json

1.36.4.1.7 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

1.36.4.1.8 LSP Ping and Trace (Activate a Service)

Request

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

Response

- samples/LSP_Ping_And_Trace_Activate_A_Service/response.json

1.36.4.1.9 LSP Traceout Request and Response

Request

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

Response

- samples/LSP_TraceOut_Request_and_Response/response.json

1.36.4.1.10 PW Ping and Traceroute

Operation	**Description**
service-oam-config	This operation is to run PW ping and Traceroute
HTTP Method	**Resource Path**
POST	/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-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

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

1.36.4.1.11 CFM Ping

Operation	**Description**
service-oam-config	This operation is to run CFM Ping
HTTP Method	**Resource Path**
POST	/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-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

1.36.4.1.12 CFM Traceroute

Operation	**Description**
service-oam-config	This operation is to run CFM Traceroute
HTTP Method	**Resource Path**
POST	/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-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

Request

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

Response

- samples/CFM_Traceroute/response.json

samples/CFM_Traceroute/Cfm-traceroute-with-endpoints-response.xml

1.36.4.2 *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	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	

1.36.4.2.1 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

1.36.4.2.2 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

1.36.4.2.3 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

1.36.4.2.4 LSP Ping and Trace – GET Ping Details

Request

- GET /restconf/operations/v1/cisco-service-oam:service-oam-config/mpls-lsp-ping/1006?check-ready=true

Response

- samples/LSP_Ping_And_Trace_GET_Ping_Details/response.xml

1.36.4.2.5 GET LSP Traceout Details

Request

- GET /restconf/operations/v1/cisco-service-oam:service-oam-config/mpls-lsp-trace-route/1006?check-ready=true

Response

- samples/LSP_Ping_And_Trace_GET_Ping_Details/response.xml

1.36.4.2.6 GET PW Ping and Traceroute

Resource	**Description**
	Retrieves standalone service performance test result in Cisco EPN Manager.
HTTP Method	**Resource Path**
GET	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

1.36.4.2.7 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

1.36.4.2.8 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

1.36.5 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.

1.36.6 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.

1.36.6.1 *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

1.36.6.2 *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

1.36.6.3 *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	/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.
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	

1.36.6.4 *Get All Service Profiles*

Request

- GET /restconf/data/v1/cisco-service-profile:service-profileHTTP

Response

- samples/Get_All_Service_Profiles/response.xml

1.37 Customer CRUD

Customer resource path to create, retrieve, update, and delete Customer values.

1.37.1 Retrieve Customer

Resource	**Description**
Customer	Customer resource that is used in the provisioning order data. Retrieves the Customer resource.
HTTP Method	**Resource Path**
GET	/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.	
Yang file name	cisco-customer.yang	

1.37.1.1 *Get All Customers*

Request

- GET /restconf/data/v1/cisco-customer:customer

Response

- samples/Get_All_Customers/response.xml

1.37.2 Create Customer

Resource	Description
Customer	Creates a Customer Resource - Customer resource that is used in the provisioning order data.
HTTP Method	**Resource Path**
POST	/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.

Yang file name	cisco-customer.yang

Request

- samples/Create_Customer/request.xml
- samples/Create_Customer/request.json

1.37.3 Update Customer

Resource	**Description**	
Customer	Update the customer - Customer resource that is used in the provisioning order data.	
HTTP Method	**Resource Path**	
PUT	/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.	
Yang file name	cisco-customer.yang	

Request

- samples/Update_Customer/request.xml
- samples/Update_Customer/request.json

1.37.4 Delete Customer

Resource	**Description**	
Customer	Deletes the Customer - Customer resource that is used in the provisioning order data.	
HTTP Method	**Resource Path**	
DELETE	/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.
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

1.38 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.

1.38.1 Operations

1.38.1.1 *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	/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.
Yang file name	cisco-resource-activation.yang

1.38.1.1.1 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.
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.

1.38.1.1.2 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.

1.38.1.1.3 Run CLI Template

Request

- POST /restconf/operations/v1/cisco-resource-activation:get-cli-configuration-run-status
- samples/Run_CLI_Template/request.xml

Response

- samples/Run_CLI_Template/response.xml

1.38.1.1.4 Resource_Configuration-Create

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

1.38.1.1.5 Resource_Configuration-Modify

Request

- POST /restconf/ operations/v1/cisco-resource-activation:create-config
- samples/Resource_Configuration_Modify/request.xml
- samples/Resource_Configuration_Modify/request.json

Response

- samples/Resource_Configuration_Modify/response.xml

1.38.1.1.6 Resource_Configuration-Delete

Request

- POST /restconf/ operations/v1/cisco-resource-activation:create-config
- samples/Resource_Configuration_Delete/request.xml
- samples/Resource_Configuration_Delete/request.json

Response

- samples/Resource_Configuration_Delete/response.xml

1.38.1.2 *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	/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.
Yang file name	cisco-resource-activation.yang

1.38.1.2.1 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.

1.38.1.2.2 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

1.38.1.2.3 GET CLI Template

Request

- GET /restconf/data/v1/cisco-resource-activation:cli-template HTTP/1.1

Response

- samples/Get_CLI_Template/response.xml

1.39 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	/operations/v1/cisco-resource-activation:create-explicit-path /operations/v1/cisco-resource-activation:modify-explicit-path /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 • Device WorkCenter
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.
Yang file name	cisco-mpls-te-extension.yang

1.39.1 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.

1.39.2 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

path-entries	Data Type	Description
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-channel**) This fields is applicable only for Path Constraint type 'strict'.

1.39.1 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

1.39.2 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

1.39.3 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

1.40 MPLS TE WAE Server PCE Computed Path

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 and Write • MBC UI Framework Access • Device WorkCenter	
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.	
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

1.41 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 • Device WorkCenter	
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.	
Yang fiel name	cisco-protection-profile.yang	

1.41.1 Get All Protection Profile

Request

- GET /restconf/data/v1/cisco-resource-ems:protection-profile

Response

- samples/Get_All_Protection_Profile/response.xml

1.41.2 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

1.42 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	/operations/v1/cisco-resource-activation:create-protection-profile /operations/v1/cisco-resource-activation:modify-protection-profile /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 • Device WorkCenter
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.
Yang file name	cisco-protection-profile.yang

1.42.1 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

Name	Data Type	Description
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

1.42.2 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

1.42.3 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

1.42.4 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

1.43 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	/operations/v1/cisco-resource-activation:create-patch-cord /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 • Device WorkCenter
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.
Yang file name	cisco-topology.yang

1.43.1 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

1.43.2 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

1.43.3 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

1.43.4 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

1.43.5 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

1.44 Shared Risk Resource Assign Link and Node

Shared Risk Resource Assign and Un-Assing 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
description	String	Description for the SSRG
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.	
Yang file name	cisco-srrg.yang	

1.44.1 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

1.44.2 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

1.44.1 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

1.45 Shared Risk Resource UnAssign Node and Link

1.45.1 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

1.45.2 UnAssign SRRG to a Node

Request

- samples/UnAssign_SRRG_to_a_Node/request.xml

Response

- samples/UnAssign_SRRG_to_a_Node/response.xml

1.46 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

1.46.1 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

1.46.2 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.	
Yang file name	cisco-srrg.yang	

1.46.2.1 *GET SRRG Retrival*

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

1.46.2.2 *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

1.46.2.3 *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.	
Yang file name	cisco-srrg.yang	

1.46.1 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 restconf/data/v1/cisco-resource-network:srrg-pool*

Response

- samples/GET_SRRG_Pool_List/response.xml

1.46.1.1 *GET SRRG Pools List by FDN*

Request

- */restconf restconf/data/v1/cisco-resource-network:srrg-pool*?fdn=<fdn>

Response

- samples/GET_SRRG_Pool_List_by_FDN/response.xml

1.46.1.2 *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.	
Yang file name	cisco-srrg.yang	

1.46.2 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 restconf/data/v1/cisco-resource-network:srrg-pool-type*

Response

- samples/GET_SRRG_Pool_Type/response.xml

1.47 LAG Operations

The LAG operations supported are Create, Delete, Assign ports to LAG groups and Un-Assign ports from LAG groups.

1.47.1 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 • Device WorkCenter	
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.	
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

1.47.2 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 • Device WorkCenter	
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.	
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

1.47.3 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 • Device WorkCenter	
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.	
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

1.47.4 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 • Device WorkCenter	
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.	
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

1.48 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 retreived. Eg: /restconf/data/v1/cisco-resource-network:perf-

		metrics?tlFdn=MD=CISCO_EPNM!TL=10.58.234.42:[WDMSIDE-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.	
Yang file name	cisco-performance-analytics.yang	

1.48.1 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

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

1.49 Alarm Retrieval

Alarm Retrieval through Restconf with various filters.

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?{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=OTU20/6/

		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, interminate
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.	
Yang file name	cisco-alarms.yang	

1.49.1 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
source-object-ref	Fdn String	FDN for the Source device associcated 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-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

alarm -type	Data Type	Description
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
system-received-time	String	Alarm occurred time
system-update-time	String	Last updated time of the alarm
node-event-time	String	Device timestamp of the alarm
probable-cause	String	Probable cause of the alarm
service-affecting	String	Service Affecting with respect to alarm will have following values • service-affecting • non-service-affecting • service-affecting-unknown
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

1.49.2 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 associcated 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

1.49.3 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

1.49.4 Get All Alarms

Request

- GET /restconf/data/v1/cisco-rtm:alarm

Response

- samples/Get_All_Alarm/response.xml

1.49.5 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

1.49.6 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

1.49.7 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

1.49.8 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

1.49.9 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

1.49.10 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

1.49.11 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

1.49.12 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>
```

Request

- PUT /restconf/data/v1/cisco-alarm:handle-alarm
- samples/Alarm_Handling/request.xml

Response

- samples/Alarm_Handling/response.xml

1.49.13 Alarm to Service Association

Alarms releated 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

1.49.14 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 alrams 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.
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

1.49.15 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	/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 associcated 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.	
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

1.49.16 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.
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

1.49.17 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	/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 associcated 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.	
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

1.50 Controller Port

Controller Port resource path to retrieve and update media type controller mode.

1.50.1 Retrieve ControllerPort

Resource	**Description**	
ControllerPort	Retrieves the Controller Port.	
HTTP Method	**Resource Path**	
GET	/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 • Device WorkCenter	
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.	
Yang File Name	cisco-nrf-controller.yang	

1.50.2 Get Controller Port

Request

- GET https://{{host}}/restconf/data/v1/cisco-nrf-controller:controller-port

Response

- samples/Get_Controller_Port/response.xml

1.50.3 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	/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.
Yang File Name	cisco-nrf-controller.yang

1.50.4 Update Controller Port – MediaType Controller Mode

Request

- PUT /restconf/data/v1/cisco-nrf-controller:controller-port
- samples/Update_Controller_Port/request.xml

1.51 LMP Link Create / Delete / Retrieval

LMP Link creation and deletion are done via., POST operations. LMP Links can be created between NCS2K and NCS4K or NCS4K and NCS4K nodes.
LMP Link creation requies the source and destination endpoints (Termination point FDN) to be specified.
LMP Link deletion requires the LMP Link FDN to be passed as a query parameter to the DELETE URL.

LMP Link retrieval is similar to regular topological link retrieval. The Topological Link retrieval URL is provided with the LMP Link FDN as query parameter.

1.51.1 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		
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		
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**
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.	
Yang file name	cisco-topology.yang	

1.51.2 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
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.	
Yang file name	cisco-topology.yang	

1.51.3 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

1.51.4 LMP Link Delete Request / Response

Request

- POST /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

1.51.5 LMP Link Retrieval

LMP Link is treated similar to 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

1.52 PCE Computation Path

Request

- POST /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

1.53 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

1.53.1 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.

1.54 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	/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 • Device WorkCenter
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.
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

1.55 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	/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 • Device WorkCenter
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.
Yang file name	cisco-nrf-physical.yang

1.55.1 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

1.55.2 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>

1.55.3 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.

1.55.4 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

1.55.5 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

1.56 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	/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 • Device WorkCenter
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.
Yang file name	Cisco-service-action.yang

1.56.1 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

attribute	Data Type	Description
protection-role	Enum	Accepts following values • working-path • protect-path • restore-path

1.56.2 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 device-configuration	String(fdn) String	Fdn of the node Eg: MD=CISCO_EPNM!ND=454A-234-50 Actual device configuration when the operation is applied to the device

1.56.3 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

1.56.4 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

1.56.5 Lockout on Working Path

1.56.5.1 *Request*

POST /restconf/data/v1/cisco-service-action:protection-switch

- samples/Lockout_on_Working_Path/request.xml

1.56.5.2 *Response*

- samples/Lockout_on_Working_Path/response.xml

1.56.6 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

1.56.1 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

1.56.2 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

1.57 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.
Yang File Name	cisco-service-action.yang

1.57.1 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

1.57.2 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

1.57.3 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.

1.58 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 value : EQ_MODE_5G
4	resource-name	String	Slot to be used e.g. slot0/3

1.58.1 Request

- POST /restconf/data/v1/cisco-nrf-physical:provision-equipment
- samples/Provision_5G_Slot_Mode_to_EOWYN_Line_Card/request.xml

1.58.2 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

1.59 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 • Device WorkCenter
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.
Yang file name	cisco-nrf-physical.yang

1.59.1 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

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.

YANG Schema for Cisco EPN Manager RESTCONF NBI Data Modules

Download Yang and XSD Schema files.

1.60 Yang Modules

1.60.1 List Supported Yang Modules

Request

```
GET /restconf/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

1.61 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.

1.62 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

1.63 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 the RESTConf web application for these changes to come into effect. This can be done by running the 'touch' command on the web.xml file located at:
  - /opt/CSCOlumos/server/webapps/restconf/WEB-INF/web.xml

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”

1.64 Notification URLs

1.64.1 Connection-Less

/restconf/data/v1/cisco-notifications:subscriptions/

1.64.2 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

1.65 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.

1.66 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
    - **Method**: GET
    - **Authentication**: Basic Authentication
    - **NOTE**: "root" user can see subscriptions made by any user while any non-root user can see only notification details that they subscribed to.
    - samples/notifications/subscription_retrieval.xml
- To get details of a single subscription:
    - **URL**: /restconf/data/v1/cisco-notifications:subscription/{subscription-id}
    - **Method**: GET
    - **Authentication**: Basic Authentication
- To delete a subscription:
    - **URL**: /restconf/data/v1/cisco-notifications:subscription/{subscription-id}
    - **Method:** DELETE
    - **Authentication:** Basic Authentication

1.67 Notification Filters

1.67.1 Filter Support

Filters are supported for the following notification types:

- Inventory
- Alarms

1.67.2 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”

1.67.3 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.

1.67.4 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:

- customer
- customer-facing-service
- equipment
- ipsla-profile-details
- link-aggregation-group
- ni
- node
- physical-connector
- qos-profile
- shared-risk-resource-group
- shared-risk-resource-group-pool
- shared-risk-resource-group-pool-type
- termination-point
- topological-link
- virtual-connection
- virtual-connection-multi-layer-route-list

Subscribing with multiple elementType filters is supported. A subscription with the filters below will receive both RC_Node notifications AND Equipment notifications.

- 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

1.67.5 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

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
    - 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%20ASR%204000&productFamily=Routers

1.67.6 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"
     }
}
```

1.68 Inventory Notifications

Inventory notifications in Cisco EPN Manager restconf is supported for three types of operations:

- CREATE
    - when a device is added to Cisco EPN Manager
    - when a service was provisioned on one or more devices that created an object in the system.
    - In this case, the entire object that was created is sent as part of the notification.
- MODIFY/ UPDATE/ AVC (Attribute Value Change)
    - when a device or object that exists in the system is updated.
    - 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
    - when a device or object is deleted from the system.
    - 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

Authorization Required	One or more from following for /restconf/streams/v1/template-execution[.xml|.json] • Chassis View Read • Chassis View Read and Write • Circuit or VC Provisioning • Circuit or VC Monitoring and Troubleshooting • Network Topology • Device WorkCenter 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 • Device WorkCenter • View Alerts and Events Configure Templates One or more from following

1.68.1 Inventory Notification - Examples

1.68.1.1 *Create notification*

- samples/notifications/create_notification.xml

1.68.1.2 *Update Notification*

- samples/notifications/update_notification.xml

1.68.1.3 *Delete Notification*

- samples/notifications/delete_notification.xml

1.69 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, FAILED otherwise)
- 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 • Device WorkCenter • View Alerts and Events • Configure Templates

1.70 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`

1.70.1 Alarm Specific Filters

Alarms also have 2 filters exclusively available to them:

- category
- severity

This filters are applied the same as device level filters.

1.70.1.1 *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 • Device WorkCenter • View Alerts and Events • Configure Templates

1.71 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 • Device WorkCenter • View Alerts and Events • Configure Templates

1.72 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 • Device WorkCenter • View Alerts and Events • Configure Templates

1.73 High-Availability Notifications

HA notifications are sent for:

- Failover: when the secondary becomes active
- Failback: when the primary becomes active again.

1.73.1 Sample HA Notifications

1.73.1.1 *Failover*

- samples/notifications/ha.failover.xml

1.73.1.2 *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 • Device WorkCenter • View Alerts and Events • Configure Templates

1.74 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".

1.74.1 Sample client code

- samples/notifications/notification_client_code.txt

1.75 Notifications Schema

- samples/notifications/notification_schema.yang

Software Image Management (SWIM)

1.76 Job Details

1.76.1 Operations

The following sub-sections provide the details of the operations that can be used for retrieving the job details for swim jobs.

1.76.2 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.

1.76.2.1 *Service Request*

Name	**Type**	**Description**
jobId	Long	The Job Id

1.76.2.2 *Service Response*

Name	**Type**	**Description**
SwimDashboardJobDetailsDTO	Container element	Holds the data for swim job details

1.77 Collection Service

1.77.1 Operations

The following sub-sections provide the details of the operations that can be used for importing images to EPNM.

1.77.2 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.

1.77.2.1 *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.

1.77.2.2 *Service Response*

Name	Type	Description
SwimJobResultDTO	Container element	Holds the data for job schedule result.

1.78 Commit Service

1.78.1 Operations

The following sub-sections provide the details of the operations that can be used to commit change in the device.

1.78.2 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.

1.78.2.1 *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.

1.78.2.2 *Service Response*

Name	Type	Description
SwimJobResultDTO	Container element	Holds the data for job schedule result.

1.79 Distribution Service

1.79.1 Operations

The following sub-sections provide the details of the operations that can be used to copy image to cisco device.

1.79.2 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.

1.79.2.1 *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.

1.79.2.2 *Service Response*

Name	Type	Description
SwimJobResultDTO	Container element	Holds the data for job schedule result.

1.80 Activation Service

1.80.1 Operations

The following sub-sections provide the details of the operations that can be used to install or activate image.

1.80.2 Service

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.

1.80.2.1 *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.

1.80.2.2 *Service Response*

Name	**Type**	**Description**
SwimJobResultDTO	Container element	Holds the data for job schedule result.

References

RESTCONF Specification
YANG Specification