



# Use gRPC Protocol to Define Network Operations with Data Models

---

XR devices ship with the YANG files that define the data models they support. Using a management protocol such as NETCONF or gRPC, you can programmatically query a device for the list of models it supports and retrieve the model files.

gRPC is an open-source RPC framework. It is based on Protocol Buffers (Protobuf), which is an open source binary serialization protocol. gRPC provides a flexible, efficient, automated mechanism for serializing structured data, like XML, but is smaller and simpler to use. You define the structure using protocol buffer message types in `.proto` files. Each protocol buffer message is a small logical record of information, containing a series of name-value pairs.

gRPC encodes requests and responses in binary. gRPC is extensible to other content types along with Protobuf. The Protobuf binary data object in gRPC is transported over HTTP/2.

gRPC supports distributed applications and services between a client and server. gRPC provides the infrastructure to build a device management service to exchange configuration and operational data between a client and a server. The structure of the data is defined by YANG models.



---

**Note** All 64-bit IOS XR platforms support gRPC and TCP protocols. All 32-bit IOS XR platforms support only TCP protocol.

---

Cisco gRPC IDL uses the protocol buffers interface definition language (IDL) to define service methods, and define parameters and return types as protocol buffer message types. The gRPC requests are encoded and sent to the router using JSON. Clients can invoke the RPC calls defined in the IDL to program the router.

The following example shows the syntax of the proto file for a gRPC configuration:

```
syntax = "proto3";

package IOSXRExtensibleManagabilityService;

service gRPCConfigOper {

    rpc GetConfig(ConfigGetArgs) returns(stream ConfigGetReply) {};

    rpc MergeConfig(ConfigArgs) returns(ConfigReply) {};

    rpc DeleteConfig(ConfigArgs) returns(ConfigReply) {};
```

```

rpc ReplaceConfig(ConfigArgs) returns(ConfigReply) {};

rpc CliConfig(CliConfigArgs) returns(CliConfigReply) {};

rpc GetOper(GetOperArgs) returns(stream GetOperReply) {};

rpc CommitReplace(CommitReplaceArgs) returns(CommitReplaceReply) {};
}
message ConfigGetArgs {
    int64 ReqId = 1;
    string yangpathjson = 2;
}

message ConfigGetReply {
    int64 ResReqId = 1;
    string yangjson = 2;
    string errors = 3;
}

message GetOperArgs {
    int64 ReqId = 1;
    string yangpathjson = 2;
}

message GetOperReply {
    int64 ResReqId = 1;
    string yangjson = 2;
    string errors = 3;
}

message ConfigArgs {
    int64 ReqId = 1;
    string yangjson = 2;
}

message ConfigReply {
    int64 ResReqId = 1;
    string errors = 2;
}

message CliConfigArgs {
    int64 ReqId = 1;
    string cli = 2;
}

message CliConfigReply {
    int64 ResReqId = 1;
    string errors = 2;
}

message CommitReplaceArgs {
    int64 ReqId = 1;
    string cli = 2;
    string yangjson = 3;
}

message CommitReplaceReply {
    int64 ResReqId = 1;
    string errors = 2;
}

```

Example for gRPCExec configuration:

```

service gRPCExec {
    rpc ShowCmdTextOutput(ShowCmdArgs) returns(stream ShowCmdTextReply) {};
    rpc ShowCmdJSONOutput(ShowCmdArgs) returns(stream ShowCmdJSONReply) {};
}

message ShowCmdArgs {
    int64 ReqId = 1;
    string cli = 2;
}

message ShowCmdTextReply {
    int64 ResReqId = 1;
    string output = 2;
    string errors = 3;
}

```

Example for OpenConfiggRPC configuration:

```

service OpenConfiggRPC {
    rpc SubscribeTelemetry(SubscribeRequest) returns (stream SubscribeResponse) {};
    rpc UnSubscribeTelemetry(CancelSubscribeReq) returns (SubscribeResponse) {};
    rpc GetModels(GetModelsInput) returns (GetModelsOutput) {};
}

message GetModelsInput {
    uint64 requestId = 1;
    string name = 2;
    string namespace = 3;
    string version = 4;
    enum MODLE_REQUEST_TYPE {
        SUMMARY = 0;
        DETAIL = 1;
    }
    MODLE_REQUEST_TYPE requestType = 5;
}

message GetModelsOutput {
    uint64 requestId = 1;
    message ModelInfo {
        string name = 1;
        string namespace = 2;
        string version = 3;
        GET_MODEL_TYPE modelType = 4;
        string modelData = 5;
    }
    repeated ModelInfo models = 2;
    OC_RPC_RESPONSE_TYPE responseCode = 3;
    string msg = 4;
}

```

This article describes, with a use case to configure interfaces on a router, how data models helps in a faster programmatic and standards-based configuration of a network, as compared to CLI.

- [gRPC Operations, on page 4](#)
- [gRPC Network Management Interface, on page 5](#)
- [gRPC Network Operations Interface , on page 5](#)
- [gRPC Network Security Interface , on page 6](#)
- [gRPC Authentication Modes, on page 12](#)

- [Configure Interfaces Using Data Models in a gRPC Session, on page 15](#)

## gRPC Operations

The following are the defined manageability service gRPC operations for Cisco IOS XR:

gRPC Operation	Description
GetConfig	Retrieves the configuration from the router.
GetModels	Gets the supported Yang models on the router
MergeConfig	Merges the input config with the existing device configuration.
DeleteConfig	Deletes one or more subtrees or leaves of configuration.
ReplaceConfig	Replaces part of the existing configuration with the input configuration.
CommitReplace	Replaces all existing configuration with the new configuration provided.
GetOper	Retrieves operational data.
CliConfig	Invokes the input CLI configuration.
ShowCmdTextOutput	Returns the output of a show command in the text form
ShowCmdJSONOutput	Returns the output of a show command in JSON form.

### gRPC Operation to Get Configuration

This example shows how a gRPC GetConfig request works for LLDP feature.

The client initiates a message to get the current configuration of LLDP running on the router. The router responds with the current LLDP configuration.

gRPC Request (Client to Router)	gRPC Response (Router to Client)
<pre>rpc GetConfig {   "Cisco-IOS-XR-cdp-cfg:cdp": [     "cdp": "running-configuration"   ] }  rpc GetConfig {   "Cisco-IOS-XR-ethernet-lldp-cfg:lldp": [     "lldp": "running-configuration"   ] }</pre>	<pre>{   "Cisco-IOS-XR-cdp-cfg:cdp": {     "timer": 50,     "enable": true,     "log-adjacency": [       null     ],     "hold-time": 180,     "advertise-vl-only": [       null     ]   } }  {   "Cisco-IOS-XR-ethernet-lldp-cfg:lldp": {     "timer": 60,     "enable": true,     "reinit": 3,     "holdtime": 150   } }</pre>

## gRPC Network Management Interface

gRPC Network Management Interface (gNMI) is a gRPC-based network management protocol used to modify, install or delete configuration from network devices. It is also used to view operational data, control and generate telemetry streams from a target device to a data collection system. It uses a single protocol to manage configurations and stream telemetry data from network devices.

The subscription in a gNMI does not require prior sensor path configuration on the target device. Sensor paths are requested by the collector (such as pipeline), and the subscription mode can be specified for each path. gNMI uses gRPC as the transport protocol and the configuration is same as that of gRPC.

## gRPC Network Operations Interface

gRPC Network Operations Interface (gNOI) defines a set of gRPC-based microservices for executing operational commands on network devices. These services are to be used in conjunction with gRPC network management interface (gNMI) for all target state and operational state of a network. gNOI uses gRPC as the transport protocol and the configuration is same as that of gRPC. For more information about gNOI, see the [Github](#) repository.



**Note** This feature is not supported for the following PIDs:

- N540-ACC-SYS
- N540X-ACC-SYS (Premium)
- N540-24Z8Q2C-SYS

# gRPC Network Security Interface

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
gRPC Network Security Interface	Release 7.11.1	<p>This release implements authorization mechanisms to restrict access to gRPC applications and services based on client permissions. This is made possible by introducing an authorization protocol buffer service for gRPC Network Security Interface (gNSI).</p> <p>Prior to this release, the gRPC services in the gNSI systems could be accessed by unauthorized users.</p> <p>This feature introduces the following change:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>• <b>gnsi load service authorization policy</b></li> <li>• <b>show gnsi service authorization policy</b></li> </ul> <p>To view the specification of gNSI, see <a href="#">Github</a> repository.</p>

gRPC Network Security Interface (gNSI) is a repository which contains security infrastructure services necessary for safe operations of an OpenConfig platform. The services such as authorization protocol buffer manage a network device's certificates and authorization policies.

This feature introduces a new authorization protocol buffer under gRPC gNSI. It contains gNSI.authz policies which prevent unauthorized users to access sensitive information. It defines an API that allows the configuration of the RPC service on a router. It also controls the user access and restricts authorization to update specific RPCs.

By default, gRPC-level authorization policy is provisioned using [Secure ZTP](#). If the router is in zero-policy mode that is, in the absence of any policy, you can use gRPC authorization policy configuration to restrict access to specific users. The default authorization policy at the gRPC level can permit access to all RPCs except for the gNSI.authz RPCs.

If there is no policy specified or the policy is invalid, the router will fall back to zero-policy mode, in which the default behavior allows access to all gRPC services to all the users if their profiles are configured. If an invalid policy is configured, you can revert it by loading a valid policy using exec command **gnsi load service authorization policy**. For more information on how to create user profiles and update authorization policy for these user profiles, see [How to Update gRPC-Level Authorization Policy, on page 7](#). Using **show gnsi service authorization policy** command, you can see the active policy in a router.

We have introduced the following commands in this release :

- **gnsi load service authorization policy**: To load and update the gRPC-level authorization policy in a router.
- **show gnsi service authorization policy**: To see the active policy applied in a router.



**Note** When both gNSI and gNOI are configured, gNSI takes precedence over gNOI. If neither gNSI nor gNOI is configured, then tls trsutpoint's data is considered for certificate management.

The following RPCs are used to perform key operations at the system level such as updating and displaying the current status of the authorization policy in a router.

**Table 2: Operations**

RPC	Description
gNSI.authz.Rotate()	Updates the gRPC-level authorization policy.
gNSI.authz.Probe()	Verifies the authenticity of a user based on the defined policy of the gRPC-level authorization policy engine.
gNSI.authz.Get()	Shows the current instance of the gRPC-level authorization policy, including the version and date of creation of the policy.

## How to Update gRPC-Level Authorization Policy

gRPC-level authorization policy is configured by default at the time of router deployment using secure ZTP. You can update the same gRPC-level authorization policy using any of two the following methods:

- Using gNSI Client.
- Using exec command.

### Updating the gRPC-Level Authorization Policy in the Router Using gNSI Client

#### Before you start

When a router boots for the first time, it should have the following prerequisites:

- The gNSI.authz service is up and running.
- The default gRPC-level authorization policy is added for all gRPC services.
- The default gRPC-level authorization policy allows access to all RPCs.

The following steps are used to update the gRPC-level authorization policy:

1. Initiate the **gNSI.authz.Rotate()** streaming RPC. This step creates a streaming connection between the router and management application (client).




---

**Note** Only one `gNSI.authz.Rotate()` must be in progress at a time. Any other RPC request is rejected by the server.

---

- The client uploads new gRPC-level authorization policy using the **UploadRequest** message.




---

**Note**

- There must be only one gRPC-level authorization policy in the router. All the policies must be defined in the same gRPC-level authorization policy which is being updated. As `gNSI.authz.Rotate()` method replaces all previously defined or used policies once the **finalize** message is sent.
- The upgrade information is passed to the `version` and the `created_on` fields. These information are not used by the `gNSI.authz` service. It is designed to help you to track the active gRPC-level authorization policy on a particular router.

---

- The router activates the gRPC-level authorization policy.
- The router sends the `UploadResponse` message back to the client after activating the new policy.
- The client verifies the new gRPC-level authorization policy using separate `gNSI.authz.Probe()` RPCs.
- The client sends the **FinalizeRequest** message, indicating the previous gRPC-level authorization policy is replaced.




---

**Note** It is not recommended to close the stream without sending the **finalize** message. It results in the abandoning of the uploaded policy and rollback to the one that was active before the `gNSI.authz.Rotate()` RPC started.

---

Below is an example of a gRPC-level authorization policy that allows admins, V1, V2, V3 and V4, access to all RPCs that are defined by the `gNSI.ssh` interface. All the other users won't have access to call any of the `gNSI.ssh` RPCs:

```
{
  "version": "version-1",
  "created_on": "1632779276520673693",
  "policy": {
    "name": "gNSI.ssh policy",
    "allow_rules": [{
      "name": "admin-access",
      "source": {
        "principals": [
          "spiffe://company.com/sa/V1",
          "spiffe://company.com/sa/V2"
        ]
      }
    }],
    "request": {
      "paths": [
        "/gnsi.ssh.Ssh/*"
      ]
    }
  }
},
  "deny_rules": [{
    "name": "sales-access",
```



```

"source": {
  "principals": [
    "spiffe://company.com/sa/V3",
    "spiffe://company.com/sa/V4"
  ]
},
"request": {
  "paths": [
    "/gnsi.ssh.Ssh/MutateAccountCredentials",
    "/gnsi.ssh.Ssh/MutateHostCredentials"
  ]
}
}}
}

```

### Updating the gRPC-Level Authorization Policy file Using Exec Command

Use the following steps to update the authorization policy in the router.

1. Create the users profiles for the users who need to be added in the authorization policy. You can skip this step if you have already defined the user profiles.

The following example creates three users who are added in the authorization policy.

```

Router(config)#username V1
Router(config-un)#group root-lr
Router(config-un)#group cisco-support
Router(config-un)#secret x
Router(config-un)#exit
Router(config)#username V2
Router(config-un)#group root-lr
Router(config-un)#password x
Router(config-un)#exit
Router(config)#username V3
Router(config-un)#group root-lr
Router(config-un)#password x
Router(config-un)#commit

```

2. Enable **tls-mutual** to establish the secure mutual between the client and the router.

```

Router(config)#grpc
Router(config-grpc)#port 0
Router(config-grpc)#tls-mutual
Router(config-grpc)#certificate-authentication
Router(config-grpc)#commit

```

3. Define the gRPC-level authorization policy.

The following sample gRPC-level authorization policy defines authorization policy for the users V1, V2 and V3.

```

{
  "name": "authz",
  "allow_rules": [
    {
      "name": "allow all gNMI for all users",
      "source": {
        "principals": [
          "*"
        ]
      }
    }
  ]
}

```

```

    },
    "request": {
      "paths": [
        "*"
      ]
    }
  },
],
"deny_rules": [
  {
    "name": "deny gNMI set for oper users",
    "source": {
      "principals": [
        "V1"
      ]
    },
    "request": {
      "paths": [
        "/gnmi.gNMI/Get"
      ]
    }
  },
  {
    "name": "deny gNMI set for oper users",
    "source": {
      "principals": [
        "V2"
      ]
    },
    "request": {
      "paths": [
        "/gnmi.gNMI/Get"
      ]
    }
  },
  {
    "name": "deny gNMI set for oper users",
    "source": {
      "principals": [
        "V3"
      ]
    },
    "request": {
      "paths": [
        "/gnmi.gNMI/Set"
      ]
    }
  }
]
}

```

#### 4. Copy the gRPC-level authorization policy to the router.

The following example copies the gNSI Authz policy to the router:

```

-bash-4.2$ scp test.json V1@192.0.2.255:/disk0:/
Password:
test.json
100% 993 161.4KB/s 00:00
-bash-4.2$

```

#### 5. Activate the gRPC-level authorization policy to the router.

The following example loads the policy to the router.

```
Router(config)#gnsi load service authorization policy /disk0:/test.json
Successfully loaded policy
```

### Verification

Use the **show gnsi service authorization policy** to verify if the policy is active in the router.

```
Router#show gnsi service authorization policy
Wed Jul 19 10:56:14.509 UTC{
  "version": "1.0",
  "created_on": 1700816204,
  "policy": {
    "name": "authz",
    "allow_rules": [
      {
        "name": "allow all gNMI for all users",
        "request": {
          "paths": [
            "*"
          ]
        },
        "source": {
          "principals": [
            "*"
          ]
        }
      }
    ],
    "deny_rules": [
      {
        "name": "deny gNMI set for oper users",
        "request": {
          "paths": [
            "/gnmi.gNMI/*"
          ]
        },
        "source": {
          "principals": [
            "User1"
          ]
        }
      }
    ]
  }
}
```

In the following example, User1 user tries to access the **get** RPC request for which the permission is denied in the above authorization policy.

```
bash-4.2$ ./gnmi_cli -address 198.51.100.255 -ca_cert
certs/certs/ca.cert -client_cert certs/certs/User1.pem -client_key
certs/certs/User1.key -server_name ems.cisco.com -get -proto get-oper.proto
```

### Output

```
E0720 14:49:42.277504 26473 gnmi_cli.go:195]
target returned RPC error for Get({"path":{"origin:"openconfig-interfaces"
elem:{name:"interfaces"
elem:{name:"interface" key:{key:"name" value:"HundredGigE0/0/0/0"}}}
type:OPERATIONAL encoding:JSON_IETF}):
rpc error: code = PermissionDenied desc = unauthorized RPC request rejected
```

# gRPC Authentication Modes

gRPC supports the following authentication modes to secure communication between clients and servers. These authentication modes help ensure that only authorized entities can access the gRPC services, like gNOI, gRIBI, and P4RT. Upon receiving a gRPC request, the device will authenticate the user and perform various authorization checks to validate the user.

The following table lists the authentication type and configuration requirements:

**Table 3: gRPC Authentication Modes and Configuration Requirements**

Type	Authentication Method	Authorization Method	Configuration Requirement	Requirement From Client
Metadata with TLS	username, password	username	<b>grpc</b>	username, password, and CA
Metadata without TLS	username, password	username	<b>grpc no-tls</b>	username, password
Metadata with Mutual TLS	username, password	username	<b>grpc tls-mutual</b>	username, password, client certificate, client key, and CA
Certificate based Authentication	client certificate's common name field	username from client certificate's common name field	<b>grpc tls-mutual</b> and <b>grpc certificate authentication</b>	client certificate, client key, and CA

## Certificate based Authentication

In Extensible Manageability Services (EMS) gRPC, the certificates play a vital role in ensuring secure and authenticated communication. The EMS gRPC utilizes the following certificates for authentication:

```
/misc/config/grpc/ems.pem
/misc/config/grpc/ems.key
/misc/config/grpc/ca.cert
```



**Note** For clients to use the certificates, ensure to copy the certificates from **/misc/config/grpc/**

## Generation of Certificates

These certificates are typically generated using a Certificate Authority (CA) by the device. The EMS certificates, including the server certificate (**ems.pem**), public key (**ems.key**), and CA certificate (**ca.cert**), are generated with specific parameters like the common name **ems.cisco.com** to uniquely identify the EMS server and placed in the **/misc/config/grpc/** location.

The default certificates that are generated by the server are Server-only TLS certificates and by using these certificates you can authenticate the identity of the server.

## Usage of Certificates

These certificates are used for enabling secure communication through Transport Layer Security (TLS) between gRPC clients and the EMS server. The client should use **ems.pem** and **ca.cert** to initiate the TLS authentication.

To update the certificates, ensure to copy the new certificates that has been generated earlier to the location and restart the server.

### Custom Certificates

If you want to use your own certificates for EMS gRPC communication, then you can follow a workflow to generate a custom certificates with the required parameters and then configure the EMS server to use these custom certificates. This process involves replacing the default EMS certificates with the custom ones and ensuring that the gRPC clients also trust the custom CA certificate. For more information on how to customize the **common-name**, see *Certificate Common-Name For Dial-in Using gRPC Protocol*.

## Certificate Common-Name For Dial-in Using gRPC Protocol

Table 4: Feature History Table

Feature Name	Release Information	Description
Certificate Common-Name For Dial-in Using gRPC Protocol	Release 24.1.1	<p>You can now specify a <b>common-name</b> for the certificate generated by the router while using gRPC dial-in. Earlier, the <b>common-name</b> in the certificate was fixed as <i>ems.cisco.com</i> and was not configurable. Using a specified <b>common-name</b> avoids potential certification failures where you may specify a hostname different from the fixed common name to connect to the router.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>•</li> </ul> <p><b>YANG Data Model:</b></p> <ul style="list-style-type: none"> <li>• New XPath for <code>Cisco-IOS-XR-um-grpc-cfg.yang</code></li> <li>• New XPath for <code>Cisco-IOS-XR-man-ems-cfg</code></li> </ul> <p>(see <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a>)</p>

When using gRPC dial-in on Cisco IOS-XR router, the **common-name** associated with the certificate generated by the router is fixed as *ems.cisco.com* and this caused failure during certificate verification.

From Cisco IOS XR Release 24.1.1, you can now have the flexibility of specifying the common-name in the certificate using the **grpc certificate common-name** command. This allows gRPC clients to verify if the domain name in the certificate matches the domain name of the gRPC server being accessed.

## Configure Certificate Common Name For Dial-in

Configure a common name to be used in EMSD certificates for gRPC dial-in.

### Procedure

**Step 1** Configure a common name.

#### Example:

```
Router#config
Router(config)#grpc
Router(config-grpc)#certificate common-name cisco.com
Router(config-grpc)#commit
```

Use the show command to verify the common name:

```
Router#show grpc
Certificate common name           : cisco.com
```

**Note** For the above configuration to be successful, ensure to regenerate the certificate. so that the new EMSD certificates include the configured common name.

To **regenerate** the self-signed certificate, perform the following steps.

**Step 2** Remove the certificates: /misc/config/grpc/ems.pem, /misc/config/grpc/ems.key, and /misc/config/grpc/ca.cert from /misc/config/grpc file.

#### Example:

```
Router#run ls -ltr /misc/config/grpc/

total 16
drwx-----. 2 root root 4096 Feb 14 09:17 dialout
-rw-rw-rw-. 1 root root 1505 Feb 14 10:58 ems.pem
-rw-----. 1 root root 1675 Feb 14 10:58 ems.key
-rw-r--r--. 1 root root 1505 Feb 14 10:58 ca.cert

Router#run rm -rf /misc/config/grpc/ems.pem /misc/config/grpc/ems.key

Router#run ls -ltr /misc/config/grpc/

total 8
drwx-----. 2 root root 4096 Feb 14 09:17 dialout
-rw-r--r--. 1 root root 1505 Feb 14 10:58 ca.cert
```

**Step 3** Restart gRPC server by toggling the TLS configuration.

Configure gRPC with non TLS and then re-configure with TLS.

#### Example:

```
Router#config
Router(config)#grpc
Router(config-grpc)#no-tls
Router(config-grpc)#commit
```

```

Router#run ls -ltr /misc/config/grpc/

total 8
drwx-----. 2 root root 4096 Feb 14 09:17 dialout
-rw-r--r--. 1 root root 1505 Feb 14 10:58 ca.cert

Router#config
Router(config)#grpc
Router(config-grpc)#no no-tls
Router(config-grpc)#commit

Router#run ls -ltr /misc/config/grpc/

total 16
drwx-----. 2 root root 4096 Feb 14 09:17 dialout
-rw-rw-rw-. 1 root root 1505 Feb 14 14:23 ems.pem
-rw-----. 1 root root 1675 Feb 14 14:23 ems.key
-rw-r--r--. 1 root root 1505 Feb 14 14:23 ca.cert

```

Copy the newly generated `/misc/config/grpc/ems.pem` certificate in this path (from the device) to the gRPC client.

## Configure Interfaces Using Data Models in a gRPC Session

Google-defined remote procedure call () is an open-source RPC framework. gRPC supports IPv4 and IPv6 address families. The client applications use this protocol to request information from the router, and make configuration changes to the router.

The process for using data models involves:

- Obtain the data models.
- Establish a connection between the router and the client using gRPC communication protocol.
- Manage the configuration of the router from the client using data models.



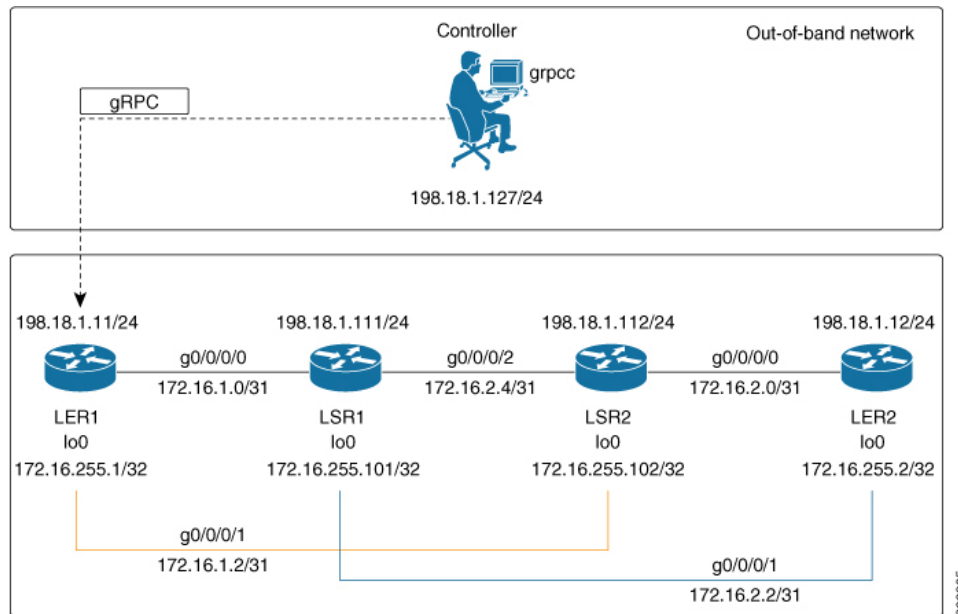
**Note** Configure AAA authorization to restrict users from uncontrolled access. If AAA authorization is not configured, the command and data rules associated to the groups that are assigned to the user are bypassed. An IOS-XR user can have full read-write access to the IOS-XR configuration through Network Configuration Protocol (NETCONF), google-defined Remote Procedure Calls (gRPC) or any YANG-based agents. In order to avoid granting uncontrolled access, enable AAA authorization using **aaa authorization exec** command before setting up any configuration. For more information about configuring AAA authorization, see the *System Security Configuration Guide*.

In this section, you use native data models to configure loopback and ethernet interfaces on a router using a gRPC session.

Consider a network topology with four routers and one controller. The network consists of label edge routers (LER) and label switching routers (LSR). Two routers LER1 and LER2 are label edge routers, and two routers LSR1 and LSR2 are label switching routers. A host is the controller with a gRPC client. The controller communicates with all routers through an out-of-band network. All routers except LER1 are pre-configured with proper IP addressing and routing behavior. Interfaces between routers have a point-to-point configuration with /31 addressing. Loopback prefixes use the format `172.16.255.x/32`.

The following image illustrates the network topology:

**Figure 1: Network Topology for gRPC session**



You use Cisco IOS XR native model `Cisco-IOS-XR-ifmgr-cfg.yang` to programmatically configure router LER1.

### Before you begin

- Retrieve the list of YANG modules on the router using NETCONF monitoring RPC. For more information
- Configure Transport Layer Security (TLS). Enabling gRPC protocol uses the default HTTP/2 transport with no TLS. gRPC mandates AAA authentication and authorization for all gRPC requests. If TLS is not configured, the authentication credentials are transferred over the network unencrypted. Enabling TLS ensures that the credentials are secure and encrypted. Non-TLS mode can only be used in secure internal network.

## Procedure

### Step 1 Enable gRPC Protocol

To configure network devices and view operational data, gRPC protocol must be enabled on the server. In this example, you enable gRPC protocol on LER1, the server.

**Note** Cisco IOS XR 64-bit platforms support gRPC protocol. The 32-bit platforms do not support gRPC protocol.

- Enable gRPC over an HTTP/2 connection.

#### Example:

```
Router#configure
```



```
Router(config)#grpc
Router(config-grpc)#port <port-number>
```

The port number ranges from 57344 to 57999. If a port number is unavailable, an error is displayed.

- b) Set the session parameters.

**Example:**

```
Router(config)#grpc {address-family | certificate-authentication | dscp | max-concurrent-streams
| max-request-per-user | max-request-total | max-streams |
max-streams-per-user | no-tls | tlsv1-disable | tls-cipher | tls-mutual | tls-trustpoint |
service-layer | vrf}
```

where:

- `address-family`: set the address family identifier type.
- `certificate-authentication`: enables certificate based authentication
- `dscp`: set QoS marking DSCP on transmitted gRPC.
- `max-request-per-user`: set the maximum concurrent requests per user.
- `max-request-total`: set the maximum concurrent requests in total.
- `max-streams`: set the maximum number of concurrent gRPC requests. The maximum subscription limit is 128 requests. The default is 32 requests.
- `max-streams-per-user`: set the maximum concurrent gRPC requests for each user. The maximum subscription limit is 128 requests. The default is 32 requests.
- `no-tls`: disable transport layer security (TLS). The TLS is enabled by default
- `tlsv1-disable`: disable TLS version 1.0
- `service-layer`: enable the grpc service layer configuration.  
This parameter is not supported in Cisco ASR 9000 Series Routers, Cisco NCS560 Series Routers, , and Cisco NCS540 Series Routers.
- `tls-cipher`: enable the gRPC TLS cipher suites.
- `tls-mutual`: set the mutual authentication.
- `tls-trustpoint`: configure trustpoint.
- `server-vrf`: enable server vrf.

After gRPC is enabled, use the YANG data models to manage network configurations.

**Step 2** Configure the interfaces.

In this example, you configure interfaces using Cisco IOS XR native model `Cisco-IOS-XR-ifmgr-cfg.yang`. You gain an understanding about the various gRPC operations while you configure the interface. For the complete list of operations, see [gRPC Operations, on page 4](#). In this example, you merge configurations with `merge-config` RPC, retrieve operational statistics using `get-oper` RPC, and delete a configuration using `delete-config` RPC. You can explore the structure of the data model using YANG validator tools such as [pyang](#).

LER1 is the gRPC server, and a command line utility `grpcoc` is used as a client on the controller. This utility does not support YANG and, therefore, does not validate the data model. The server, LER1, validates the data mode.

**Note** The OC interface maps all IP configurations for parent interface under a VLAN with index 0. Hence, do not configure a sub interface with tag 0.

- a) Explore the XR configuration model for interfaces and its IPv4 augmentation.

**Example:**

```
controller:grpc$ pyang --format tree --tree-depth 3 Cisco-IOS-XR-ifmgr-cfg.yang
Cisco-IOS-XR-ipv4-io-cfg.yang
module: Cisco-IOS-XR-ifmgr-cfg
  +--rw global-interface-configuration
  | +--rw link-status? Link-status-enum
  +--rw interface-configurations
    +--rw interface-configuration* [active interface-name]
      +--rw dampening
      | ...
      +--rw mtus
      | ...
      +--rw encapsulation
      | ...
      +--rw shutdown? empty
      +--rw interface-virtual? empty
      +--rw secondary-admin-state? Secondary-admin-state-enum
      +--rw interface-mode-non-physical? Interface-mode-enum
      +--rw bandwidth? uint32
      +--rw link-status? empty
      +--rw description? string
      +--rw active Interface-active
      +--rw interface-name xr:Interface-name
      +--rw ipv4-io-cfg:ipv4-network
      | ...
      +--rw ipv4-io-cfg:ipv4-network-forwarding ...
```

- b) Configure a loopback0 interface on LER1.

**Example:**

```
controller:grpc$ more xr-interfaces-lo0-cfg.json
{
  "Cisco-IOS-XR-ifmgr-cfg:interface-configurations": [
    { "interface-configuration": [
      {
        "active": "act",
        "interface-name": "Loopback0",
        "description": "LOCAL TERMINATION ADDRESS",
        "interface-virtual": [
          null
        ],
        "Cisco-IOS-XR-ipv4-io-cfg:ipv4-network": {
          "addresses": {
            "primary": {
              "address": "172.16.255.1",
              "netmask": "255.255.255.255"
            }
          }
        }
      }
    ]
  }
}
```

- c) Merge the configuration.

**Example:**

```

controller:grpc$ grpc -username admin -password admin -oper merge-config
-server_addr 198.18.1.11:57400 -json_in_file xr-interfaces-gi0-cfg.json
emsMergeConfig: Sending ReqId 1
emsMergeConfig: Received ReqId 1, Response '
'

```

- d) Configure the ethernet interface on LER1.

**Example:**

```

controller:grpc$ more xr-interfaces-gi0-cfg.json
{
  "Cisco-IOS-XR-ifmgr-cfg:interface-configurations": {
    "interface-configuration": [
      {
        "active": "act",
        "interface-name": "GigabitEthernet0/0/0/0",
        "description": "CONNECTS TO LSR1 (g0/0/0/0)",
        "Cisco-IOS-XR-ipv4-io-cfg:ipv4-network": {
          "addresses": {
            "primary": {
              "address": "172.16.1.0",
              "netmask": "255.255.255.254"
            }
          }
        }
      }
    ]
  }
}

```

- e) Merge the configuration.

**Example:**

```

controller:grpc$ grpc -username admin -password admin -oper merge-config
-server_addr 198.18.1.11:57400 -json_in_file xr-interfaces-gi0-cfg.json
emsMergeConfig: Sending ReqId 1
emsMergeConfig: Received ReqId 1, Response '
'

```

- f) Enable the ethernet interface GigabitEthernet 0/0/0/0 on LER1 to bring up the interface. To do this, delete shutdown configuration for the interface.

**Example:**

```

controller:grpc$ grpc -username admin -password admin -oper delete-config
-server_addr 198.18.1.11:57400 -yang_path "$(< xr-interfaces-gi0-shutdown-cfg.json )"
emsDeleteConfig: Sending ReqId 1, yangJson {
  "Cisco-IOS-XR-ifmgr-cfg:interface-configurations": {
    "interface-configuration": [
      {
        "active": "act",
        "interface-name": "GigabitEthernet0/0/0/0",
        "shutdown": [
          null
        ]
      }
    ]
  }
}
emsDeleteConfig: Received ReqId 1, Response ''

```

**Step 3** Verify that the loopback interface and the ethernet interface on router LER1 are operational.

**Example:**

```

controller:grpc$ grpc -username admin -password admin -oper get-oper
-server_addr 198.18.1.11:57400 -oper_yang_path "$(< xr-interfaces-briefs-oper-filter.json )"
emsGetOper: Sending ReqId 1, yangPath {
  "Cisco-IOS-XR-pfi-im-cmd-oper:interfaces": {
    "interface-briefs": [
      null
    ]
  }
}
{ "Cisco-IOS-XR-pfi-im-cmd-oper:interfaces": {
  "interface-briefs": {
    "interface-brief": [
      {
        "interface-name": "GigabitEthernet0/0/0/0",
        "interface": "GigabitEthernet0/0/0/0",
        "type": "IFT_ETHERNET",
        "state": "im-state-up",
        "actual-state": "im-state-up",
        "line-state": "im-state-up",
        "actual-line-state": "im-state-up",
        "encapsulation": "ether",
        "encapsulation-type-string": "ARPA",
        "mtu": 1514,
        "sub-interface-mtu-overhead": 0,
        "l2-transport": false,
        "bandwidth": 1000000
      },
      {
        "interface-name": "GigabitEthernet0/0/0/1",
        "interface": "GigabitEthernet0/0/0/1",
        "type": "IFT_ETHERNET",
        "state": "im-state-up",
        "actual-state": "im-state-up",
        "line-state": "im-state-up",
        "actual-line-state": "im-state-up",
        "encapsulation": "ether",
        "encapsulation-type-string": "ARPA",
        "mtu": 1514,
        "sub-interface-mtu-overhead": 0,
        "l2-transport": false,
        "bandwidth": 1000000
      },
      {
        "interface-name": "Loopback0",
        "interface": "Loopback0",
        "type": "IFT_LOOPBACK",
        "state": "im-state-up",
        "actual-state": "im-state-up",
        "line-state": "im-state-up",
        "actual-line-state": "im-state-up",
        "encapsulation": "loopback",
        "encapsulation-type-string": "Loopback",
        "mtu": 1500,
        "sub-interface-mtu-overhead": 0,
        "l2-transport": false,
        "bandwidth": 0
      },
      {
        "interface-name": "MgmtEth0/RP0/CPU0/0",
        "interface": "MgmtEth0/RP0/CPU0/0",

```

```

    "type": "IFT_ETHERNET",
    "state": "im-state-up",
    "actual-state": "im-state-up",
    "line-state": "im-state-up",
    "actual-line-state": "im-state-up",
    "encapsulation": "ether",
    "encapsulation-type-string": "ARPA",
    "mtu": 1514,
    "sub-interface-mtu-overhead": 0,
    "l2-transport": false,
    "bandwidth": 1000000
  },
  {
    "interface-name": "Null0",
    "interface": "Null0",
    "type": "IFT_NULL",
    "state": "im-state-up",
    "actual-state": "im-state-up",
    "line-state": "im-state-up",
    "actual-line-state": "im-state-up",
    "encapsulation": "null",
    "encapsulation-type-string": "Null",
    "mtu": 1500,
    "sub-interface-mtu-overhead": 0,
    "l2-transport": false,
    "bandwidth": 0
  }
]
}
}
}
}
emsGetOper: ReqId 1, byteRecv: 2325

```

In summary, router LER1, which had minimal configuration, is now programmatically configured using data models with an ethernet interface and is assigned a loopback address. Both these interfaces are operational and ready for network provisioning operations.

