Use Service Layer API to Bring your Controller on Cisco IOS XR Router

Bring your protocol or controller on IOS XR router to interact with the network infrastructure layer components using Service Layer API.

For example, you can bring your controller to gain control over the Routing Information Base (RIB) tables and many more use cases.

Get to Know Service Layer API

Service Layer API is a model-driven API over Google-defined remote procedure call (gRPC).

gRPC enables you to bring your applications, routing protocols, controllers in a rich set of languages including C++, Python, GO, and many more.

Service Layer API is available out of the box and no extra packages required.

In IOS XR, routing protocols use RIB, the MPLS label manager, BFD, and other modules, to program the forwarding plane. You can expose these protocols through the service layer API.

Benefits

The Service Layer API gives direct access to the Network Infrastructure Layer (Service-Adaptation Layer). Therefore, you have the following advantages:

- **High Performance**: Direct access to the Network Infrastructure Layer, without going through a Network state database, results in higher performance than equivalent Management APIs.

  For example, Batch updates straight to the Label Switching Data Base (LSDB), the Routing Information Base (RIB) (over gRPC). The LSDB stores label-to-address mappings for efficient traffic routing in Label-switching routers. And, RIB contains the active and potential routes to various network destinations.

- **Flexibility**: The Service Layer API gives you the flexibility to bring your Protocol or Controller over gRPC.

- **Offload low-level tasks to IOS XR**: IOS XR infrastructure layer handles the following. Hence, you can focus on higher-layer protocols and controller logic:
  - Conflict resolution
  - Transactional notifications
  - Data plane abstraction

Components of Service Layer API

The following are the components of the Service Layer API architecture:

- **Functionality Verticals/Domains**: The verticals define the broader capability categories supported by the API. The following are the supported verticals. Each vertical supports data structure and RPCs defined in gpb
  - **Initialization**: Handles global initialization, sets up an event notification channel using GRPC streaming capabilities.

    The initialization RPCs are mandatory. Use the initialization RPCs to connect a client to the gRPC server on the router. Also, to send heartbeats and termination requests from the server to the client.
  - **IPv4, IPv6 Route (RIB)**: Handles route manipulations (add, update, delete) for a certain VRF.
  - **MPLS**: Handles allocation of label blocks and any incoming MPLS label mapping to a forwarding function.
  - **Interface**: Handles subscription of the registered clients to the interface state event notifications.
  - **IPv4, IPv6 BFD**: Manages BFD sessions, and corresponding BFD session state notifications.
- **Protobuf Schema/Model**: Use gRPC to model the service layer API.
- **gRPC**: gRPC utilizes GPB protobuf IDL by default to convert the models into bindings in various languages (c++, python, golang, and more). The gRPC server (running on the router) and the gRPC client use the generated bindings to serialize data and encode or decode the request or response between the server and the client.
- **Service Layer gRPC clients**: Based on the business needs, the gRPC clients for service layer can exist in one of the following ways:
  - On-box (agents runnning on their own sand-boxed third-party containers)
  - Off-box (within Controllers or other open-source tools)
- **gRPC Authentication Modes:**

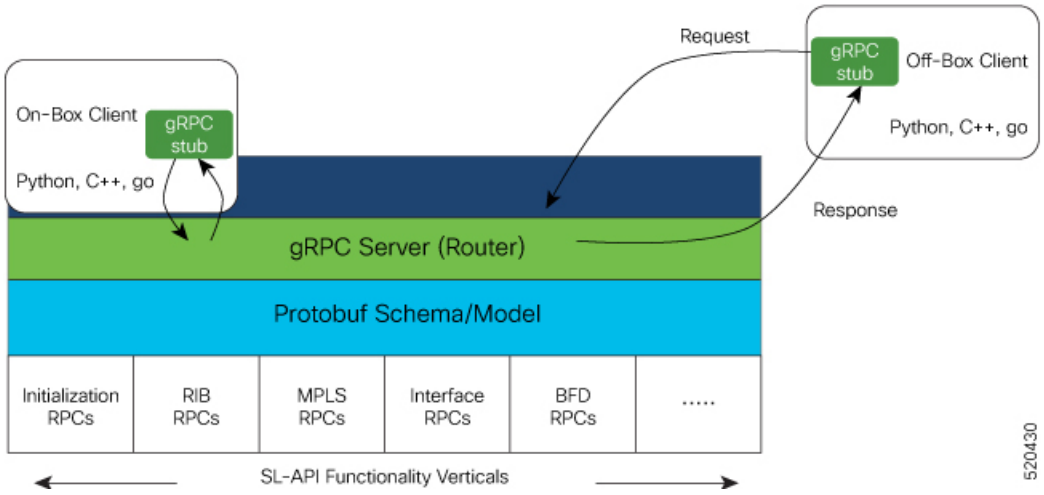
  gRPC supports the following authentication modes to secure communication between clients and servers. These authentication modes help ensure that only authorized entities can access the gRPC services, like gNOI, gRIBI, and P4RT. Upon receiving a gRPC request, the device will authenticate the user and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

  The following table lists the authentication type and configuration requirements:

Table 1: Types of Authentication with Configuration

Type	Authentication Method	Authorization Method	Configuration Requirement	Requirement From Client
Metadata with TLS	username, password	username	**grpc**	username, password, and CA
Metadata without TLS	username, password	username	**grpc no-tls**	username, password
Metadata with Mutual TLS	username, password	username	**grpc tls-mutual**	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	**grpc tls-mutual** and **grpc certificate authentication**	client certificate, client key, and CA

Figure 1: Components of Service Layer API



Bring your controller

To bring your controller on IOS XR, first, enable the service layer on the router and then write your Service Layer Client API.

1. Enable Service Layer, on page 4
2. Write Your Service Layer Client API

Enable Service Layer

Step 1 Enable the Service Layer.

Example:

```
Router#configure
Router(config)#grpc
Router(config-grpc)#port 57777
Router(config-grpc)#service-layer
Router(config-grpc)#no-tls
Router(config-grpc)#commit
```

The default port value for gNMI service port is 9339. You can set gNMI service port value from 57344 to 57999. Whereas, the default port value for gRIBI service port is default 9340. You can set gRIBI service port value from 57344 to 57999.

Step 2 Verify if the Service Layer is operational:

Example:

```
Router#show running-config grpc
Mon Nov  4 04:19:14.044 UTC
grpc
 port 57777
 no-tls
 service-layer
 !
!
```

Step 3 Verify the gRPC state.

Example:

```
Router#show service-layer state
Mon Feb 24 04:18:40.055 UTC
------------service layer state----------
config on:                    YES
standby connected :           NO
idt done:                     NO
blocked on ndt:               NO
connected to RIB for IPv4:    YES
connected to RIB for IPv6:    YES
Initialization state:         estab sync
pending requests:             0
BFD Connection:               UP
MPLS Connection:              UP
Interface Connection:         UP
Objects accepted:             NO
interface registered:         NO
bfd registered for IPv4:      NO
bfd registered for IPv6:      NO
```

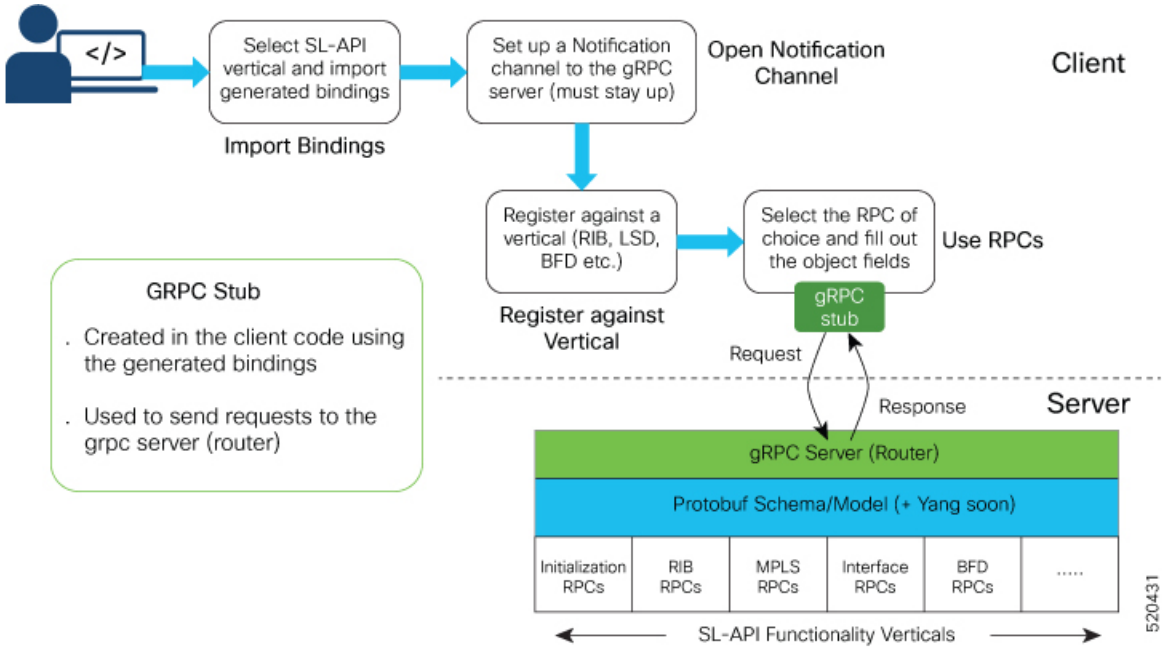
Write Your Service Layer Client API

You can write a Service Layer API based on your business needs. Follow these steps to write a Service Layer API client for a particular functionality vertical.

- **Import Bindings**: After generating the bindings, import the binding in your code.
- **Open Notification Channel:** Utilize the initialization functionality vertical to create a notification channel to register the client to the gRPC server running on the router.
- **Register against Vertical**: Register for a functionality vertical to utilize an RPC using the registration RPC before making calls. The system rejects any calls without prior registration.
- **Use RPCs**: Once registered against a vertical, select the RPC of your choice. Then complete the object fields in the gRPC stub.

To know more about creating a Service Layer API, see. Cisco IOS-XR Service Layer.

Figure 2: Service Layer API Workflow



Note Removing VRF or interface configurations referenced by SL-API objects is not supported and can impact traffic. Ensure Service Layer API clients reroute traffic and update routing before making such changes.

To know more about using gRPC protocol, see Use gRPC Protocol to Define Network Operations with Data Models Chapter in Programmability Configuration Guide.

Preprogram Backup LSPs Using Service Layer API

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Preprogram Backup LSPs Using Service Layer API	Release 24.2.11	This feature extends the Service Layer API, allowing the controller to preprogram backup Label Switched Paths (LSPs) in the hardware. When the *Path Priority* flag indicates a transition from the backup LSP to the primary LSP, the controller switches the traffic to the backup LSP.

With this feature, the primary LSP failure is detected through a controller-defined mechanism. Upon detecting a failure, the controller switches the primary LSP to backup in a down state and promotes the backup LSP to primary using the provided API parameters.

You can use the Service Layer API to preprogram LSPs as either primary or backup paths by using the *Path Priority* attribute. You can group LSPs with the *set-ID* attribute and determine their operational status as active or inactive using the *Path State* attribute. To ensure seamless traffic management, you can monitor the status of the LSPs using the controller. If traffic needs to be rerouted to the backup LSP, you can modify the priority of the preconfigured backup LSP to primary through the controller, thus allowing the backup path to take over the traffic load. The primary LSP then acts as the backup with its *Path State* set as down to retain the preprogram state. For more information about Service Layer API, see Github - Service Layer API and https://xrdocs.io/cisco-service-layer/.

Verify the Preprogramed Backup Paths

Use the **show service-layer mpls** command to verify the backup programming state for an LSP. For a given path, you can view path priority, and path set ID.

In the following command output, the Next-Hop Label Forwarding Entry 1 (**NHLFE 1**) is the primary LSP as the **path priority** is primary and the LSP state is up. **NHLFE 2** is the backup LSP as the **path priority** is backup and it belongs to the set ID 1. The status of the backup LSP is up.

```
Router#show service-layer mpls label 24000 exp default
Tue Jun 11 04:58:03.154 UTC
vrf name: mpls-default,  vrf state: eof,
vrf magic: valid,  purge timer: 600 seconds,  vrf flags: eof,

local label: 24000, update priority: high, magic: valid, flags: elsp, EXP: default,
    nhlfe: 1, magic: valid,
        ref count: 1, protected bitmap: 0x0, path id: 0, backup path id: 0,
        flags: path priority: primary, path setid: 0, path up
        path protection flags: 0, next hop: 10.10.10.2, load metric: 32,
        label action: 1,
        remote address:
        remote labels: 34000,
        interface name: Bundle-Ether1,

    nhlfe: 2, magic: valid,
```

```
    ref count: 1, protected bitmap: 0x0, path id: 0, backup path id: 0,
    flags: path priority: backup, path setid: 1, path up
    path protection flags: 0, next hop: 10.10.10.3, load metric: 1,
    label action: 1,
    remote address:
    remote labels: 44000,
    interface name: Bundle-Ether2,

nhlfe: 3, magic: valid,
    ref count: 1, protected bitmap: 0x0, path id: 0, backup path id: 0,
    flags: path priority: backup, path setid: 1, path up
    path protection flags: 0, next hop: 10.10.10.8, load metric: 31,
    label action: 1,
    remote address:
    remote labels: 44000,
    interface name: Bundle-Ether3
```

The following table describes the possible values for the path attributes:

Attribute	Possible Values
Path Priority	Primary or Backup
set-ID	0–3
Path State	Up or Down

TPM Enrollment and Attestation

Table 3: Feature History Table

Feature Name	Release Information	Description
TPM Enrollment and Attestation	Release 24.3.1	Introduced in this release on: Fixed Systems (8200, 8700); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) You can now use the new gNSI service for enrollment and attestation, EnrollZ and AttestZ, to enhance security of networking devices. The EnrollZ has been added to meet open-source requirements, thereby providing advantages such as the verification of device identity and integrity during boot-up, and the provisioning of owner-specific certificates. This bypasses the need for router vendor certificate authorities, offering a user-friendly and secure system. Sensitive credentials are only available to devices that have completed the EnrollZ and AttestZ processes.

Secure TPM Enrollment and Attestation Workflow for Network Devices

The EnrollZ and AttestZ gNSI services provide a secure method for verifying the identity and integrity of network devices. The EnrollZ service handles the TPM 2.0 enrollment workflow, involving cryptographic verification of the device's TPM-rooted identity and provisioning of attestation and Transport Layer Security (TLS) certificates by the device owner. This ensures that the device is under the control of the owner and not dependent on external vendor Certificate Authorities (CAs) during the attestation process. The AttestZ service manages the TPM 2.0 attestation workflow, confirming the device's integrity throughout the boot process by comparing observed Platform Configuration Register (PCR) values against expected ones to verify the device's boot state. This approach simplifies the TPM enrollment process for device owners, enhances control over certificate management, and eliminates external dependencies, while aligning with Trusted Computing Group (TCG) specifications.

Enroll a TPM 2.0 on Network Devices

The Trusted Platform Module (TPM) 2.0 enrollment workflow is a secure process for network devices to obtain the necessary credentials and configurations for TPM management. This workflow is initiated after the device boot process and involves interaction with various gRPC API endpoints.

Before you begin

- Device has completed the Bootz workflow.
- Device is equipped with a default SSL profile using the Secure Unique Device Identifier (SUDI) key pair and certificate.
- EnrollZ service is available and ready to enroll the TPM on the control card.
- Router owner has access to the trust bundle/anchor from the router vendor.

Step 1 Prepare Device for TPM Enrollment: Ensure the device has completed the Bootz workflow and is ready to serve TPM enrollment gRPC API endpoints on the required port.

Step 2 Trigger EnrollZ Service: Use the `GetIakCert` API to retrieve the Initial Attestation Key (IAK) and IDevID certificates.

Step 3 Verify and Validate Certificates:

- Verify the signature over the IAK certificate using the trust bundle/anchor from the router vendor.
- Confirm that the device identity fields in the IAK and IDevID certificates meet the expected criteria.

Step 4 Request and Install Owner Certificates:

- Request the router owner CA to issue the Owner IAK (oIAK) and Owner IDevID (oIDevID) certificates based on the public keys.
- Use the `RotateOIakCert` API to install the oIAK and oIDevID certificates on the control card.

Step 5 Verify and Store Certificates:

- Verify that the public keys in the oIAK and oIDevID certificates match with respective IAK and SUDI public key.
- Store the oIAK and oIDevID certificates in non-volatile memory for presentation during the TPM attestation (`attestz`) workflow.

Step 6 Update SSL Profile: Update the SSL profile to use the trust bundle and rotate the certificates to the Owner IDevID certificate.

Step 7 Enroll Secondary Control Card: Repeat the enrollment workflow for the secondary control card, if present.

TPM 2.0 Attestation

The TPM 2.0 attestation workflow ensures the integrity and identity of network devices by verifying their configurations and credentials. This process involves interaction with gRPC TPM 2.0 attestation endpoints and requires the device to be booted with the correct OS image and configurations.

Before you begin

- Device must be booted with the correct OS image.
- Correct configurations and credentials must be applied.
- Primary/active control card is responsible for all RPCs directed to the secondary/standby control card.

Step 1 Serve gRPC TPM 2.0 Attestation Endpoints: Ensure the device serves gRPC TPM 2.0 attestation endpoints on port 9339, the same port as gNOI/gNSI/gNMI.

The device must be booted with the correct OS image and configurations.

Step 2 Authenticate Standby Control Card: Perform an authentication handshake between the active and standby control cards using the IDevID key pair/cert.

The active control card is responsible for this handshake as the router owner cannot directly TLS authenticate the standby card.

Step 3 Secure Initial Attestation RPCs: Use the active control card's IDevID private key and oIDevID cert to secure TLS for the initial attestation RPCs.

Step 4 Call AttestZ Service: AttestZ service calls the device's Attest endpoint for a given control card (and a random nonce) to get back:

- An oIAK cert signed by the router owner's CA.
- Final observed PCR hashes/values.
- PCR Quote structure and signature over it signed by IAK private key.
- (Optional) oIDevID cert of the standby control card.

Step 5 Verify Certificates and Signatures:

- AttestZ service uses the trust bundle/anchor from the router owner CA to verify the oIAK cert and its validity/revocation status.
- Ensure that the control card serial number in the oIAK cert and oIDevID cert is the same.

Step 6 Compare PCR Values: The AttestZ service compares the PCR values against the known PCR values provided by the OEM vendor specific to a release.

Step 7 Compare PCR Values and Record Attestation Status: AttestZ service fetches expected final PCR values from its database and compares them to the observed ones reported by the device.

AttestZ service records a successful attestation status for the given control card and repeats the workflow for the secondary/standby control card if one is available.