



gNMI Protocol

This feature describes the model-driven configuration and retrieval of operational data using the gRPC Network Management Interface (gNMI) CAPABILITIES, Get and Set remote procedure calls (RPCs). gNMI version 0.4.0 is supported.

- [Restrictions for the gNMI Protocol, on page 1](#)
- [Information About the gNMI Protocol, on page 2](#)
- [How to Enable the gNMI Protocol, on page 15](#)
- [Configuration Examples for the gNMI Protocol, on page 20](#)
- [Additional References for the gNMI Protocol, on page 21](#)
- [Feature Information for the gNMI Protocol, on page 21](#)

Restrictions for the gNMI Protocol

The following restrictions apply to the feature:

- Subscribe RPC services are not supported.
- JSON, BYTES, PROTO, and ASCII encoding options are not supported.
JSON IETF keys must contain a YANG-prefix where the namespace of the following elements differs from the parent. This means that the routed-vlan derived from augmentation in openconfig-vlan.yang must be entered as *oc-vlan:routed-vlan* because it is different from the namespace of the parent nodes (parent nodes have the prefix, oc-if)
- GetRequest:
 - Operational data filtering is not supported.
 - Use models are not supported. These are a set of model data messages indicating the schema definition modules that define the data elements that must be returned in response to a Get RPC call.
- GetResponse:
 - Alias is not supported. It is a string that provides an alias for a prefix specified within the notification message.
 - Delete is not supported. It is a set of paths that are to be removed from a data tree.

Information About the gNMI Protocol

About GNMI

gNMI is gRPC Network Management Interface developed by Google. gNMI provides the mechanism to install, manipulate, and delete the configuration of network devices, and also to view operational data. The content provided through gNMI can be modeled using YANG.

gRPC is a remote procedure call developed by Google for low-latency, scalable distributions with mobile clients communicating to a cloud server. gRPC carries gNMI, and provides the means to formulate and transmit data and operation requests.

When a gNMI service failure occurs, the gNMI broker (GNMIB) will indicate an operational change of state from up to down, and all RPCs will return a service unavailable message until the database is up and running. Upon recovery, the GNMIB will indicate a change of operation state from down to up, and resume normal handling of RPCs.

JSON IETF Encoding for YANG Data Trees

RFC 7951 defines JavaScript Object Notation (JSON) encoding for YANG data trees and their subtrees. gNMI uses JSON for encoding data in its content layer.

The JSON type indicates that the value is encoded as a JSON string. JSON_IETF-encoded data must conform to the rules for JSON serialisation described in RFC 7951. Both the client and target must support JSON encoding.

Instances of YANG data nodes (leafs, containers, leaf-lists, lists, anydata nodes, and anyxml nodes) are encoded as members of a JSON object or name/value pairs. Encoding rules are identical for all types of data trees, such as configuration data, state data, parameters of RPC operations, actions, and notifications.

Every data node instance is encoded as a name/value pair where the name is formed from the data node identifier. The value depends on the category of the data node.

The "leaf" Data Node

A leaf node has a value, but no children, in a data tree. A leaf instance is encoded as a name/value pair. This value can be a string, number, literal "true" or "false", or the special array "[null]", depending on the type of the leaf. In the case that the data item at the specified path is a leaf node (which means it has no children, and an associated value) the value of that leaf is encoded directly. (A bare JSON value is included; it does not require a JSON object.)

The following example shows a leaf node definition:

```
leaf foo {  
  type uint8;  
}
```

The following is a valid JSON-encoded instance:

```
"foo": 123
```

gNMI GET Request

The gNMI Get RPC specifies how to retrieve one or more of the configuration attributes, state attributes, derived state attributes, or all attributes associated with a supported mode from a data tree. A GetRequest is sent from a client to the target to retrieve values from the data tree. A GetResponse is sent in response to a GetRequest.

Table 1: GetRequest JSON Structure

GetRequest	GetResponse
<p>The following is a path for the openconfig-interfaces model</p> <pre>+++++++ Sending get request: ++++++++ path { elem { name: "interfaces" } elem { name: "interface" key { key: "name" value: "Loopback111" } } }</pre>	

The total set of deletes, replace, and updates contained in any one SetRequest is treated as a single transaction. If any subordinate element of the transaction fails; the entire transaction will be disallowed and rolled back. A SetResponse is sent back for a SetRequest.

Table 3: Example of a SetRequest JSON Structure

SetRequest	SetResponse
<pre> +++++++ Sending set request: ++++++ update { path { elem { name: "interfaces" } elem { name: "interface" key { key: "name" value: "Loopback111" } } elem { name: "config" } } val { json_ietf_val: "{\"openconfig-interfaces:enabled\": \"false\"}" } } </pre>	<pre> +++++++ Received set response: ++++++ response { path { elem { name: "interfaces" } elem { name: "interface" key { key: "name" value: "Loopback111" } } elem { name: "config" } } op: UPDATE } timestamp: 1521699342123890045 </pre>

Table 4: Example of a SetRequest on Leaf Value

SetRequest	SetResponse
<pre> +++++++ Sending set request: ++++++ update { path { elem { name: "interfaces" } elem { name: "interface" key { key: "name" value: "Loopback111" } } elem { name: "config" } elem { name: "description" } } val { json_ietf_val: "\"UPDATE DESCRIPTION\"" } } </pre>	<pre> +++++++ Received set response: ++++++ response { path { elem { name: "interfaces" } elem { name: "interface" key { key: "name" value: "Loopback111" } } elem { name: "config" } elem { name: "description" } } op: UPDATE } timestamp: 1521699342123890045 </pre>

gNMI Namespace

A namespace specifies the path prefixing to be used in the *origin* field of a message.

This section describes the namespaces used in Cisco IOS XE Gibraltar 16.10.1 and later releases:

- RFC 7951-specified namespaces: Path prefixes use the YANG module name as defined in RFC 7951.

The RFC 7951-specified value prefixing uses the YANG module name.

Value prefixing is not affected by the selected path prefix namespace. The following example shows an RFC 7951-specified value prefix:

```
val {
  json_ietf_val:"{
    \"openconfig-interfaces:config\": {
      \"openconfig-interfaces:description\":
        \"DESCRIPTION\"
    }
  }"
```

An RFC 7951-specified namespace prefixing also uses the YANG module name. For example, the openconfig path to a loopback interface will be

```
/openconfig-interfaces:interfaces/interface[name=Loopback111]/
```

The following example shows a gNMI path with RFC7951 namespacing:

```
path {
  origin: "rfc7951"
  elem {
    name: "openconfig-interface:interfaces"
  }
  elem {
    name: "interface"
    key {
      key: "name"
      value: "Loopback111"
    }
  }
}
```

- Openconfig: No path prefixes are used. These can only be used with a path to an openconfig model.

The behavior of the Openconfig namespace prefixing is the same when no origin or namespace is provided. For example, the openconfig path to a loopback interface will be

```
/interfaces/interface[name=Loopback111]/
```

The following example shows a gNMI path with an Openconfig namespacing:

```
path {
  origin: "openconfig"
  elem {
    name: "interfaces"
  }
  elem {
    name: "interface"
    key {
      key: "name"
      value: "Loopback111"
    }
  }
}
```

```

    }
  }

```

- Blank: Same as the openconfig prefix. This is the default.

The following example shows a gNMI path with a blank Openconfig namespacing:

```

path {
  elem {
    name: "interfaces"
  }
  elem {
    name: "interface"
    key {
      key: "name"
      value: "Loopback111"
    }
  }
}

```

This section describes the path prefixing used in releases prior to Cisco IOS XE Gibraltar 16.10.1.

Here, path prefixing uses the YANG module prefix as defined in the YANG module definition. For example, the openconfig path to a loopback interface will be

```
/oc-if:interfaces/interface[name=Loopback111]/
```

The following example shows a gNMI Path with with legacy namespacing:

```

path {
  origin: "legacy"
  elem {
    name: "oc-if:interfaces"
  }
  elem {
    name: "interface"
    key {
      key: "name"
      value: "Loopback111"
    }
  }
}

```

gNMI Wildcards

The gNMI protocol supports wildcards for Get paths. This is the ability to use a wildcards in a path to match multiple elements. These wildcards indicate all elements in a given subtree in the schema.

An *elem* is an element, and it is a value between / characters in an xpath. An *elem* is also available in a gNMI path. For example, the position of a wildcard relative to *elem* names implies that the wildcard stands for an interface, and is interpreted as all interfaces.

There are two types of wildcards; implicit and explicit, and both are supported. Get paths support all types and combinations of path wildcards.

- Implicit wildcards: These expand a list of elements in an element tree. Implicit wildcard occurs when a key value is not provided for elements of a list.

The following is a sample path implicit wildcard. This wildcard will return the descriptions of all interfaces on a device:

```

path {
  elem {
    name: "interfaces"
  }
  elem {
    name: "interface"
  }
  elem {
    name: "config"
  }
  elem {
    name: "description"
  }
}

```

- Explicit wildcards: Provides the same functionality by
 - Specifying an asterisk (*) for either the path element name or key name.

The following is example shows a path asterisk wildcard as the key name. This wildcard returns the description for all interfaces on a device.

```

path {
  elem {
    name: "interfaces"
  }
  elem {
    name: "interface"
    key {
      key: "name"
      value: "*"
    }
  }
  elem {
    name: "config"
  }
  elem {
    name: "description"
  }
}

```

The following example shows a path asterisk wildcard as the path name. This wildcard will return the description for all elements that are available in the Loopback111 interface.

```

path {
  elem {
    name: "interfaces"
  }
  elem {
    name: "interface"
    key {
      key: "name"
      value: "Loopback111"
    }
  }
  elem {
    name: "*"
  }
  elem {
    name: "description"
  }
}

```

- Specifying an ellipsis (...) or a blank entry as element names. These wildcards can expand to multiple elements in a path.

The following example shows a path ellipsis wildcard. This wildcard will return all description fields available under /interfaces.

```
path {
  elem {
    name: "interfaces"
  }
  elem {
    name: "..."
  }
  elem {
    name: "description"
  }
}
```

The following is a sample GetRequest with an implicit wildcard. This GetRequest will return the oper-status of all interfaces on a device.

```
path {
  elem {
    name: "interfaces"
  }
  elem {
    name: "interface"
  }
  elem {
    name: "state"
  }
  elem {
    name: "oper-status"
  }
},
type: 0,
encoding: 4
```

The following is a sample GetResponse with an implicit wildcard:

```
notification {
  timestamp: 1520627877608777450
  update {
    path {
      elem {
        name: "interfaces"
      }
      elem {
        name: "interface"
        key {
          key: "name"
          value: "\"FortyGigabitEthernet1/1/1\""
        }
      }
      elem {
        name: "state"
      }
    }
    elem {
      name: "oper-status"
    }
  }
}
```

```

    }
    val {
      json_ietf_val: "\"LOWER_LAYER_DOWN\""
    }
  },
<snip>
...
</snip>

update {
  path {
    elem {
      name: "interfaces"
    }
    elem {
      name: "interface"
      key {
        key: "name"
        value: "\"Vlan1\""
      }
    }
    elem {
      name: "state"
    }
    elem {
      name: "oper-status"
    }
  }
  val {
    json_ietf_val: "\"DOWN\""
  }
}
}

```

gNMI Error Messages

When errors occur, gNMI returns descriptive error messages. The following section displays some gNMI error messages.

The following sample error message is displayed when the path is invalid:

```

gNMI Error Response:
<_Rendezvous of RPC that terminated with (StatusCode.TERMINATED,
  An error occurred while parsing provided xpath: unknown tag:
  "someinvalidxpath" Additional information: badly formatted or nonexistent path)>

```

The following sample error message is displayed for an unimplemented error:

```

gNMI Error Response:
<_Rendezvous of RPC that terminated with (StatusCode.UNIMPLEMENTED,
  Requested encoding "ASCII" not supported)>

```

The following sample error message is displayed when the data element is empty:

```

gNMI Error Response:
<_Rendezvous of RPC that terminated with (StatusCode.NOT_FOUND,
  Empty set returned for path "/oc-if:interfaces/noinfohere")>

```

How to Enable the gNMI Protocol

Perform the following steps to enable the gNMI protocol:

1. Create a set of certs for the gNMI client and device signed by a Certificate Authority (CA).
 - a. Create Certs with OpenSSL on Linux.
 - b. Install Certs on a device.
 - c. Configure gNMI on the device.
 - d. Verify whether gNMI is enabled and running.
2. Connect the gNMI client using client and root certificates configured in previous steps.

Creating Certs with OpenSSL on Linux

Certs and trustpoint are only required for secure gNMI servers.

The following example shows how to create Certs with OpenSSL on a Linux machine:

```
# Setting up a CA
openssl genrsa -out rootCA.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=rootCA -x509 -new -nodes -key rootCA.key -sha256 -out
rootCA.pem

# Setting up device cert and key
openssl genrsa -out device.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=<hostnameFQDN> -new -key device.key -out device.csr
openssl x509 -req -in device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
device.crt -sha256
# Encrypt device key - needed for input to IOS
openssl rsa -des3 -in device.key -out device.des3.key -passout pass:<password - remember
this for later>

# Setting up client cert and key
openssl genrsa -out client.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=gnmi_client -new -key client.key -out client.csr
openssl x509 -req -in client.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
client.crt -sha256
```

Installing Certs on a Device

The following example show how to install certs on a device:

```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

# Receive:
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of rootCA.pem, followed by newline + 'quit' + newline:
```

```

-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.

# Send:
# Contents of device.des3.key, followed by newline + 'quit' + newline:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20
<snip>
-----END RSA PRIVATE KEY-----
quit

# Receive:
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of device.crt, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% PEM files import succeeded.
Device(config)#

# Send:
Device(config)# crypto pki trustpoint trustpoint1
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device#

```

Enabling gNMI in Insecure Mode



Note This task is applicable in Cisco IOS XE Fuji 16.8.1 through Amsterdam 17.2.x.

In a Day Zero setup, first enable the device in insecure mode, then disable it, and enable the secure mode. To stop gNMI in insecure mode, use the **no gnmi-yang server** command.



Note gNMI insecure and secure servers can run simultaneously.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gnmi-yang**

4. **gnmi-yang server**
5. **gnmi-yang port *port-number***
6. **end**
7. **show gnmi-yang state**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	gnmi-yang Example: Device(config)# gnmi-yang	Starts the gNMI process.
Step 4	gnmi-yang server Example: Device(config)# gnmi-yang server	Enables the gNMI server in insecure mode.
Step 5	gnmi-yang port <i>port-number</i> Example: (Optional) Device(config)# gnmi-yang port 50000	Sets the gNMI port to listen to. <ul style="list-style-type: none"> • The default insecure gNMI port is 9339.
Step 6	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	show gnmi-yang state Example: Device# show gnmi-yang state	Displays the status of gNMI servers.

Example

The following is sample output from the **show gnmi-yang state** command:

```
Device# show gnmi-yang state
State Status
-----
Enabled Up
```

Enabling gNMI in Secure Mode



Note This task is applicable in Cisco IOS XE Fuji 16.8.1 through Amsterdam 17.2.x.

To stop gNMI in secure mode, use the **no gnmi-yang secure-server** command.



Note gNMI insecure and secure servers can run simultaneously.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gnmi-yang**
4. **gnmi-yang secure-server**
5. **gnmi-yang secure-trustpoint** *trustpoint-name*
6. **gnmi-yang secure-client-auth**
7. **gnmi-yang secure-port**
8. **end**
9. **show gnmi-yang state**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	gnmi-yang Example: Device(config)# gnmi-yang	Starts the gNMI process.
Step 4	gnmi-yang secure-server Example: Device(config)# gnmi-yang secure-server	Enables the gNMI server in secure mode.
Step 5	gnmi-yang secure-trustpoint <i>trustpoint-name</i> Example: Device(config)# gnmi-yang secure-trustpoint trustpoint1	Specifies the trustpoint and cert set that gNMI uses for authentication.

	Command or Action	Purpose
Step 6	gnmi-yang secure-client-auth Example: Device(config)# gnmi-yang secure-client-auth	(Optional) The gNMI process authenticates the client certificate against the root certificate.
Step 7	gnmi-yang secure-port Example: Device(config)# gnmi-yang secure-port	(Optional) Sets the gNMI port to listen to. <ul style="list-style-type: none"> • The default insecure gNMI port is 9339.
Step 8	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	show gnmi-yang state Example: Device# show gnmi-yang state	Displays the status of gNMI servers.

Example

The following is sample output from the **show gnmi-yang state** command:

```
Device# show gnmi-yang state

State Status
-----
Enabled Up
```

Connecting the gNMI Client

The gNMI client is connected by using the client and root certificates that are previously configured.

The following example shows how to connect the gNMI client using Python:

```
# gRPC Must be compiled in local dir under path below:
>>> import sys
>>> sys.path.insert(0, "reference/rpc/gnmi/")
>>> import grpc
>>> import gnmi_pb2
>>> import gnmi_pb2_grpc
>>> gnmi_dir = '/path/to/where/openssl/creds/were/generated/'

# Certs must be read in as bytes
>>> with open(gnmi_dir + 'rootCA.pem', 'rb') as f:
>>>     ca_cert = f.read()
>>> with open(gnmi_dir + 'client.crt', 'rb') as f:
>>>     client_cert = f.read()
>>> with open(gnmi_dir + 'client.key', 'rb') as f:
>>>     client_key = f.read()

# Create credentials object
```

```
>>> credentials = grpc.ssl_channel_credentials(root_certificates=ca_cert,
private_key=client_key, certificate_chain=client_cert)

# Create a secure channel:
# Default port is 50052, can be changed on ios device with 'gnmi-yang secure-port ####'
>>> port = 50052
>>> host = <HOSTNAME FQDN>
>>> secure_channel = grpc.secure_channel("%s:%d" % (host, port), credentials)

# Create secure stub:
>>> secure_stub = gnmi_pb2_grpc.gNMISub(stub=secure_channel)

# Done! Let's test to make sure it works:
>>> secure_stub.Capabilities(gnmi_pb2.CapabilityRequest())
supported_models {
<snip>
}
supported_encodings: <snip>
gNMI_version: "0.4.0"
```

Configuration Examples for the gNMI Protocol

Example: Enabling the gNMI Protocol



Note This example is applicable in Cisco IOS XE Fuji 16.8.1 through Amsterdam 17.2.x.

Example: Enabling gNMI in Insecure Mode

The following example shows how to enable the gNMI server in insecure mode:

```
Device# configure terminal
Device(config)# gnmi-yang
Device(config)# gnmi-yang server
Device(config)# gnmi-yang port 50000 <The default port is 9339.>
Device(config)# end
Device#
```

Example: Enabling gNMI in Secure Mode

The following example shows how to enable the gNMI server in secure mode:

```
Device# configure terminal
Device(config)# gnmi-yang server
Device(config)# gnmi-yang secure-server
Device(config)# gnmi-yang secure-trustpoint trustpoint1
Device(config)# gnmi-yang secure-client-auth
Device(config)# gnmi-yang secure-port 50001 <The default port is 9339.>
Device(config)# end
Device#
```

Additional References for the gNMI Protocol

Related Documents

Related Topic	Document Title
DevNet	https://developer.cisco.com/site/ios-xe/
gNMI	https://github.com/openconfig/reference/blob/master/rpc/gnmi/gnmi-specification.md
gNMI path encoding	https://github.com/openconfig/reference/blob/master/rpc/gnmi/gnmi-path-conventions.md

Standards and RFCs

Standard/RFC	Title
RFC 7951	JSON Encoding of Data Modeled with YANG

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for the gNMI Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for the gNMI Protocol

Feature Name	Release	Feature Information
gNMI Protocol	Cisco IOS XE Fuji 16.8.1a	<p>This feature describes the model-driven configuration and retrieval of operational data using the gNMI capabilities, GET and SET RPCs.</p> <p>This feature was implemented on the following platforms:</p> <ul style="list-style-type: none">• Cisco Catalyst 9300 Series Switches• Cisco Catalyst 9400 Series Switches• Cisco Catalyst 9500 Series Switches
	Cisco IOS XE Gibraltar 16.10.1	<p>In Cisco IOS XE Gibraltar 16.10.1, this feature was implemented on Cisco Catalyst 9500-High Performance Series Switches.</p>