H3C S6850 & S9850 Switch Series

Telemetry Configuration Guide

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 6555 and later
Document version: 6W101-20200820

Preface

This configuration guide describes gRPC and INT features and configuration tasks.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.
- Documentation feedback.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the S6850 & S9850 switch series.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Configuring gRPC

About gRPC

gRPC is an open source remote procedure call (RPC) system initially developed at Google. It uses HTTP 2.0 for transport and provides network device configuration and management methods that support multiple programming languages.

gRPC protocol stack layers

Table 1 describes the gRPC protocol stack layers.

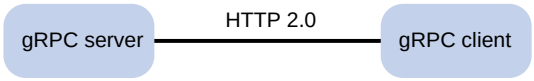
Table 1 gRPC protocol stack layers

Layer	Description
Content layer	Defines the data of the service module. Two peers must notify each other of the data models that they are using.
Protocol buffer encoding layer	Encodes data by using the protocol buffer code format.
gRPC layer	Defines the protocol interaction format for remote procedure calls.
HTTP 2.0 layer	Carries gRPC.
TCP layer	Provides connection-oriented reliable data links.

Network architecture

As shown in Figure 1, the gRPC network uses the client/server model. It uses HTTP 2.0 for packet transport.

Figure 1 gRPC network architecture



The gRPC network uses the following mechanism:

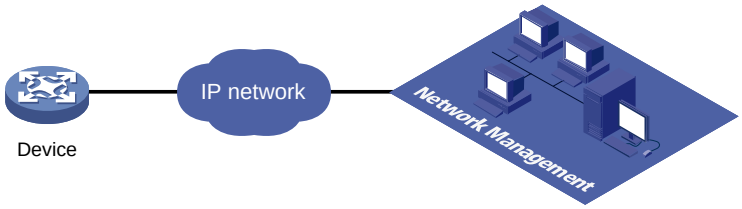
1. The gRPC server listens to connection requests from clients at the gRPC service port.
2. A user runs the gRPC client application to log in to the gRPC server, and uses methods provided in the .proto file to send requests.
3. The gRPC server responds to requests from the gRPC client.

The device can act as the gRPC server or client.

Telemetry technology based on gRPC

Telemetry is a remote data collection technology for monitoring device performance and operating status. H3C telemetry technology uses gRPC to push data from the device to the collectors on the NMSs. As shown in Figure 2, after a gRPC connection is established between the device and NMSs, the NMSs can subscribe to data of modules on the device.

Figure 2 Telemetry technology based on gRPC



Telemetry modes

The device supports the following telemetry modes:

- **Dial-in mode**—The device acts as a gRPC server and the collectors act as gRPC clients. A collector initiates a gRPC connection to the device to subscribe to device data.

  Dial-in mode applies to small networks where collectors need to deploy configurations to devices.

  Dial-in mode supports the following operations:

  - **Get**—Obtains device status and settings.
  - **Set**—Deploys settings to the device.
  - **CLI**—Executes commands on the device.
- **Dial-out mode**—The device acts as a gRPC client and the collectors act as gRPC servers. The device initiates a gRPC connection to the collectors and pushes subscribed device data to the collectors.

  Dial-out mode applies to larger networks where devices need to push device data to collectors.

Protocols

RFC 7540, *Hypertext Transfer Protocol version 2 (HTTP/2)*

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

gRPC is not supported in FIPS mode.

Configuring the gRPC dial-in mode

gRPC dial-in mode configuration tasks at a glance

To configure the gRPC dial-in mode, perform the following tasks:

1. Configuring the gRPC service
2. Configuring a gRPC user

Configuring the gRPC service

1. Enter system view.

system-view

2. (Optional.) Set the gRPC service port number.
   grpc port *port-number*
   By default, the gRPC service port number is 50051.
3. Enable the gRPC service.
   grpc enable
   By default, the gRPC service is disabled.
4. (Optional.) Set the gRPC session idle timeout timer.
   grpc idle-timeout *minutes*
   By default, the gRPC session idle timeout timer is 5 minutes.

Configuring a gRPC user

About gRPC users

For gRPC clients to establish gRPC sessions with the device, you must configure local users for the gRPC clients.

Procedure

1. Enter system view.
   system-view
2. Add a local user with the device management right.
   local-user *user-name* [**class manage**]
3. Configure a password for the user.
   password [{ **hash** | **simple** } *password*]
   By default, no password is configured for a local user. A non-password-protected user can pass authentication after providing the correct username and passing attribute checks.
4. Assign user role network-admin to the user.
   authorization-attribute user-role *user-role*
   By default, a local user is assigned the network-operator role.
5. Authorize the user to use the HTTPS service.
   service-type https
   By default, no service types are authorized to a local user.

For more information about the **local-user**, **password**, **authorization-attribute**, and **service-type** commands, see AAA configuration in *Security Command Reference*.

Configuring the gRPC dial-out mode

gRPC dial-out mode configuration tasks at a glance

To configure the gRPC dial-out mode, perform the following tasks:

1. Enabling the gRPC service
2. Configuring sensors
3. Configuring collectors
4. Configuring a subscription

Enabling the gRPC service

Restrictions and guidelines

If the gRPC service fails to be enabled, use the **display tcp** or **display ipv6 tcp** command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again. For more information about the **display tcp** and **display ipv6 tcp** commands, see *Layer 3—IP Services Command Reference*.

Procedure

1. Enter system view.
   system-view
2. Enable the gRPC service.
   grpc enable
   By default, the gRPC service is disabled.

Configuring sensors

About sensors

The device uses sensors to sample data. A sensor path indicates a data source.

Supported data sampling types include:

- **Event-triggered sampling**—Sensors in a sensor group sample data when certain events occur. For sensor paths of this data sampling type, see *NETCONF XML API Event Reference* for the module.
- **Periodic sampling**—Sensors in a sensor group sample data at intervals. For sensor paths of this data sampling type, see the NETCONF XML API references for the module except for *NETCONF XML API Event Reference*.

Procedure

1. Enter system view.
   system-view
2. Enter telemetry view.
   telemetry
3. Create a sensor group and enter sensor group view.
   sensor-group *group-name*
4. Specify a sensor path.
   sensor path *path*
   To specify multiple sensor paths, execute this command multiple times.

Configuring collectors

About collectors

Collectors are used to receive sampled data from network devices. For the device to communicate with collectors, you must create a destination group and add collectors to the destination group.

Restrictions and guidelines

As a best practice, configure a maximum of five destination groups. If you configure too many destination groups, system performance might degrade.

Procedure

1. Enter system view.

   system-view

2. Enter telemetry view.

   telemetry

3. Create a destination group and enter destination group view.

   destination-group *group-name*

4. Specify a collector.

   IPv4:

   ipv4-address *ipv4-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

   IPv6:

   ipv6-address *ipv6-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

   The IPv6 address cannot be a link-local address. For more information about link-local addresses, see IPv6 basics configuration in *Layer 3—IP Services Configuration Guide*.

   To specify multiple collectors, execute this command multiple times. One collector must have a different address, port, or VPN instance than the other collectors.

Configuring a subscription

About configuring a subscription

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

Procedure

1. Enter system view.

   system-view

2. Enter telemetry view.

   telemetry

3. Create a subscription and enter subscription view.

   subscription *subscription-name*

4. (Optional.) Specify the source IP address for packets sent to collectors.

   source-address { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

   By default, the device uses the primary IPv4 address of the output interface for the route to the collectors as the source address.

   Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.

5. Specify a sensor group.

   sensor-group *group-name* [**sample-interval** *interval*]

   Specify the **sample-interval** *interval* option for periodic sensor paths and only for periodic sensor paths.

   - If you specify the option for event-triggered sensor paths, the sensor paths do not take effect.
   - If you do not specify the option for periodic sensor paths, the device does not sample or push data.

6. Specify a destination group.
   destination-group *group-name*

Display and maintenance commands for gRPC

Execute **display** commands in any view.

Task	Command
Display gRPC dial-in mode information.	**display grpc**

gRPC configuration examples

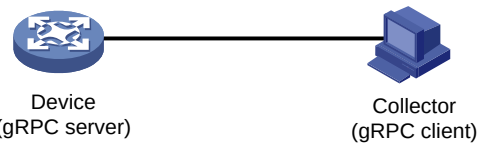
These configuration examples describe only CLI configuration tasks on the device. The collectors need to run an extra application. For information about collector-side application development, see "Developing the collector-side application."

Example: Configuring the gRPC dial-in mode

Network configuration

As shown in Figure 3, configure the gRPC dial-in mode on the device so the device acts as the gRPC server and the gRPC client can subscribe to LLDP events on the device.

Figure 3 Network diagram



Procedure

1. Assign IP addresses to interfaces on the gRPC server and client and configure routes. Make sure the server and client can reach each other.
2. Configure the device as the gRPC server:

   # Enable the gRPC service.

   ```
   <Device> system-view
   [Device] grpc enable
   ```

   # Create a local user named **test**. Set the password to **test**, and assign user role network-admin and the HTTPS service to the user.

   ```
   [Device] local-user test
   [Device-luser-manage-test] password simple test
   [Device-luser-manage-test] authorization-attribute user-role network-admin
   [Device-luser-manage-test] service-type https
   [Device-luser-manage-test] quit
   ```
3. Configure the gRPC client.
   a. Prepare a PC and install the gRPC environment on the PC. For more information, see the user guide for the gRPC environment.
   b. Obtain the H3C proto definition file and uses the protocol buffer compiler to generate code of a specific language, for example, Java, Python, C/C++, or Go.

c. Create a client application to call the generated code.
d. Start the application to log in to the gRPC server.

Verifying the configuration

When an LLDP event occurs on the gRPC server, verify that the gRPC client receives the event.

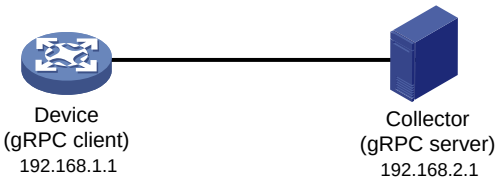
Example: Configuring the gRPC dial-out mode

Network configuration

As shown in Figure 4, the device is connected to a collector. The collector uses port 50050.

Configure gRPC dial-out mode on the device so the device pushes the device capability information of its interface module to the collector at 10-second intervals.

Figure 4 Network diagram



Procedure

Configure IP addresses as required so the device and the collector can reach each other. (Details not shown.)

Enable the gRPC service.

```
<Device> system-view
[Device] grpc enable
```

Create a sensor group named **test**, and add sensor path **ifmgr/devicecapabilities/**.

```
[Device] telemetry
[Device-telemetry] sensor-group test
[Device-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/
[Device-telemetry-sensor-group-test] quit
```

Create a destination group named **collector1**. Specify a collector that uses IPv4 address 192.168.2.1 and port number 50050.

```
[Device-telemetry] destination-group collector1
[Device-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Device-telemetry-destination-group-collector1] quit
```

Configure a subscription named **A** to bind sensor group **test** with destination group **collector1**. Set the sampling interval to 10 seconds.

```
[Device-telemetry] subscription A
[Device-telemetry-subscription-A] sensor-group test sample-interval 10
[Device-telemetry-subscription-A] destination-group collector1
[Device-telemetry-subscription-A] quit
```

Verifying the configuration

Verify that the collector receives the device capability information of the interface module from the device at 10-second intervals. (Details not shown.)

Protocol buffer code

Protocol buffer code format

Google Protocol Buffers provide a flexible mechanism for serializing structured data. Different from XML code and JSON code, the protocol buffer code is binary and provides higher performance.

Table 2 compares a protocol buffer code format example and the corresponding JSON code format example.

Table 2 Protocol buffer and JSON code format examples

Protocol buffer code format example	Corresponding JSON code format example

{
1:“H3C”
2:“H3C”
3:“H3C Simware”
4:“Syslog/LogBuffer”
5:"notification": {
"Syslog": {
"LogBuffer": {
"BufferSize": 512,
"BufferSizeLimit": 1024,
"DroppedLogsCount": 0,
"LogsCount": 100,
"LogsCountPerSeverity": {
"Alert": 0,
"Critical": 1,
"Debug": 0,
"Emergency": 0,
"Error": 3,
"Informational": 80,
"Notice": 15,
"Warning": 1
},
"OverwrittenLogsCount": 0,
"State": "enable"
}
},
"Timestamp": "1527206160022"
}
}
	{
	"producerName": "H3C",
	"deviceName": "H3C",
	"deviceModel": "H3C Simware",
	"sensorPath": "Syslog/LogBuffer",
	"jsonData": {
	"notification": {
	"Syslog": {
	"LogBuffer": {
	"BufferSize": 512,
	"BufferSizeLimit": 1024,
	"DroppedLogsCount": 0,
	"LogsCount": 100,
	"LogsCountPerSeverity": {
	"Alert": 0,
	"Critical": 1,
	"Debug": 0,
	"Emergency": 0,
	"Error": 3,
	"Informational": 80,
	"Notice": 15,
	"Warning": 1
	},
	"OverwrittenLogsCount": 0,
	"State": "enable"
	}
	},
	"Timestamp": "1527206160022"
	}
	}
	}

Proto definition files

You can define data structures in a proto definition file. Then, you can compile the file with utility protoc to generate code in a programing language such as Java and C++. Using the generated code, you can develop an application for a collector to communicate with the device.

H3C provides proto definition files for both dial-in mode and dial-out mode.

Proto definition files in dial-in mode

Public proto definition files

Dial-in mode supports the following public proto definition files:

- **grpc_service.proto**—Defines the public RPC methods in dial-in mode.
- **gnmi.proto**—Defines the public RPC methods for Set operations.
- **gnmi_ext.proto**—Defines the extended message structures required by file **gnmi.proto**.

Files **gnmi.proto** and **gnmi_ext.proto** are from Google. For information about the download paths, see "Obtaining proto definition files."

The **grpc_service.proto** file is provided by H3C. The following are the contents of the file:

```
syntax = "proto2";
package grpc_service;
message GetJsonReply {   // Reply to the Get method
    required string result = 1;
}
message SubscribeReply { // Subscription result
    required string result = 1;
}
message ConfigReply {    // Configuration result
    required string result = 1;
}
message ReportEvent {    // Subscribed event
    required string token_id = 1;    // Login token_id
    required string stream_name = 2; // Event stream name
    required string event_name = 3;  // Event name
    required string json_text = 4;   // Subscription result, a JSON string
}
message GetReportRequest{ // Obtains the event subscription result
    required string token_id = 1; // Returns the token_id upon a successful login
}
message LoginRequest {  // Login request parameters
    required string user_name = 1; // Username
    required string password = 2; // Password
}
message LoginReply {  // Reply to a login request
    required string token_id = 1; // Returns the token_id upon a successful login
}
message LogoutRequest { // Logout parameter
    required string token_id = 1; // token_id
}
```

```
message LogoutReply { // Reply to a logout request
    required string result = 1; // Logout result
}
message SubscribeRequest { // Event stream name
    required string stream_name = 1;
}
message CliConfigArgs { // Sends a configuration command and the parameters to the device
    required int64 ReqId = 1; // Command request ID
    required string cli = 2;  // Command string
}
message CliConfigReply { // Reply to a configuration command execution request
    required int64 ResReqId = 1; // Request ID, which corresponds to that in CliConfigArgs
  required string output = 2;    // Output from the command
    required string errors = 3;  // Command execution result
}
message DisplayCmdArgs { // Sends a display command and the parameters to the device
    required int64 ReqId = 1; // Command request ID
    required string cli = 2;  // Command string
}
message DisplayCmdReply { // Reply to a display command execution request
    required int64 ResReqId =1; // Request ID, which corresponds to that in DisplayCmdArgs
    required string output = 2;  // Output from the command
    required string errors = 3;  // Command execution result
}
service GrpcService {    // gRPC methods
    rpc Login (LoginRequest) returns (LoginReply) {}      // Login method
    rpc Logout (LogoutRequest) returns (LogoutReply) {}   // Logout method
    rpc SubscribeByStreamName (SubscribeRequest) returns (SubscribeReply) {} // Event
subscription method
    rpc GetEventReport (GetReportRequest) returns (stream ReportEvent) {} // Method for
obtaining the subscribed event
    rpc CliConfig (CliConfigArgs)  returns (stream CliConfigReply) {} // Method for
executing a configuration command and returning the execution result
    rpc DisplayCmdTextOutput(DisplayCmdArgs)  returns(stream DisplayCmdReply) {} //
Method for executing a display command and returning the execution result
}
```

Proto definition files for service modules

The dial-in mode supports proto definition files for the following service modules: Device, Ifmgr, IPFW, LLDP, and Syslog.

The following are the contents of the **Device.proto** file, which defines the RPC methods for the Device module:

```
syntax = "proto2";
import "grpc_service.proto";
package  device;
message DeviceBase { // Structure for obtaining basic device information
    optional string HostName = 1;    // Device name
    optional string HostOid = 2;     // sysoid
    optional uint32 MaxChassisNum = 3;    //Maximum number of chassis
```

```
    optional uint32 MaxSlotNum = 4;  // Maximum number of slots
    optional string HostDescription = 5; // Device description
}
message DevicePhysicalEntities { // Structure for obtaining physical entity information
of the device
    message Entity {
        optional uint32 PhysicalIndex = 1;    // Entity index
        optional string VendorType = 2;       // Vendor type
        optional uint32 EntityClass = 3;      // Entity class
        optional string SoftwareRev = 4;      // Software version
        optional string SerialNumber = 5;     // Serial number
        optional string Model = 6;            // Model
    }
    repeated Entity entity = 1;
}
service DeviceService { // RPC methods
    rpc GetJsonDeviceBase(DeviceBase) returns (grpc_service.GetJsonReply) {} // Method
for obtaining basic device information
    rpc GetJsonDevicePhysicalEntities(DevicePhysicalEntities) returns
(grpc_service.GetJsonReply) {}   // Method for obtaining physical entity information of
the device
}
```

Proto definition file in dial-out mode

The **grpc_dialout.proto** file defines the public RPC methods in dial-out mode. The following are the contents of the file:

```
syntax = "proto2";
package grpc_dialout;
message DeviceInfo{  // Pushed device information
    required string producerName = 1; // Vendor name
    required string deviceName = 2;   // Device name
    required string deviceModel = 3;  // Device model
}
message DialoutMsg{   // Format of the pushed data
    required DeviceInfo deviceMsg = 1; // Device information described by DeviceInfo
    required string sensorPath = 2; // Sensor path, which corresponds to xpath in NETCONF
    required string jsonData = 3;  // Sampled data, a JSON string
}
message DialoutResponse{  // Response from the collector. Reserved. The value is not
processed.
    required string response = 1;
}
service gRPCDialout {  // Data push method
    rpc Dialout(stream DialoutMsg) returns (DialoutResponse);
}
```

Obtaining proto definition files

To obtain files **gnmi.proto** and **gnmi_ext.proto**, download them from the following websites:

- https://github.com/openconfig/gnmi/tree/master/proto/gnmi/gnmi.proto
- https://github.com/openconfig/gnmi/tree/master/proto/gnmi_ext/gnmi_ext.proto

To obtain other proto definition files, contact H3C Technical Support.

Example: Developing a gRPC collector-side application

Use a language (for example, C++) to develop a gRPC collector-side application on Linux to achieve the following goals:

- Collect device data by using Get operations in dial-in mode or by using dial-out mode.
- Deploy settings to the device by using Set or CLI operations in dial-in mode.

Prerequisites

1. Obtain proto definition files.
   - For Get operations in dial-in mode, obtain the **grpc_service.proto** file and proto definition files for service modules.
   - For Set operations in dial-in mode, obtain files **grpc_service.proto**, **gnmi.proto**, and **gnmi_ext.proto**.
   - For CLI operations in dial-in mode, obtain the **grpc_service.proto** file.
   - For dial-out mode, obtain the **grpc_dialout.proto** file.
2. Obtain utility protoc from https://github.com/google/protobuf/releases.
3. Obtain the protobuf plug-in for C++ (**protobuf-cpp**) from https://github.com/google/protobuf/releases.

Generating the C++ code for the proto definition files

Dial-in mode

Copy the required proto definition files to the current directory, for example, **grpc_service.proto** and **BufferMonitor.proto**.

```
$protoc --plugin=./grpc_cpp_plugin  --grpc_out=. --cpp_out=. *.proto
```

Dial-out mode

Copy proto definition file **grpc_dialout.proto** to the current directory.

```
$ protoc --plugin=./grpc_cpp_plugin  --grpc_out=.  --cpp_out=. *.proto
```

Developing the collector-side application

Using Get operations in dial-in mode

In dial-in mode, the application needs to provide the code to be run on the gRPC client.

The C++ code generated from the proto definition files already encapsulates the service classes, which are GrpcService and BufferMonitorService in this example. For the gRPC client to initiate RPC requests, you only need to call the RPC method in the application.

The application performs the following operations:

- Log in to obtain the token_id.
- Prepare parameters for the RPC method, use the service classes generated from the proto definition files to call the RPC method, and resolve the returned result.
- Log out.

To develop the collector-side application in dial-in mode:

1. Create a GrpcServiceTest class.

In the class, use the GrpcService::Stub class generated from grpc_service.proto. Implement login and logout with the Login and Logout methods generated from grpc_service.proto.

```
class GrpcServiceTest
{
public:
    /* Constructor functions */
    GrpcServiceTest(std::shared_ptr<Channel> channel):
GrpcServiceStub(GrpcService::NewStub(channel))  {}

    /* Member functions */
    int Login(const std::string& username, const std::string& password);
    void Logout();
    void listen();
Status listen(const std::string& command);

    /* Member variable */
    std::string token;

private:
    std::unique_ptr<GrpcService::Stub> GrpcServiceStub;  // Use the
GrpcService::Stub class generated from grpc_service.proto.
};
```

2. Customize the Login method.

Call the Login method of the GrpcService::Stub class to allow a user who provides the correct the username and password to log in.

```
int GrpcServiceTest::Login(const std::string& username, const std::string& password)
{
    LoginRequest request;   // Username and password.
    request.set_user_name(username);
    request.set_password(password);

LoginReply reply;
ClientContext context;

    // Call the Login method.
    Status status = GrpcServiceStub->Login(&context, request, &reply);
    if (status.ok())
    {
        std::cout << "login ok!" << std::endl;
        std::cout <<"token id is :" << reply.token_id() << std::endl;
        token = reply.token_id();  // The login succeeds. The token is obtained.
```

```
        return 0;
    }
    else{
        std::cout << status.error_code() << ": " << status.error_message()
                  << ". Login failed!" << std::endl;
        return -1;
    }
}
```

3. Initiate an RPC request to the device. In this example, the application subscribes to interface packet drop events.

```
rpc SubscribePortQueDropEvent(PortQueDropEvent) returns
(grpc_service.SubscribeReply) {}
```

4. Create the BufMon_GrpcClient class to encapsulate the RPC method.

Use the BufferMonitorService::Stub class generated from BufferMonitor.proto to call the RPC method.

```
class BufMon_GrpcClient
{
public:
    BufMon_GrpcClient(std::shared_ptr<Channel> channel):
mStub(BufferMonitorService::NewStub(channel))
    {}

    std::string BufMon_Sub_AllEvent(std::string token);
    std::string BufMon_Sub_BoardEvent(std::string token);
    std::string BufMon_Sub_PortOverrunEvent(std::string token);
    std::string BufMon_Sub_PortDropEvent(std::string token);

    /* Get entries */
    std::string BufMon_Sub_GetStatistics(std::string token);
    std::string BufMon_Sub_GetGlobalCfg(std::string token);
    std::string BufMon_Sub_GetBoardCfg(std::string token);
    std::string BufMon_Sub_GetNodeQueCfg(std::string token);
    std::string BufMon_Sub_GetPortQueCfg(std::string token);

private:
   std::unique_ptr<BufferMonitorService::Stub> mStub; // Use the class generated
from BufferMonitor.proto.
};
```

5. Use std::string BufMon_Sub_PortDropEvent(std::string token) to implement interface packet drop event subscription.

```
std::string BufMon_GrpcClient::BufMon_Sub_PortDropEvent(std::string token)
{
    std::cout << "-------BufMon_Sub_PortDropEvent-------- " << std::endl;

   PortQueDropEvent stNodeEvent;
   PortQueDropEvent_PortQueDrop* pstParam = stNodeEvent.add_portquedrop();

    UINT uiIfIndex = 0;
    UINT uiQueIdx = 0;
```

```
    UINT uiAlarmType = 0;

    std::cout<<"Please input interface queue info : ifIndex queIdx alarmtype " <<
std::endl;
    cout<<"alarmtype : 1 for ingress; 2 for egress; 3 for port headroom"<<endl;

    std::cin>>uiIfIndex>>uiQueIdx>>uiAlarmType; // Set the subscription parameters
and interface index.
    pstParam->set_ifindex(uiIfIndex);
    pstParam->set_queindex(uiQueIdx);
    pstParam->set_alarmtype(uiAlarmType);

    ClientContext context;

    /* Token needs to be added to context */ // Set the token_id to be returned after
a successful login
    std::string key = "token_id";
    std::string value = token;
    context.AddMetadata(key, value);

    SubscribeReply reply;
    Status status = mStub->SubscribePortQueDropEvent(&context,stNodeEvent,&reply);
// Call the RPC method.

    return reply.result();
}
```

6. Use a loop to listen for event reports.

Implement this method in the GrpcServiceTest class.

```
void GrpcServiceTest::listen()
{
    GetReportRequest reportRequest;
    ClientContext context;
    ReportEvent reportedEvent;

    /* Add the token to the request */
    reportRequest.set_token_id(token);

    std::unique_ptr< ClientReader< ReportEvent>>
reader(GrpcServiceStub->GetEventReport(&context, reportRequest)); // Use
GetEventReport (which is generated from grpc_service.proto) to obtain event
information.

    std::string streamName;
    std::string eventName;
    std::string jsonText;
    std::string token;

    JsonFormatTool jsonTool;
```

```
    std::cout << "Listen to server for Event" << std::endl;
    while(reader->Read(&reportedEvent) ) // Read the received event report.
    {
        streamName = reportedEvent.stream_name();
        eventName = reportedEvent.event_name();
        jsonText = reportedEvent.json_text();
        token = reportedEvent.token_id();

          std::cout << "/***********EVENT COME**************/" << std::endl;
        std::cout << "TOKEN: " << token << std::endl;
        std::cout << "StreamName: "<< streamName << std::endl;
        std::cout << "EventName: " << eventName << std::endl;
        std::cout << "JsonText without format: " << std::endl << jsonText << std::endl;
        std::cout << std::endl;
        std::cout << "JsonText Formated: " << jsonTool.formatJson(jsonText) <<
std::endl;
        std::cout << std::endl;
    }

    Status status = reader->Finish();
    std::cout << "Status Message:" << status.error_message() << "ERROR code :" <<
status.error_code();
}  // Login and RPC request finished.
```

7. To log out, call the Logout method.

```
void GrpcServiceTest:: Logout ()
{
    LogoutRequest request;
    request.set_token_id(token);
    LogoutReply reply;
    ClientContext context;
    Status status = mStub->Logout(&context, request, &reply);
std::cout << "Logout! :" << reply.result() << std::endl;
}
```

Using Set operations in dial-in mode

1. Create a GrpcServiceTest class in the same way you do for Get operations.
2. Customize the Login method in the same way you do for Get operations.
3. Initiate an RPC request to the device.

   This example uses the Device module.

   ```
   rpc Set(SetRequest) returns (SetResponse)
   ```

4. Create a gNMITest class to encapsulate the RPC method.

   Use the gNMI::Stub class that is automatically created by gnmi.proto to call the RPC method.

   ```
   class gNMITest
   {
   public:
   gNMITest(std::shared_ptr<Channel> channel, const std::string tokenId ):

   mStubGrpcService(GrpcService::NewStub(channel)),
   ```

```
mStubgNMIService(gNMI::NewStub(channel)),
                                                mTokenID(tokenId ){}
     SetResponse TestSetResponseInformation(SetRequest &request, const std::string
tokenId);
/*---delete: Device/Base/HostName. Restore the default for HostName -----------*/
SetResponse DeleteDeviceBaseHostName();      /* delete: Device Base/HostName*/

/* update: Device/Base/HostName, string_val("string_hostname") */
SetResponse UpdateDeviceBaseHostNameStringVal();

/* replace: Device/Base/HostName, string_val("string_hostname") */
REPL_001 SetResponse ReplaceDeviceBaseHostNameStringVal();

private:
std::unique_ptr<GrpcService::Stub> mStubGrpcService;
std::unique_ptr<gNMI::Stub> mStubgNMIService;
std::string mTokenID;
};
```

5. Use customized methods to perform Set operations on the Device module.

```
// Call the Set method to implement communication between client and server and get
the response.
SetResponse gNMITest::TestSetResponseInformation(SetRequest &request, const
std::string tokenId)
{
SetResponse reply;
ClientContext context;
context.AddMetadata("token_id", tokenId);

/* Call the Set method */
Status ret = mStubgNMIService->Set(&context,request,&reply);
if( StatusCode::OK != ret.error_code())
{
std::cout<<"error: "<<ret.error_message()<<std::endl;
}
return reply;
}
// Delete operation
SetResponse gNMITest:: DeleteDeviceBaseHostName ()       /* prefix == Device/Base
*/
{
SetRequest  request;
/* SetRequest->prefix */
Path        *path01 = request.mutable_prefix();
PathElem    *pathelem01 = path01->add_elem();
pathelem01->set_name("Device");
PathElem    *pathelem02 = path01->add_elem();
pathelem02->set_name("Base");
```

```
/* SetRequest->delete */
Path        *path02 = request.add_delete_();
PathElem    *pathelem03 = path02->add_elem();
pathelem03->set_name("HostName");
/* Gather response info. */
return TestSetResponseInformation(request, mTokenID);
}
// Update operation
SetResponse gNMITest::UpdateDeviceBaseHostNameStringVal()
{
SetRequest  request;

/* SetRequest->prefix */
Path        *path01 = request.mutable_prefix();
PathElem    *pathelem01 = path01->add_elem();
pathelem01->set_name("Device");
PathElem    *pathelem02 = path01->add_elem();
pathelem02->set_name("Base");

/* SetRequest->update */
Update      *update01 = request.add_update();
Path        *path02 = update01->mutable_path();
PathElem    *pathelem03 = path02->add_elem();
pathelem03->set_name("HostName");

TypedValue  *typevalue01 = update01->mutable_val();
typevalue01->set_string_val("string_hostname");

/* Gather response info. */
return TestSetResponseInformation(request, mTokenID);
}
// Replace operation
SetResponse gNMITest::ReplaceDeviceBaseHostNameStringVal()
{
SetRequest  request;

/* SetRequest->prefix */
Path        *path01 = request.mutable_prefix();
PathElem    *pathelem01 = path01->add_elem();
pathelem01->set_name("Device");
PathElem    *pathelem02 = path01->add_elem();
pathelem02->set_name("Base");

/* SetRequest->replace */
Update      *replace01 = request.add_replace();
Path        *path02 = replace01->mutable_path();
PathElem    *pathelem03 = path02->add_elem();
pathelem03->set_name("HostName");
```

```
TypedValue  *typevalue01 = replace01->mutable_val();
typevalue01->set_string_val("string_hostname");

/* Gather response info. */
return TestSetResponseInformation(request, mTokenID);
}
```

6. To log out, call the Logout method in the same way you do for Get operations.

Using CLI operations in dial-in mode

1. Create a GrpcServiceTest class in the same way you do for Get operations.
2. Customize the Login method in the same way you do for Get operations.
3. Initiate an RPC request to the device.

   This example uses the CliConfig method in file **grpc_service.proto**.

   ```
   rpc CliConfig (CliConfigArgs)  returns (stream CliConfigReply) {}
   ```

4. Use the GrpcServiceTest class to encapsulate the RPC method in the same way you do for Get operations in dial-in mode.
5. Use customized methods to support CliConfig operations.

   ```
   // Make a thread to listen to the sever and get messages
   Status GrpcServiceTest::listen(const std::string& command)
   {
   CliConfigArgs reportRequest;
   ClientContext context;
   CliConfigReply reportedEvent;
   std::string key = "token_id";
   std::string value = token;
   context.AddMetadata(key, value);
   /* Add token to request */
   reportRequest.set_reqid(12345678);
   reportRequest.set_cli(command);

   std::unique_ptr< ClientReader< CliConfigReply>> reader(mStub->CliConfig(&context,
   reportRequest));

   std::string streamName;
   std::string output;
   int64 resreqid;

   std::cout << "Command result" << std::endl;
   while( reader->Read(&reportedEvent) )
   {
   streamName = reportedEvent.errors();
   output = reportedEvent.output();
   resreqid = reportedEvent.resreqid();
   std::cout << "resreqid: "<< resreqid << std::endl;
   std::cout << "errors: "<< streamName << std::endl;
   std::cout << "output: \n"<< output << "\n"<< std::endl;
   }
   Status status = reader->Finish();
   ```

```
return status;
}
```

6. Use a loop in the main function to wait for commands.

   Use the GrpcServiceTest class.

```
int main(int argc, char *argv[])
{
const char *cmd;
unsigned int i = 0;
unsigned int cycle = 0;

if (4 == argc)
{
g_server_address = argv[1];
g_username = argv[2];
g_password = argv[3];
std::cout << "server_address: " << g_server_address <<std::endl;
std::cout << "username: " << g_username << " " << "password: " << g_password <<
std::endl;
auto channel =
grpc::CreateChannel(g_server_address,grpc::InsecureChannelCredentials());
 // 1. Log in
GrpcServiceTest reporter(channel);
if(0 != reporter.Login(g_username, g_password))
        {
            return 0;
        }
        while(1)
        {// 2. Read a command and execute the command
                std::cout<<"\n\nPlease Input Command:\n";
                getline(std::cin,g_command);          // Read a command
                Status status = reporter.listen(g_command);
                if (!status.ok())
               {
                   std::cout << status.error_code() << ": " << status.error_message()
<< std::endl;
                    break;
               }
        }
    }
    std::cout<<"Complete exec Command."<<std::endl;
    return 0;
}
```

7. To log out, call the Logout method in the same way you do for Get operations.

Using dial-out mode

In dial-out mode, the application needs to provide the gRPC server code so the collector can receive and resolve data obtained from the device.

The application performs the following operations:

- Inherit the automatically generated GRPCDialout::Service class, overload the automatically generated RPC Dialout service, and resolve the fields.
- Register the RPC service with the specified listening port.

To develop the collector-side application in dial-out mode:

1. Inherit and overload RPC service Dialout.

Create class DialoutTest and inherit GRPCDialout::Service.

```
class DialoutTest final : public GRPCDialout::Service { // Overload the automatically generated abstract class.
    Status Dialout(ServerContext* context, ServerReader< DialoutMsg>* reader, DialoutResponse* response) override; // Implement RPC method Dialout.
};
```

2. Register the DialoutTest service as a gRPC service and specify the listening port.

```
using grpc::Server;
using grpc::ServerBuilder;
std::string server_address("0.0.0.0:60057"); // Specify the address and port to listen to.
DialoutTest dialout_test; // Define the object declared in step 1.
ServerBuilder builder;
builder.AddListeningPort(server_address, grpc::InsecureServerCredentials());// Add the listening port.
builder.RegisterService(&dialout_test); // Register the service.
std::unique_ptr<Server> server(builder.BuildAndStart()); // Start the service.
server->Wait();
```

3. Implement the Dialout method and data resolution.

```
Status DialoutTest::Dialout(ServerContext* context, ServerReader< DialoutMsg>* reader, DialoutResponse* response)
{
        DialoutMsg msg;

        while( reader->Read(&msg))
        {
            const DeviceInfo &device_msg = msg.devicemsg();
            std::cout<< "Producer-Name: " << device_msg.producername() << std::endl;
            std::cout<< "Device-Name: " << device_msg.devicename() << std::endl;
            std::cout<< "Device-Model: " << device_msg.devicemodel() << std::endl;
            std::cout<<"Sensor-Path: " << msg.sensorpath()<<std::endl;
            std::cout<<"Json-Data: " << msg.jsondata()<<std::endl;
            std::cout<<std::endl;
        }
        response->set_response("test");

        return Status::OK;
}
```

4. After obtaining the DialoutMsg object (generated from the proto definition file) through the Read method, you can call the method to obtain the field values.

Contents

Configuring INT

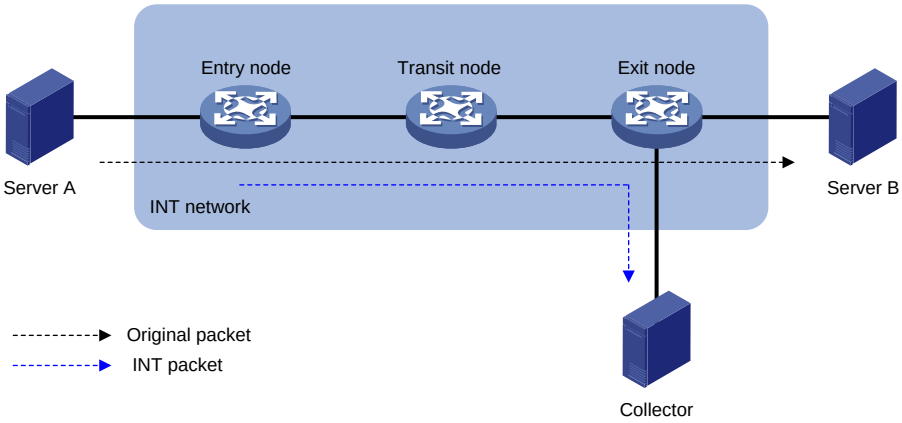
About INT

The Inband Network Telemetry (INT) feature is a network monitoring technology designed to collect data from the device. The device sends data to a collector in real time for device performance monitoring and network monitoring.

INT network components

As shown in Figure 1, an INT network contains the following INT-enabled devices: one entry node, one transit node, and one exit node.

Figure 1 INT network

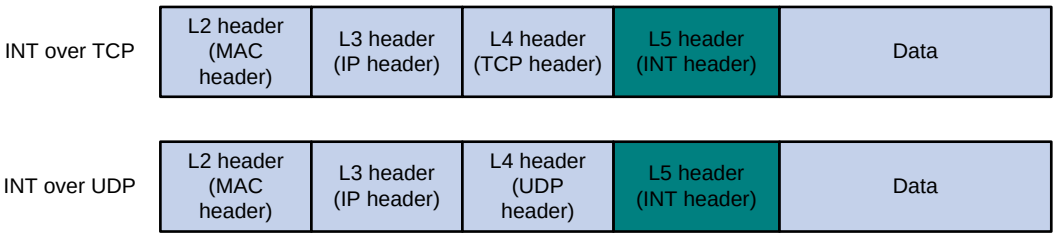


INT packet formats

INT generates INT packets by mirroring original packets, inserting INT headers, and collecting data. The INT header and collected data are in the original IP header. Therefore, an INT packet and its original packet have the same IP header and forwarding path.

The device supports generating INT packets from TCP packets and UDP packets. Figure 2 shows the INT packet formats. The 64 most significant bits of the INT header are fixed at 0xaaaaaaaabbbbbbbb, which are the INT mark.

Figure 2 INT packet formats



How INT works

INT supports common INT and flexible INT. The two types of INT have the following differences:

- **Common INT**—Each node needs to be configured with an INT role on its input interface: ingress, transit, and egress. Traffic flows are defined on the entry node by using a QoS policy. INT flows are automatically identified on the transit node and exit node and processed according to configured actions. On each input interface in the path, you can perform INT processing only on the flows defined on the entry node.
- **Flexible INT**—No device role needs to be configured on each node. On each node, an ACL can be used to define a flow and an action used to take on the defined flow. For the same flow, the original packets are matched on the entry node, and the INT packets are matched on the transit node and exit node. You can define multiple flows on an interface and take different actions on different flows.

Common INT is easy to configure and is recommended. Use flexible INT only when you need to process multiple flows on an interface.

Common INT

As shown in Figure 3, the nodes in common INT perform the following functions:

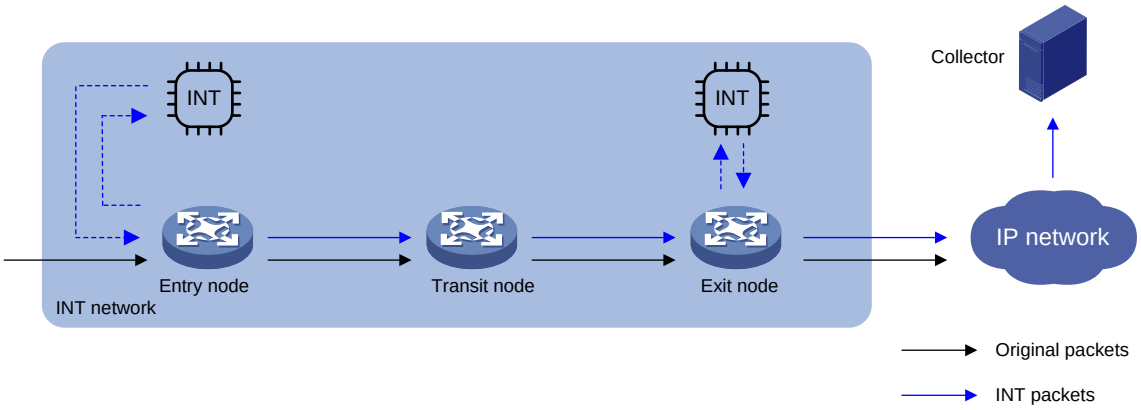
1. On the entry node, the ingress port uses a QoS policy to sample matching packets, and mirrors sampled packets to the INT processor. Then, the INT processor adds an INT header to the INT packet and loops it back to the ingress port. The ingress port identifies the looped-back INT packet according to the INT mark, adds collected data to it, and forwards it to the egress port. The egress port adds collected data to the INT packet and sends it to the transit node.
2. On the transit node, the ingress port identifies the INT packet according to the INT mark, adds collected data to it, and forwards it to the egress port. The egress port adds collected data to the INT packet, and sends it to the exit node.
3. On the exit node, the ingress port identifies the INT packet according to the INT mark, adds collected data to the INT packet, encapsulates the INT packet with the configured parameters, and sends it to the collector.

Flexible INT

As shown in Figure 3, the nodes in flexible INT perform the following functions:

1. On the entry node, the input interface uses an ACL to sample matching packets, and mirrors sampled packets to the INT processor. Then, the INT processor adds an INT header to the INT packet and loops it back to the input interface. The ingress port identifies the looped-back INT packet according to an ACL and adds collected data to it, and forwards it. The egress port adds collected data to the INT packet and sends it to the transit node.
2. On the transit node, the input interface uses an ACL to identify INT packets, adds collected data to INT packets, and forwards them to the input interface. The input interface adds collected data to INT packets and sends them to the exit node.
3. On the exit node, the input interface uses an ACL to identify INT packets and mirrors them to the INT processor. The INT processor encapsulates the INT packets and sends them to the collector.

Figure 3 Flexible INT



Restrictions and guidelines: INT configuration

Common INT and flexible INT can only be deployed in underlay networks.

As a best practice to configure INT, first configure the transit node and exit node, and then the entry node.

Configuring common INT

Configuring the exit node

1. Specify a device ID.
   a. Enter system view.
      system-view
   b. Specify a device ID for the exit node.
      telemetry ifa device-id *address*
      By default, the exit node does not have a device ID.
2. Configure the egress interface.
   a. Enter interface view.
      interface *interface-type interface-number*
   b. Specify the interface as the egress interface.
      telemetry ifa role egress
      By default, an interface is not used as the egress interface.
   c. Return to system view
      quit
3. Configure addressing parameters to encapsulate in INT packets sent to the collector.
   telemetry ifa collector source *source-address* **destination** *dest-address* **source-port** *port* **destination-port** *port* [**vlan** *vlan-id*]
   By default, no addressing parameters are configured for INT packets.
4. Enable INT globally.
   telemetry ifa global enable
   By default, INT is enabled globally.

Configuring the transit node

1. Specify a device ID.
   a. Enter system view.
      system-view
   b. Specify a device ID for the transit node.
      telemetry ifa device-id *address*
      By default, the transit node does not have a device ID.
2. Configure the transit interface.
   a. Enter interface view.
      interface *interface-type interface-number*
   b. Specify the interface as the transit interface.
      telemetry ifa role transit
      By default, an interface is not used as the transit interface.
   c. Return to system view
      quit
3. Enable INT globally.
   telemetry ifa global enable
   By default, INT is enabled globally.

Configuring the entry node

1. Specify a device ID.
   a. Enter system view.
      system-view
   b. Specify a device ID for the entry node.
      telemetry ifa device-id *address*
      By default, the entry node does not have a device ID.
2. Configure the ingress interface.
   a. Enter interface view.
      interface *interface-type interface-number*
   b. Specify the interface as the ingress interface.
      telemetry ifa role ingress
      By default, an interface is not used as the ingress interface.
   c. Return to system view
      quit
3. Enable internal loopback on an interface.
   a. Enter interface view.
      interface *interface-type interface-number*
   b. Enable internal loopback on the interface.
      telemetry ifa loopback
      By default, internal loopback is disabled on an interface.

Enable internal loopback on any interface that is in the same port group as the ingress port. To view port grouping information, execute the **display qos-acl resource** command. Ports under the same **Interfaces** field are in the same port group.

c. Return to system view

quit

This function is required only on the S9850 series switches.

4. Mirror packets to the INT processor.

a. Execute the following commands in sequence to define a traffic class:

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

if-match *match-criteria*

quit

For more information about the **if-match** command, see QoS commands in *ACL and QoS Command Reference*.

b. Execute the following commands in sequence to define a traffic behavior:

traffic behavior *behavior-name*

mirror-to ifa-processor [**sampler** *sampler-name*]

quit

For more information about the **mirror-to** command, see mirroring commands in *Network Management and Monitoring Command Reference*.

c. Execute the following commands in sequence to define a QoS policy:

qos [**mirroring**] **policy** *policy-name*

classifier *classifier-name* **behavior** *behavior-name*

quit

d. Execute the following commands in sequence to apply the QoS policy to the inbound direction of an interface:

interface *interface-type interface-number*

qos apply [**mirroring**] **policy** *policy-name* **inbound**

quit

5. Enable INT globally.

telemetry ifa global enable

By default, INT is enabled globally.

Configuring flexible INT

Configuring the exit node

1. Specify a device ID.

a. Enter system view.

system-view

b. Specify a device ID for the exit node.

telemetry ifa device-id *address*

By default, the exit node does not have a device ID.

2. Mirror incoming INT packets to the INT processor and drop the original INT packets.

a. Create a user-defined ACL and enter user-defined ACL view.

For information about the **acl** configuration command, see ACL commands in *ACL and QoS Command Reference*.

b. Configure a rule for the user-defined ACL.

For information about the **rule** (user-defined ACL view) configuration command, see ACL commands in *ACL and QoS Command Reference*.

If the entry node uses an ACL when mirroring packets to the INT processor, the ACLs used for any other action on any node must have the same identification attributes plus an attribute to identify the INT flag. The identification attributes and the attribute to identify the INT flag must be in the same rule. For example, the rule in the ACL used on the entry node is **rule permit tcp source 10.0.0.3 0**, the rule in the ACL used for any other action must be **rule permit tcp source 10.0.0.3 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0**.

c. Return to system view.

quit

d. Enter interface view.

interface *interface-type interface-number*

e. Configure the action of mirroring incoming INT packets to the INT processor and dropping the original INT packets.

telemetry ifa *ifa-id* **acl user-defined** { *acl-number* | **name** *acl-name* } **action mirror-to-processor drop**

By default, no action is configured.

f. Return to system view.

quit

3. Configure addressing parameters to encapsulate in INT packets sent to the collector.

telemetry ifa collector source *source-address* **destination** *dest-address* **source-port** *port* **destination-port** *port* [**vlan** *vlan-id*]

By default, no addressing parameters are configured for INT packets.

4. Enable INT globally.

telemetry ifa global enable

By default, INT is enabled globally.

Configuring the transit node

1. Specify a device ID.

a. Enter system view.

system-view

b. Specify a device ID for the transit node.

telemetry ifa device-id *address*

By default, the transit node does not have a device ID.

2. Add collected data to INT packets on the input interface.

a. Create a user-defined ACL and enter user-defined ACL view.

For information about the **acl** configuration command, see ACL commands in *ACL and QoS Command Reference*.

b. Configure a rule for the user-defined ACL.

For information about the **rule** (user-defined ACL view) configuration command, see ACL commands in *ACL and QoS Command Reference*.

If the entry node uses an ACL when mirroring packets to the INT processor, the ACLs used for any other action on any node must have the same identification attributes plus an attribute to identify the INT flag. The identification attributes and the attribute to identify the INT flag must be in the same rule. For example, the rule in the ACL used on the entry node is **rule permit tcp source 10.0.0.3 0**, the rule in the ACL used for any other action must be **rule permit tcp source 10.0.0.3 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0**.

c. Return to system view.

quit

d. Enter interface view.

interface *interface-type interface-number*

e. Configure the action of adding collected data to incoming INT packets.

telemetry ifa *ifa-id* **acl user-defined** { *acl-number* | **name** *acl-name* } **action add-metadata**

By default, no action is configured.

f. Return to system view.

quit

3. Enable INT globally.

telemetry ifa global enable

By default, INT is enabled globally.

Configuring the entry node

1. Specify a device ID.

a. Enter system view.

system-view

b. Specify a device ID for the entry node.

telemetry ifa device-id *address*

By default, the entry node does not have a device ID.

2. Mirror original packets on the input interface to the INT processor.

a. Create an IPv4, Layer 2, or user-defined ACL and enter ACL view.

For information about the **acl** configuration command, see ACL commands in *ACL and QoS Command Reference*.

b. Configure a rule for the ACL.

For information about the **rule** configuration command, see ACL commands in *ACL and QoS Command Reference*.

c. Return to system view.

quit

d. Enter interface view.

interface *interface-type interface-number*

e. Configure the action of mirroring incoming original packets to the INT processor.

telemetry ifa *ifa-id* [**acl** [**mac** | **user-defined**]{ *acl-number* | **name** *acl-name* }] **action mirror-to-processor** [**sampler** *sampler-name*]

By default, no action is configured.

f. Return to system view.

quit

3. Enable internal loopback on an interface.
   a. Enter interface view.
      interface *interface-type interface-number*
   b. Enable internal loopback on the interface.
      telemetry ifa loopback
      By default, internal loopback is disabled on an interface.
   c. Return to system view
      quit
   This function is required only on the S9850 series switches.
4. Add collected data to local loopback traffic on the input interface.
   a. Create a user-defined ACL and enter user-defined ACL view.
      For information about the **acl** configuration command, see ACL commands in *ACL and QoS Command Reference*.
   b. Configure a rule for the user-defined ACL.
      For information about the **rule** (user-defined ACL view) configuration command, see ACL commands in *ACL and QoS Command Reference*.
      If the entry node uses an ACL when mirroring original packets to the INT processor, the ACLs used for any other action on any node must have the same identification attributes plus an attribute to identify the INT flag. The identification attributes and the attribute to identify the INT flag must be in the same rule. For example, the rule in the ACL used to mirror original packets to the INT processor is **rule permit tcp source 10.0.0.3 0**, the rule in the ACL used for any other action must be **rule permit tcp source 10.0.0.3 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0**.
   c. Return to system view.
      quit
   d. Enter interface view.
      interface *interface-type interface-number*
   e. Configure the action of adding collected data to local loopback traffic.
      telemetry ifa *ifa-id* **acl user-defined** { *acl-number* | **name** *acl-name* } **local-loopback action add-metadata**
      By default, no action is configured.
   f. Return to system view.
      quit
5. Enable INT globally.
   telemetry ifa global enable
   By default, INT is enabled globally.

Display and maintenance commands for INT

Execute **display** commands in any view.

Task	Command
Display information about QoS policies applied to interfaces (see *ACL and QoS Command Reference*).	**display qos** [**mirroring**] **policy interface** [*interface-type interface-number*] [**slot** *slot-number*] **inbound**

Task	Command
Display INT configuration.	**display telemetry ifa**

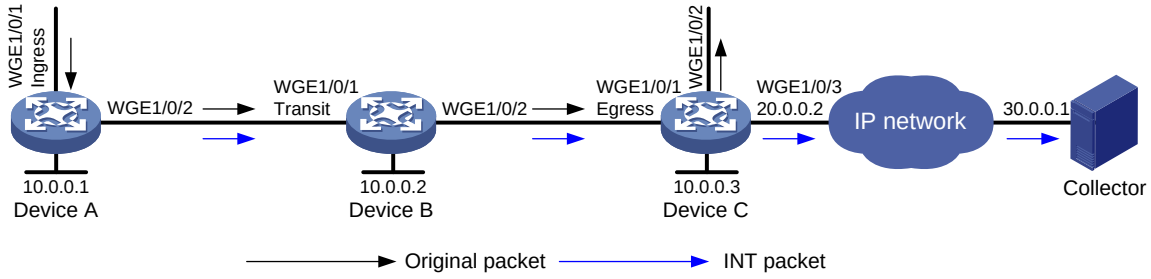
INT configuration examples

Example: Configuring common INT

Network configuration

As shown in Figure 4, configure common INT to send INT packets to the collector.

Figure 4 Network diagram



Procedure

1. Assign IP addresses to interfaces and configure routes. Make sure the network connections are available. (Details not shown.)
2. Configure Device C:

   # Specify 10.0.0.3 as the device ID of the exit node.

   ```
   [DeviceC] telemetry ifa device-id 10.0.0.3
   ```

   # Specify Twenty-FiveGigE 1/0/1 as the egress interface.

   ```
   [DeviceC] interface twenty-fivegige 1/0/1
   [DeviceC-Twenty-FiveGigE1/0/1] telemetry ifa role egress
   [DeviceC-Twenty-FiveGigE1/0/1] quit
   ```

   # Configure addressing parameters to encapsulate in INT packets sent to the collector.

   ```
   [DeviceC] telemetry ifa collector source 20.0.0.2 destination 30.0.0.1 source-port
   12 destination-port 14
   ```

   # Enable INT globally.

   ```
   [DeviceC] telemetry ifa global enable
   ```
3. Configure Device B:

   # Specify 10.0.0.2 as the device ID of the transit node.

   ```
   <DeviceB> system-view
   [DeviceB] telemetry ifa device-id 10.0.0.2
   ```

   # Specify Twenty-FiveGigE 1/0/1 as the transit interface.

   ```
   [DeviceB] interface twenty-fivegige 1/0/1
   [DeviceB-Twenty-FiveGigE1/0/1] telemetry ifa role transit
   [DeviceB-Twenty-FiveGigE1/0/1] quit
   ```

   # Enable INT globally.

   ```
   [DeviceB] telemetry ifa global enable
   ```
4. Configure Device A:

Specify 10.0.0.1 as the device ID of the entry node.

```
<DeviceA> system-view
[DeviceA] telemetry ifa device-id 10.0.0.1
```

Specify Twenty-FiveGigE 1/0/1 as the ingress interface.

```
[DeviceA] interface twenty-fivegige 1/0/1
[DeviceA-Twenty-FiveGigE1/0/1] telemetry ifa role ingress
[DeviceA-Twenty-FiveGigE1/0/1] quit
```

(For only S9850 series switches.) Enable internal loopback on Twenty-FiveGigE 1/0/3.

```
[DeviceA] interface twenty-fivegige 1/0/3
[DeviceA-Twenty-FiveGigE1/0/3] telemetry ifa loopback
[DeviceA-Twenty-FiveGigE1/0/3] quit
```

Create a sampler named **samp** in random sampling mode, and set the sampling rate to 8. One packet from 256 packets is selected.

```
<DeviceA> system-view
[DeviceA] sampler samp mode random packet-interval n-power 8
```

Create a traffic class named **classifier1**, and use destination MAC address a08c-fdd7-fd99 as the match criterion in the traffic class.

```
[DeviceA] traffic classifier classifier1
[DeviceA-classifier-classifier1] if-match destination-mac a08c-fdd7-fd99
[DeviceA-classifier-classifier1] quit
```

Create a traffic behavior named **behavior1**, and configure the action of mirroring traffic to the INT processor.

```
[DeviceA] traffic behavior behavior1
[DeviceA-behavior-behavior1] mirror-to ifa-processor sampler samp
[DeviceA-behavior-behavior 1] quit
```

Create a QoS policy named **ifa1**, and associate traffic class **classifier1** with traffic behavior **behavior1** in the QoS policy.

```
[DeviceA] qos policy ifa1
[DeviceA-qospolicy-ifa1] classifier classifier1 behavior behavior1
[DeviceA-qospolicy-ifa1] quit
```

Apply QoS policy **ifa1** to the incoming traffic of Twenty-FiveGigE 1/0/1.

```
[DeviceA] interface twenty-fivegige 1/0/1
[DeviceA-Twenty-FiveGigE1/0/1] qos apply policy ifa1 inbound
[DeviceA-Twenty-FiveGigE1/0/1] quit
```

Enable INT globally.

```
[DeviceA] telemetry ifa global enable
```

Verify the configuration

Verify the configuration on Device A.

```
[DeviceA] display qos policy interface twenty-fivegige 1/0/1 inbound
Interface: Twenty-FiveGigE1/0/1
  Direction: Inbound
  Policy: ifa1
   Classifier: classifier1
     Operator: AND
     Rule(s) :
      If-match destination-mac a08c-fdd7-fd99
     Behavior: behavior1
      Mirroring:
```

```
        Mirror to the ifa-processor sampler samp
[DeviceA] display telemetry ifa
  Telemetry ifa status: Enabled
  Telemetry ifa device-id: 10.0.0.1
  Telemetry ifa role:
    Twenty-FiveGigE1/0/1: Ingress
  Telemetry ifa loopback:
    Twenty-FiveGigE1/0/3
```

Verify the configuration on Device B.

```
[DeviceB] display telemetry ifa
  Telemetry ifa status: Enabled
  Telemetry ifa device-id: 10.0.0.2
  Telemetry ifa role:
    Twenty-FiveGigE1/0/1: Transit
```

Verify the configuration on Device C.

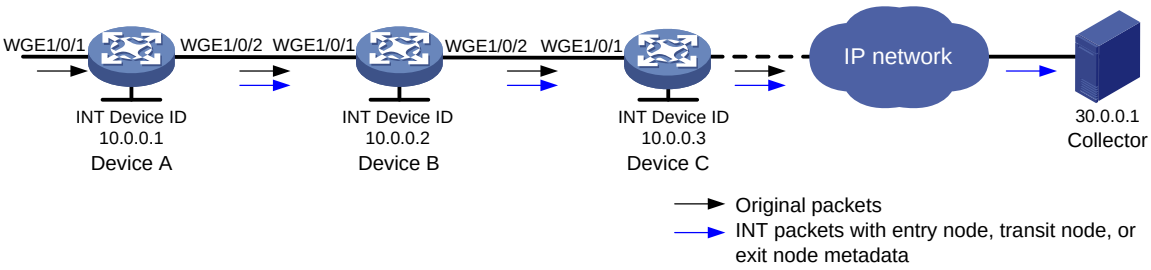
```
[DeviceC] display telemetry ifa
  Telemetry ifa status: Enabled
  Telemetry ifa device-id: 10.0.0.3
  Telemetry ifa role:
    Twenty-FiveGigE1/0/1: Egress
  Telemetry ifa collector:
    Source IP: 20.0.0.2
    Destination IP: 30.0.0.1
    Source-port: 12
    Destination-port: 14
```

Example: Configuring flexible INT

Network configuration

As shown in Figure 5, configure flexible INT to send INT packets to the collector.

Figure 5 Network diagram



Procedure

1. Assign IP addresses to interfaces and configure routes. Make sure the network connections are available. (Details not shown.)
2. Configure Device C:

   # Specify 10.0.0.3 as the device ID of the exit node.

   ```
   <DeviceC> system-view
   [DeviceC] telemetry ifa device-id 10.0.0.3
   ```

Create user-defined ACL 5000, and configure a rule to match INT packets with source IP address 192.168.1.2.

```
[DeviceC] acl user-defined 5000
[DeviceC-acl-user-5000] rule permit tcp source 192.168.1.2 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0
[DeviceC-acl-user-5000] rule permit udp source 192.168.1.2 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0
[DeviceC-acl-user-5000] quit
```

Configure the action of mirroring incoming INT packets on Twenty-FiveGigE 1/0/1 to the INT processor and dropping the original INT packets.

```
[DeviceC] interface twenty-fivegige 1/0/1
[DeviceC-Twenty-FiveGigE1/0/1] telemetry ifa 1 acl user-defined 5000 action mirror-to-processor drop
[DeviceC-Twenty-FiveGigE1/0/1] quit
```

Configure addressing parameters to encapsulate in INT packets sent to the collector.

```
[DeviceC] telemetry ifa collector source 20.0.0.2 destination 30.0.0.1 source-port 12 destination-port 14
```

Enable INT globally.

```
[DeviceC] telemetry ifa global enable
```

3. Configure Device B:

Specify 10.0.0.2 as the device ID of the transit node.

```
<DeviceB> system-view
[DeviceB] telemetry ifa device-id 10.0.0.2
```

Create user-defined ACL 5000, and configure a rule to match INT packets with source IP address 192.168.1.2.

```
[DeviceB] acl user-defined 5000
[DeviceB-acl-user-5000] rule permit tcp source 192.168.1.2 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0
[DeviceB-acl-user-5000] rule permit udp source 192.168.1.2 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0
[DeviceB-acl-user-5000] quit
```

Configure the action of mirroring INT packets on Twenty-FiveGigE 1/0/1 to the INT processor.

```
[DeviceB] interface twenty-fivegige 1/0/1
[DeviceB-Twenty-FiveGigE1/0/1] telemetry ifa 1 acl user-defined 5000 action add-metadata
[DeviceB-Twenty-FiveGigE1/0/1] quit
```

Enable INT globally.

```
[DeviceB] telemetry ifa global enable
```

4. Configure Device A:

Specify 10.0.0.1 as the device ID of the entry node.

```
<DeviceA> system-view
[DeviceA] telemetry ifa device-id 10.0.0.1
```

Create a sampler named **samp** in random sampling mode, and set the sampling rate to 8. One packet from 256 packets is selected.

```
[DeviceA] sampler samp mode random packet-interval n-power 8
```

Create IPv4 basic ACL 2000, and configure a rule to match packets with source IP address 192.168.1.2.

```
[DeviceA] acl basic 2000
[DeviceA-acl-ipv4-basic-2000] rule permit source 192.168.1.2 0
```

```
[DeviceA-acl-ipv4-basic-2000] quit
```

Configure the action of mirroring original packets on Twenty-FiveGigE 1/0/1 to the INT processor.

```
[DeviceA] interface twenty-fivegige 1/0/1
[DeviceA-Twenty-FiveGigE1/0/1] telemetry ifa 2 acl 2000 action mirror-to-processor sampler samp
[DeviceA-Twenty-FiveGigE1/0/1] quit
```

(For only S9850 series switches.) Enable internal loopback on Twenty-FiveGigE 1/0/3.

```
[DeviceA] interface twenty-fivegige 1/0/3
[DeviceA-Twenty-FiveGigE1/0/3] telemetry ifa loopback
[DeviceA-Twenty-FiveGigE1/0/3] quit
```

Create user-defined ACL 5000, and configure a rule to match INT packets with source IP address 192.168.1.2.

```
[DeviceA] acl user-defined 5000
[DeviceA-acl-user-5000] rule permit tcp source 192.168.1.2 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0
[DeviceA-acl-user-5000] rule permit udp source 192.168.1.2 0 ifa l5 aaaaaaaabbbbbbbb ffffffffffffffff 0
[DeviceA-acl-user-5000] quit
```

Configure the action of adding collected data to local loopback traffic.

```
[DeviceA] interface twenty-fivegige 1/0/1
[DeviceA-Twenty-FiveGigE1/0/1] telemetry ifa 3 acl user-defined 5000 local-loopback action add-metadata
[DeviceA-Twenty-FiveGigE1/0/1] quit
```

Enable INT globally.

```
[DeviceA] telemetry ifa global enable
```

Verify the configuration

Verify the configuration on Device A.

```
[DeviceA] display telemetry ifa
  Telemetry ifa status: Enabled
  Telemetry ifa device-id: 10.0.0.1
  Telemetry ifa action:
    Twenty-FiveGigE1/0/1:
      Telemetry ifa 1 acl 2000 action mirror-to-processor sampler samp
      Telemetry ifa 2 acl user-defined 5000 local-loopback action add-metadata
  Telemetry ifa loopback:
    Twenty-FiveGigE1/0/3
```

Verify the configuration on Device B.

```
[DeviceB] display telemetry ifa
  Telemetry ifa status: Enabled
  Telemetry ifa device-id: 10.0.0.2
  Telemetry ifa action:
    Twenty-FiveGigE1/0/1:
      Telemetry ifa 1 acl user-defined 5000 action add-metadata
```

Verify the configuration on Device C.

```
[DeviceC] display telemetry ifa
  Telemetry ifa status: Enabled
  Telemetry ifa device-id: 10.0.0.3
```

```
Telemetry ifa action:
  Twenty-FiveGigE1/0/1:
    Telemetry ifa 1 acl user-defined 5000 action mirror-to-processor drop
Telemetry ifa collector:
  Source IP: 20.0.0.2
  Destination IP: 30.0.0.1
  Source-port: 12
  Destination-port: 14
```