CISCO SERVICE CONTROL SOLUTION GUIDE

Cisco Service Control GRE and GTP Insertion Solution Guide, Release 5.2.x

Revised: September 23, 2015

Note This document supports all 5.2.x releases.

1 Overview of the Service Control GRE and GTP Insertion Solution

This section provides an overview of the Generic Routing Encapsulation (GRE) and GPRS Tunneling Protocol (GTP) insertion solution. The GRE and GTP insertion solution enables the Cisco SCE to monitor and control the GRE and GTP. This section includes:

GRE Feature Overview

Tunneling protocols are used in many networks for various purposes, including VPNs, traffic engineering (TE), security, and so on. Some encapsulations are IP based such as GRE, and some are placed in lower levels, for example in Layer 2.5.

Cisco SCE natively analyzes IP-based traffic. IP addresses are the basis for flow classification (the 5-tuple contains IP addresses) and subscriber identification (most commonly used subscriber ID is the subscriber IP address).

In tunneled networks, the IP packet is further encapsulated by some encapsulation protocol. To analyze the IP packet, Cisco SCE needs to perform specific parsing of the encapsulating protocol.

Furthermore, in some networks, the IP addresses used inside the tunneled traffic are private IP addresses. For example, addresses that are not unique among the flows seen on a single Cisco SCE. In these cases, the identification of the source and destination of the packet must be based on both the IP address and the tunnel information found in the packet.

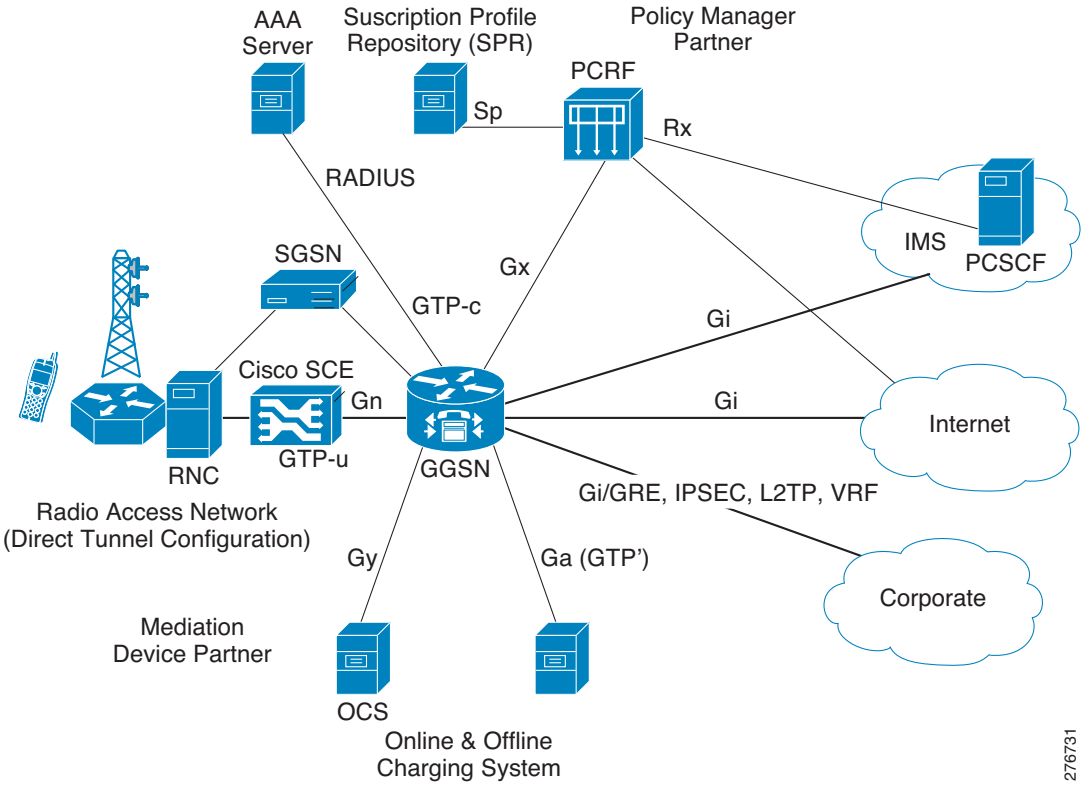
In networks with private IP addresses, or without them, it is desirable to treat a whole segment of the network as a single subscriber. Such a segment may be a whole VPN, a specific VLAN, a specific tunnel, and so on. In these cases, Cisco SCE defines the subscriber by a general identifier that applies to all the IP addresses generating traffic over that network segment. This method allows the Cisco SCE to disregard the specific client, and refer only to the group it is associated with, when defining the subscribers.

GTP Feature Overview

In a General Packet Radio Service (GPRS) backbone network, GTP is a high-level tunneling protocol used to carry signaling and data.

A GPRS backbone network (or core network) contains several nodes of GPRS Support Node (GSN), which communicate with each other using IP as shown in Figure 1. GSNs are either Serving GPRS Support Nodes (SGSNs) or Gateway GPRS Support Nodes (GGSNs). The SGSN is used to communicate with Mobile Terminal (MT) equipment or relay data inside the backbone network to outside connections and the GGSNs in turn controls these SGSNs. This relaying is implemented in the backbone network by using GTP on top of UDP/IP (GTPv1).

Figure 1 Cisco eGGGSN PCC Reference Model With DPI Intercept Application Manager



A GTP tunnel is a virtual connection between two GSNs (usually between SGSN/RNC and GGSN). One GTP Tunnel can contain several multiplexed user data connections (several MTs can share same GTP tunnel without any knowledge of each other). The GTP tunnel uses a packet data path in the GPRS backbone network, which is the UDP/IP path.

The evolvement of the wireless technology makes the wireless segment more similar to the wire line market and as a result the demand for deep packet inspection (DPI) applications in this segment is increased.

The GTP support allows Cisco SCE to monitor local and roaming traffic in the Gn/Gp pipes. Differentiated Services Code Point (DCSP) marking of active application can be implemented in the GTP environment as well.

2 GRE Tunneling Feature Details

This section summarizes the Cisco SCE 10000 support for GRE tunneling. It gives you these GRE tunneling information:

- GRE is supported only in Cisco SCE 10000 from Cisco Service Control Operating System (SCOS) Release 3.5.5.
- GRE is supported on top of other tunnels – Multiprotocol Label Switching (MPLS) and VLAN.
- GRE is supported alongside plain IP and other types of tunnels – MPLS and VLAN.
- Layer 7 classification and load balancing relate to the internal IP packet.
- Accounting and bandwidth control are based on the length of the internal IP.
- Active actions based on packet injection are supported.

This section contains these subsections:

GRE Skip Mode

For GRE support to work, the GRE skip mode must be enabled. The default setting of the GRE skip mode is disabled. Use an administrator-level CLI command to configure the GRE skip mode. For additional information, see the "GRE and GTP CLI Commands" section on page 6.

GRE Active Actions

Active actions (drop, block, redirect, and so on) have the same level of support for GRE tunneling (including GRE over other tunnels) as in case of plain IP.

GRE Internal Protocol

The protocol field in the GRE header indicates the protocol of the inner payload; the only supported protocol type is IP version 4 (IPv4) with the value of 0x800. However, the system may be configured by using the CLI to support the value of 0xFFFF also as the protocol value for protocol type IPv4. For additional information, see the "GRE and GTP CLI Commands" section on page 6.

GRE IP Fragmentation

The SCOS supports internal and external fragmentation of the GRE tunneling protocol. When the GRE skip mode is disabled, the Cisco SCE hardware treats the GRE tunneling protocol as plain IP. When GRE skip is enabled, the fragments are handled as described in these sections:

Internal Fragments

Internal fragments are fully supported by using the same process as plain IP.

External Fragments

The first external fragment is delivered to the SCOS and then, if necessary, to the application. The additional fragments are bypassed.

Reorder

Minimal reordering of external fragments might be experienced because the first fragment is sent to the software application while the following fragments are bypassed.

The reordering can be prevented by using an appropriate Quick Forwarding Traffic rule. Using a Quick Forwarding rule might result in loss of certain active actions support, such as HTTP redirect.

Accounting and Bandwidth Management

Accounting and bandwidth management are handled as usual in the context of fragmented GRE traffic.

GRE and Other Traffic

This section provides details on:

GRE and Plain IP

A mix of GRE traffic and plain IP traffic is fully supported.

GRE and Other Tunnels

A mix of GRE traffic and traffic over other tunnels is fully supported.

This means that any type of tunnel supported by the Cisco SCE is still supported in GRE skip mode. For example, GRE alongside MPLS/VPN, and so on.

GRE Tunnel Concatenation (GRE over Other Tunnels)

GRE tunneling can be configured over other tunneling protocols.

These combinations are supported:

- VLAN (skip mode only) + GRE
- MPLS (skip mode only) + GRE
- VLAN (skip mode only) + MPLS (skip mode only) + GRE

GRE DSCP Marking

In the GRE skip mode, DSCP marking can be configured on either the external IP header or the internal IP header. Both headers cannot be marked concurrently. The default is to mark the external header. Marking the internal IP header is configured through the CLI. For additional information, see the "GRE and GTP CLI Commands" section on page 6.

In external fragmentation, only the first fragment is marked.

GRE Versions and Platforms

GRE tunneling is supported only on Cisco SCE 10000 from SCOS Release 3.5.5 onwards.

3 GTP Tunneling Feature Details

This section describes the additional details of the GTP feature. It contains this subsection:

The behavior of the Cisco SCE in association with GTP is as follows:

- The Cisco SCE skips the GTP header and uses the internal IP headers for the classification.
- The Cisco SCE ignores the GTP header (for example, accounting header).
- The Cisco SCE supports a mix of GTP traffic and pure IP traffic in the network.
- DSCP marking in the GTP tunnel is performed on the type of service (ToS) byte of the external IP header or the internal IP header.
- The support for internal fragments is identical to the fragments support in pure IP traffic.
  - Internal fragments—The internal packet is fragmented.

– External fragments—The original packet was encapsulated with the tunnel header and then it was fragmented. In this case, the mid or last fragments are bypassed.

GTP Configuration and Monitoring

GTP, like IPinIP, GRE, L2TP, and MPLS, is yet another tunnel header that the Cisco SCE supports. In general, the Cisco SCE has two modes of support for tunnels, namely skip and VPN aware. In these modes, the Cisco SCE uses the tunnel information for the classification. For GTP tunneling, the Cisco SCE supports only the skip mode.

GTP skip is configured by using a CLI command. When GPT skip mode is configured, the hardware applies quick forwarding on all GTP traffic to avoid GTP-U packet reordering. Additionally, the FPGA configuration of the GTP-U UDP port (default is 2152) is done by using a CLI command. For additional information on the CLI command, see the "GRE and GTP CLI Commands" section on page 6.

The GTP-U UDP port is searched on UDP destination port.

To check if there is Layer 3 data over GTP-U, the GTP header message type is compared to 0xFF to verify if the GTP-U data has a message type of 0xFF. GTP-U data with a message type other than 0xFF is bypassed through quick forwarding by using the skip mode. The default setting for the Cisco SCE GTP skip mode configuration is disabled.

The Cisco SCE counts the number of GTP-U packets received.

4 GRE and GTP Insertion Solution Limitations

Table 1 lists the hardware platform limitations for the GTP and GRE insertion solution.

Table 1 GTP and GRE Insertion Solution Hardware Limitations

Protocol	Hardware Platform Limitations
GRE	Supported only on Cisco SCE 10000
GTP	Supported only on Cisco SCE 10000

5 GRE and GTP CLI Commands

Table 2 lists the GRE and GTP CLI commands.

Table 2 GRE and GTP CLI Commands

Command	Description	Default
show interface LineCard 'slot' {VLAN | MPLS | L2TP | asymmetric-L2-support | IP-tunnel [IPinIP | GRE | subscriber-tunneled-IPv6]}	Shows the configuration of Layer 2, L2TP, MPLS, VLAN, and IP tunnel. IPinIP, GRE, and subscriber-tunneled-IPv6 are IP tunnels but are not mutually exclusive with other tunnels, therefore, they are displayed separately by using **show interface LineCard 'slot' IP-tunnel IPinIP/GRE/subscriber-tunneled-IPv6** command.	—

Table 2 GRE and GTP CLI Commands (continued)

Command	Description	Default
[no] IP-tunnel GRE allow-special-protocol-field-value	Enables or disables the special-protocol-field value to overcome a known networking bug, whereby the protocol field is 0xFFFF for IPv4 in some cases. This command is relevant only when GRE skip is also enabled.	—
[no] IP-tunnel {L2TP skip | GTP skip | GRE {skip | DSCP-marking-skip | IPinIP {skip | DSCP-marking-skip | bypass-external-fragments} | subscriber-tunneled-IPv6 skip}	Enables or disables recognition of IP tunnels and skipping into the internal IP packet. All IP tunnels except IPinIP and GRE are mutually exclusive among them, and are also mutually exclusive with using VLAN for classification and MPLS/VPN auto-learn. IPinIP and GRE skip mode configuration (enabled or disabled), do not affect the configuration of other IP tunnels. **No IP-tunnel**—Disables all IP tunnels except IPinIP and GRE. **L2TP skip**—Identifies L2TP tunnels and skips into the internal IP packet. **IPinIP skip**—Identifies IP-over-IP tunnels and skips into the internal IP packet. **IPinIP DSCP-marking-skip**—Enables DSCP marking of IPinIP flows to be completed in the internal IP header. Marking the internal IP header is possible only when IPinIP skip is also enabled. **IPinIP bypass-external-fragments**—Disables delivering IPinIP external fragments to application. This mode protects the application from looking into packet content beyond the actual packet length. **GRE DSCP-marking-skip**—Enables DSCP marking of GRE flows to be completed in the internal IP header. Marking the internal IP header is only possible when GRE skip is also enabled. **GRE skip**—Identifies GRE tunnels and skips the internal IP packet. **GTP skip**—Identifies GTP tunnels and skips the internal IP packet.	no IP-tunnel

6 Protocol Packet Examples

This section contains examples of protocol packets and contains these subsections:

Example of GTP-U Packets with Sequence Number Option

This is an example of GTP-U Packets with sequence number option:

```
No.     Time        Source          Destination    Protocol Info
843     25.211434   172.16.108.65   13.248.2.1     GTP <TCP> [TCP segment of a reassembled PDU]

Frame 843 (1314 bytes on wire, 1314 bytes captured)
Ethernet II, Src: FoundryN_52:92:85 (00:0c:db:52:92:85), Dst: RisqModu_04:78:7a (00:c0:8b:04:78:7a)
Internet Protocol, Src: 172.17.171.1 (172.17.171.1), Dst: 172.18.10.1 (172.18.10.1)
User Datagram Protocol, Src Port: 2152 (2152), Dst Port: 2152 (2152)
    Source port: 2152 (2152)
    Destination port: 2152 (2152)
    Length: 1280
    Checksum: 0x0000 (none)
GPRS Tunneling Protocol
    Flags: 0x32
        001. .... = Version: GTP release 99 version (1)
        ...1 .... = Protocol type: GTP (1)
        .... 0... = Reserved: 0
        .... .0.. = Is Next Extension Header present?: no
        .... ..1. = Is Sequence Number present?: yes
        .... ...0 = Is N-PDU number present?: no
    Message Type: T-PDU (0xff)
    Length: 1264
    TEID: 0x2c883699
    Sequence number: 0x01a5
    N-PDU Number: 0x00
    Next extension header type: 0x00
Internet Protocol, Src: 172.16.108.65 (172.16.108.65), Dst: 13.248.2.1 (13.248.2.1)
Transmission Control Protocol, Src Port: http (80), Dst Port: 11328 (11328), Seq: 420524, Ack: 908, Len: 1220
```

Example of GTP-U Packets Without Sequence Number Option

This is an example of GTP-U packets without sequence number option:

```
No.     Time        Source          Destination    Protocol Info
845     25.249872   13.248.2.1      172.16.108.65  GTP <TCP> 11328 > http [ACK] Seq=908 Ack=415208 Win=12287 Len=0

Frame 845 (90 bytes on wire, 90 bytes captured)
Ethernet II, Src: FoundryN_52:92:85 (00:0c:db:52:92:85), Dst: Cisco_21:44:80 (00:13:5f:21:44:80)
Internet Protocol, Src: 172.18.10.1 (172.18.10.1), Dst: 172.17.171.1 (172.17.171.1)
User Datagram Protocol, Src Port: 2152 (2152), Dst Port: 2152 (2152)
    Source port: 2152 (2152)
    Destination port: 2152 (2152)
    Length: 56
    Checksum: 0xd8af [correct]
GPRS Tunneling Protocol
    Flags: 0x30
        001. .... = Version: GTP release 99 version (1)
        ...1 .... = Protocol type: GTP (1)
        .... 0... = Reserved: 0
        .... .0.. = Is Next Extension Header present?: no
        .... ..0. = Is Sequence Number present?: no
        .... ...0 = Is N-PDU number present?: no
    Message Type: T-PDU (0xff)
    Length: 40
    TEID: 0x00000016
Internet Protocol, Src: 13.248.2.1 (13.248.2.1), Dst: 172.16.108.65 (172.16.108.65)
Transmission Control Protocol, Src Port: 11328 (11328), Dst Port: http (80), Seq: 908, Ack: 415208, Len: 0
```

7 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.