Configuring GPRS Tunneling Protocol Support

The GPRS Tunneling Protocol Support feature provides firewall support for General Packet Radio Switching (GPRS) Tunneling Protocol (GTP). GPRS is a data network architecture, which integrates with existing Global System for Mobile Communication (GSM) networks and provides always-on packet switched data services to corporate networks and the Internet. The European Telecommunications Standards Institute (ETSI) 3rd Generation Partnership Project (3GPP) produced the GPRS Tunneling Protocol (GTP), which allows multiprotocol packets to be tunneled through the UMTS (Universal Mobile Telecommunications System) or GPRS backbone between the Gateway GPRS Support Node (GGSN), Servings GPRS Support Node (SGSN), and UMTS Terrestrial Radio Access Network (UTRAN).

The integration of GPRS to GSM provides mobile phone, mobile Internet, and VPN services to subscribed users. This introduces new security risks to networks. Since GTP does not inherently provide any security or encryption of user data, the router firewall should support security for GTP. The GPRS Tunneling Protocol support feature configures this firewall support for GTP.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Restrictions for Configuring GPRS Tunneling Support

- The limit for the number of match statements for a Layer 7 class map is 64.
- The limit for the number of classes (including the default class) for a Layer 7 policy map is 255.
- The limit for the number of characters in a pattern string for a regex parameter map is 245.
- The data path supports up to 512 regular expressions (regex).
- Statistics are available for only packets and bytes for a class. No statistics are available for the **match** command.

Information About Configuring GPRS Tunneling Protocol Support

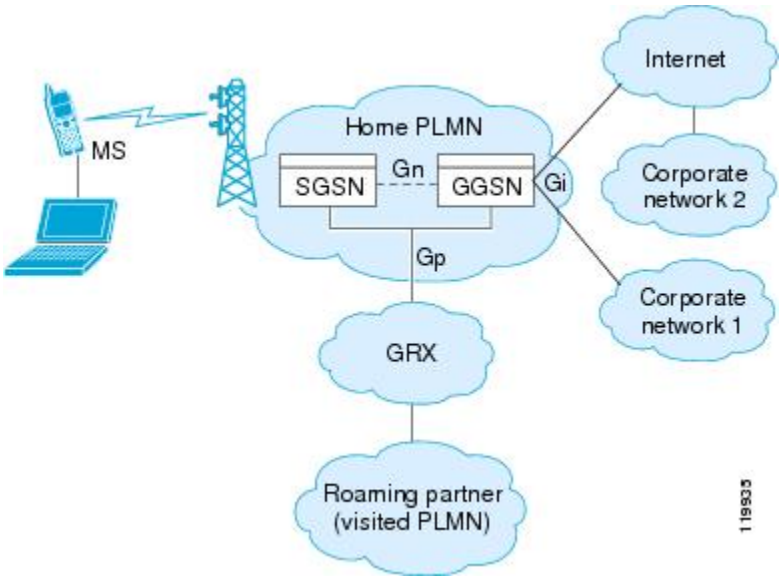
GPRS Overview

General Packet Radio Service (GPRS) provides uninterrupted connectivity for mobile subscribers between Global System for Mobile Communication (GSM) networks and corporate networks or the Internet. The Gateway GPRS Support Node (GGSN) is the interface between the GPRS wireless data network and other networks. The Serving GPRS Support Node (SGSN) performs mobility, data session management, and data compression.

The GPRS core network architecture has a mobile station (MS) that is logically connected to an SGSN. The main function of an SGSN is to provide data support services to an MS. An SGSN is logically connected to a GGSN by using GTP. If the connection is within the same operator's Public Land Mobile Network (PLMN), the connection is called the Gn interface. If the connection is between two different PLMNs, the connection is known as the Gp interface. A GGSN provides a data gateway to external networks, such as the Internet or the corporate network, through an interface called the Gi interface. GTP is used to encapsulate data from an

MS. GTP also includes mechanisms for establishing, moving, and deleting tunnels between SGSN and GGSN in roaming scenarios.

Figure 1: GPRS Core Network



The Universal Mobile Telecommunications System (UMTS) is the commercial convergence of fixed-line telephony, mobile, Internet, and computer technology. UMTS Terrestrial Radio Access Network (UTRAN) is the networking protocol used for implementing wireless networks in this system. GTP allows multiprotocol packets to be tunneled through a UMTS/GPRS backbone between a GGSN, an SGSN, and the UTRAN.

The Gp and Gi interfaces are the primary points of interconnection between an operator's network and untrusted external networks. Operators must take care to protect their networks from attacks that originate on these external networks.

The Gp interface is the logical connection that supports mobile (roaming) data users between PLMNs. GTP establishes a connection between a local SGSN and a user's home GGSN.

Data that originates from the MS is sent to the Gi interface. It is also the interface that is exposed to public data networks and networks of corporate customers.

The traffic sent out from a GGSN or arriving for an MS at the Gi interface can virtually be of any kind since the application being used by the MS is unknown.

GTP allows multiprotocol packets to be tunneled through the GPRS backbone between GPRS Support Nodes (GSNs). GTP provides a tunnel control and management protocol that allows an SGSN to provide GPRS network access for an MS by creating, modifying, and deleting tunnels. GTP uses a tunneling mechanism to provide a service for carrying user data packets.

Note When using GTP with failover, if a GTP connection is established and the active unit fails before data is transmitted over the tunnel, the GTP data connection (with a "j" flag set) is not replicated to the standby unit. This occurs because the active unit does not replicate embryonic connections to the standby unit.

GTP Overview

General Packet Radio Service (GPRS) Tunneling Protocol (GTP) allows multiprotocol packets to be tunneled through the GPRS backbone between GPRS Support Nodes (GSN). Three GTP versions are available. The GPRS Tunneling Support feature supports two GTP versions: GTP Version 0 (GTPv0) and GTP Version 1 (GTPv1).

In GTPv0, a GPRS Mobile Station (MS) is connected to a Serving GPRS Support Node (SGSN) without being aware of the protocol. A Packet Data Protocol (PDP) context is identified by the Tunnel Identifier (TID), which is a combination of the International Mobile Subscriber Identity (IMSI) and the Network Service Access Point Identifier (NSAPI). Each MS can have up to 15 NSAPIs. This allows an MS to create multiple PDP contexts with different NSAPIs, based on the application requirements for various quality of service (QoS) levels. The TID is carried in the GTPv0 header.

An IMSI has the following three parts:

- Mobile Country Code (MCC) that consists of three digits. The MCC uniquely identifies the country of domicile of a mobile subscriber.
- Mobile Network Code (MNC) that consists of two or three digits for GSM applications. The MNC identifies the home GSM Public Land Mobile Network (PLMN) of the mobile subscriber. The length of the MNC depends on the value of the MCC.

  Note A combination of two- and three-digit MNC codes within a single MCC area is not recommended.

- Mobile Subscriber Identification Number (MSIN) that identifies a mobile subscriber within a GSM PLMN. The National Mobile Subscriber Identity (NMSI) consists of the MNC and the MSIN.

GTPv1 introduces the concept of primary and secondary contexts for an MS. A primary context is associated with an IP address and indicates other parameters like the Access Point Name (APN) to be attached to the receiving GSN. Secondary contexts created for this primary PDP context share the IP address and other parameters that are already associated with the primary context. This allows an MS to initiate another context with a different quality of service (QoS) requirement and also share the IP address already obtained for the primary context. Primary and secondary contexts share the Tunnel Endpoint ID (TEID) on the control plane and have different TEID values in the data plane. Since all primary and associated secondary contexts share the IP address, Traffic Flow Templates (TFT) are used to classify traffic in the downlink direction towards the MS. TFTs are exchanged during context creation.

Only the create PDP context request for the primary PDP contains an IMSI. The IMSI and NSAPI together uniquely identify a PDP context. A secondary PDP context activation contains a Linked NSAPI (LNSAPI) indicating the NSAPI that is assigned to any one of the already activated PDP contexts for this PDP address and APN.

Note UDP is the only supported, defined path protocol for signaling messages for GTPv0 and GTPv1.

GTP Traffic Through Firewall

The main General Packet Radio Service (GPRS) Tunneling Protocol (GTP) traffic that a device inspects is the roaming traffic. Roaming traffic is caused when a Mobile Station (MS) moves from its Home Public Land Mobile Network (HPLMN) to a Visited PLMN (VPLMN).

The GTP traffic through the firewall includes the following messages:

- Serving GPRS Support Node (SGSN) to Gateway GPRS Support Node (GGSN) GTP messages
- GGSN-to-SGSN GTP messages
- SGSN-to-SGSN GTP messages

How to Configure GPRS Tunneling Protocol Support

The General Packet Radio Service (GPRS) Tunneling Protocol (GTP) commands are configured using the Cisco Common Classification Policy Language (C3PL) Layer 7 class map containing filters with the required actions, which are generated in the Layer 7 policy map. The Layer 7 policy map is configured with the inspect action as a child policy of the Layer 4 policy map, using the **service-policy (policy-map)** command in a Layer 4 class that matches the GTP protocol. The Layer 4 policy can have several classes for more than one protocol and is attached to the firewall zone pair.

Configuring GPRS Tunneling Protocol Support

Perform this to configure the GPRS Tunneling Protocol (GTP) support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *expression*
5. **exit**
6. **parameter-map type inspect** {*parameter-map-name* | **global**}
7. **gtp** {**request-queue** *elements* | **timeout** {{**gsn** | **pdp-context** | **signaling** | **tunnel**} *minutes* | **request-queue** *seconds*} | **tunnel-limit** *number*}
8. **exit**
9. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
10. **match** {**apn regex** *parameter-name* | **mcc** *country-code* **mnc** *network-code* | **message-id** *id* | **message-length min** *min-length* **max** *max-length* | **version** *number*}
11. **exit**
12. **policy-map type inspect** *protocol-name policy-map-name*
13. **class type inspect** *protocol-name class-map-name*
14. **log**
15. **exit**
16. **exit**
17. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
18. **match protocol** *protocol-name* [*parameter-map*] **[signature]**
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect** *class-map-name*
22. **inspect** [*parameter-map-name*]
23. **service-policy** *protocol-name policy-map*
24. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**parameter-map type regex** *parameter-map-name* **Example:** `Router# parameter-map type regex PARAM_REG`	Configures a parameter-map type to match a specific traffic pattern and enters parameter map configuration mode.
Step 4	**pattern** *expression* **Example:** `Router(config-profile)# pattern apn.cisco.com`	Configures a matching pattern that specifies a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering.
Step 5	**exit** **Example:** `Router(config-profile)# exit`	Exits parameter map configuration mode and returns to global configuration mode.
Step 6	**parameter-map type inspect** {*parameter-map-name* | **global**} **Example:** `Router(config)# parameter-map type inspect global`	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action and enters parameter-map type inspect mode.
Step 7	**gtp** {**request-queue** *elements* | **timeout** {{**gsn** | **pdp-context** | **signaling** | **tunnel**} *minutes* | **request-queue** *seconds*} | **tunnel-limit** *number*} **Example:** `Router(config-profile)# gtp tunnel-limit 100`	Configures the inspection parameters for GTP.
Step 8	**exit** **Example:** `Router(config-profile)# exit`	Exits parameter-map type inspect mode and returns to global configuration mode.
Step 9	**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name* **Example:** `Router(config)# class-map type inspect gtpv0 LAYER7_CLASS_MAP`	Creates a Layer 7 (application-specific) inspect type class map and enters class-map configuration mode.

	Command or Action	Purpose
Step 10	**match** {**apn regex** *parameter-name* | **mcc** *country-code* **mnc** *network-code* | **message-id** *id* | **message-length min** *min-length* **max** *max-length* | **version** *number*} **Example:** `Router(config-cmap)# match mcc 100 mnc 91`	Configures the classification criteria for inspect type class map for the GTP.
Step 11	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode and returns to global configuration mode.
Step 12	**policy-map type inspect** *protocol-name policy-map-name* **Example:** `Router(config)# policy-map type inspect gtpv0 LAYER7_POLICY_MAP`	Creates a Layer 7 (protocol-specific) inspect type policy map and enters policy-map configuration.
Step 13	**class type inspect** *protocol-name class-map-name* **Example:** `Router(config-pmap)# class type inspect gtpv0 LAYER7_CLASS_MAP`	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration.
Step 14	**log** **Example:** `Router(config-pmap-c)# log`	Generates a log of messages.
Step 15	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration and returns to policy-map configuration mode.
Step 16	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 17	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* **Example:** `Router(config)# class-map type inspect LAYER4_CLASS_MAP`	Creates a Layer 3 and Layer 4 inspect type class map and enters class-map configuration mode.
Step 18	**match protocol** *protocol-name* [*parameter-map*] **[signature]** **Example:** `Router(config-cmap)# match protocol gtpv0`	Configures the match criterion for a class map on the basis of a specified protocol.
Step 19	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration and returns to global configuration mode.
Step 20	**policy-map type inspect** *policy-map-name* **Example:** `Router(config)# policy-map type inspect LAYER4_POLICY_MAP`	Creates a Layer 3 and Layer 4 inspect type policy map and enters policy-map configuration mode.
Step 21	**class type inspect** *class-map-name* **Example:** `Router(config-pmap)# class type inspect LAYER4_CLASS_MAP`	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration mode.
Step 22	**inspect** [*parameter-map-name*] **Example:** `Router(config-pmap-c)# inspect`	Enables Cisco IOS stateful packet inspection.
Step 23	**service-policy** *protocol-name policy-map* **Example:** `Router(config-pmap-c)# service-policy gtpv0 LAYER7_POLICY_MAP`	Attaches a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map.

	Command or Action	Purpose
Step 24	**end** **Example:** `Router(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to privileged EXEC mode.

Configuration Examples for GPRS Tunneling Protocol Support

Example: Configuring the GPRS Tunneling Protocol Support

The following example shows how to configure the GTP tunneling protocol support:

```
Router> enable
Router# configure terminal
Router# parameter-map type regex PARAM_REG
Router(config-profile)# pattern apn.cisco.com
Router(config-profile)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# gtp tunnel-limit 100
Router(config-profile)# exit
Router(config)# class-map type inspect gtpv0 LAYER7_CLASS_MAP
Router(config-cmap)# match mcc 100 mnc 91
Router(config-cmap)# exit
Router(config)# policy-map type inspect gtpv0 LAYER7_POLICY_MAP
Router(config-pmap)# class type inspect gtpv0 LAYER7_CLASS_MAP
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# class-map type inspect LAYER4_CLASS_MAP
Router(config-cmap)# match protocol gtpv0
Router(config-cmap)# exit
Router(config)# policy-map type inspect LAYER4_POLICY_MAP
Router(config-pmap)# class type inspect LAYER4_CLASS_MAP
Router(config-pmap-c)# inspect
Router(config-pmap-c)# service-policy gtpv0 LAYER7_POLICY_MAP
Router(config-pmap-c)# end
```

Additional References for GPRS Tunneling Protocol Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring GPRS Tunneling Protocol Support

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 1: Feature Information for configuring GPRS Tunneling Support

Feature Name	Releases	Feature Information
Configuring GPRS Tunneling Protocol Support	Cisco IOS XE Release 3.4S	The GPRS Tunneling Protocol Support feature provides firewall support for the General Packet Radio Switching (GPRS) Tunneling Protocol (GTP). The following commands were introduced or modified: **class type inspect**, **class-map type inspect**, **gtp**, **match (gtp)**, **match protocol(zone)**, **inspect**, **parameter-map type inspect**, **parameter-map type regex**, **policy-map type inspect service-policy (policy-map)**, **show parameter-map type inspect**, **show parameter-map type regex**, **show policy-map type inspect zone-pair**.