Cisco IOS Intelligent Wireless Access Gateway Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Intelligent Wireless Access Gateway Commands

A through Z

allow-static-ip

To specify whether the static IP address provided by the Intelligent Services Gateway (ISG) session is allowed by the Intelligent Wireless Access Gateway (iWAG)-GPRS Tunneling Protocol (GTP) or not, use the **allow-static-ip** command in the GTP APN configuration mode. To not allow the assigned static IP address, use the **no** form of this command.

allow-static-ip

no allow-static-ip

Command Default

This command is used by default.

Command Modes

GTP APN configuration

Command History

Release	Modification
Cisco IOS XE Release 3.13	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Examples

The following example shows how to use the static IP address allowed by the iWAG-GTP:

```
Router(config)# gtp
Router(config-gtp)# apn 2
Router(config-gtp-apn)# allow-static-ip
```

clear mcsa statistics

To clear the mobile client service abstraction (MCSA) notification statistics, use the **clear mcsa statistics** command in privileged EXEC mode.

clear mcsa statistics {**sint**| **cint**}

Syntax Description

sint	Clears the service interface notification statistics.
cint	Clears the client interface notification statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Examples

The following example shows how to clear the MCSA service interface notification statistics:

```
Device# clear mcsa statistics sint
```

Related Commands

Command	Description
show mcsa statistics	Displays the MCSA notification statistics.

debug gtp

To enable debugging of the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) of the Intelligent Wireless Access Gateway (iWAG) feature in the Cisco ASR 1000 Series Aggregation Services Routers, use the **debug gtp** command in the privileged EXEC mode. To disable debugging of the GTP of the iWAG, use the **no** form of this command.

debug gtp {**all**| **audit**| **dns**| **internal**| **io**| **mcsa**| **path**| **pdp**| **protocol**| **timer**| **tunnel**} [**detail**| **error**| **event**| **function**| **message**]

no debug gtp {**all**| **audit**| **dns**| **internal**| **io**| **mcsa**| **path**| **pdp**| **protocol**| **timer**| **tunnel**} [**detail**| **error**| **event**| **function**| **message**]

Syntax Description

all	Debugs all the GTP parameters.
audit	Debugs the audit parameters.
dns	Debugs the domain name server parameters.
internal	Debugs the internal parameters.
io	Debugs the I/O manager instance.
mcsa	Debugs the mobile client service abstraction interface.
path	Debugs the path manager.
pdp	Debugs the Packet Data Protocol manager instance.
protocol	Debugs the GTP protocol.
timer	Debugs the timer.
tunnel	Debugs the GTP tunnel.
detail	(Optional) Debugs in detail.
error	(Optional) Debugs by error type.
event	(Optional) Debugs by event type.
function	(Optional) Debugs by function type.
message	(Optional) Debugs by message type.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **debug gtp** command:

```
Router# debug gtp all detail
IWAG GTP All component Detail debugging is on
```

The fields shown in the display are self-explanatory.

Related Commands

Command	Description
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.
show subscriber session	Displays the summary of either authenticated or unauthenticated sessions.

enable sessionmgr

To enable mobile client service abstraction (MCSA) to receive notifications from Intelligent Services Gateway (ISG), use the **enable sessionmgr** command in MCSA configuration mode. To disable this functionality, use the **no** form of this command.

enable sessionmgr

no enable sessionmgr

Syntax Description

This command has no arguments or keywords.

Command Default

MCSA does not receive notifications from ISG.

Command Modes

MCSA configuration (config-mcsa)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

Use the **show mcsa statistics sint** command to verify if the MCSA has received any notification from the ISG.

Examples

The following example shows how to enable the MCSA to receive notifications from ISG:

```
Device> enable
Device# configuration terminal
Device(config-if) mcsa
Device(config-mcsa) enable sessionmgr
Device(config-mcsa) end
```

Related Commands

Command	Description
show mcsa statistics sint	Displays the MCSA notifications statistics.

generate grekey

To dynamically generate upstream or downstream generic routing encapsulation (GRE) keys for mobile nodes (MNs) in a local mobile anchor (LMA) or a mobile access gateway (MAG) respectively, use the **generate grekey** command in MAG or LMA configuration mode respectively. To disable the dynamic generation of upstream or downstream GRE keys in an LMA or MAG, use the **no** form of this command.

generate grekey

no generate grekey

Syntax Description

This command has no arguments or keywords.

Command Default

The upstream or the downstream GRE keys for the MNs in the LMA or MAG respectively are generated dynamically.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

LMA configuration (config-ipv6-pmipv6-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

When you enter the **no generate key** command in the LMA or MAG configuration mode, the upstream or downstream GRE keys for the MNs are not generated dynamically. In that case, you must use the keys from the authentication, authorization, and accounting (AAA) profile or the local mobile node (MN) configuration.

When tunnel encapsulation mode in the configured MAG is GRE-IPv4, it is required that every mobile subscriber should have a GRE key. To provide every mobile subscriber with a GRE key value, perform one of the following:

- Enter the **generate grekey** in MAG configuration mode. The GRE key value, thus generated, are assigned to every mobile subscriber as and when the mobile subscribers attach to the MAG.
- Explicitly assign the GRE key values to the Network Access Identifier (NAI) in the PMIPv6 domain.
- Configure the GRE key for each subscriber in the AAA attributes.

Examples

The following example shows how to dynamically generate upstream GRE keys for MNs in an LMA:

```
Device> enable
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# no generate grekey
Device(config-ipv6-pmipv6-mag)# end
```

The following example shows how to explicitly configure GRE key to NAI to generate downstream GRE keys.

```
Device> enable
Device# configuration terminal
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai user1@example.com
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key up 100
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key down 200
Device(config-ipv6-pmipv6-domain-mn)# end
```

Related Commands

Command	Description
gre-encap-key	Configures the GRE key for the MN.
nai	Configures the NAI for the MN within the PMIPV6 domain.

gtp

To configure the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) of the Intelligent Wireless Access Gateway (iWAG) feature in the Cisco ASR 1000 Series Aggregation Services Routers, and to enter the GTP configuration mode, use the **gtp** command in the global configuration mode. To unconfigure the GTP of the iWAG, use the **no** form of this command.

gtp

no gtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to enable GTP and configure the parameters of an access point:

```
Router (config)# gtp
Router (config-gtp)# n3-request 3
Router (config-gtp)# interval t3-response 10
Router (config-gtp)# interval echo-request 60
Router (config-gtp)# interface local GigabitEthernet0/0/3
Router (config-gtp)# apn 1
Router (config-gtp)# apn-name starent.com
Router (config-gtp)# ip address ggsn 192.170.10.2
Router (config-gtp)# default-gw 192.168.10.1 prefix-len 16
Router (config-gtp)# dns-server 192.165.1.1
Router (config-gtp)# dhcp-server 192.168.10.1
Router (config-gtp)# dhcp-lease 30000
Router (config-gtp)# End
```

Note The configuration commands shown in the example are sufficient to bring up the GTP tunnel or Packet Data Protocol context. Few more commands are also available under the gtp command for additional configurations.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.
show subscriber session	Displays the summary of either authenticated or unauthenticated subscriber sessions.

mcsa

To enable mobile client service abstraction (MCSA), use the **mcsa** command in global configuration mode. To disable MCSA, use the **no** form of this command.

mcsa

no mcsa

Syntax Description

There are no arguments and keywords.

Command Default

An abstraction to receive event notifications is not available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced in Cisco IOS XE Release 3.8S.

Usage Guidelines

MCSA provides an abstraction to receive the discovery event and service event notifications from the MNs, and binding events from the local mobility anchor (LMA).

If you have enabled the mobile access gateway (MAG) functionality, you do not have to enable the **mcsa** command.

Enter the **sessionmgr** command in MAG configuration mode, before you enter the **mcsa** command in global configuration mode.

Enter the **no sessionmgr** command in MAG configuration mode, before you enter the **no mcsa** command in global configuration mode.

Examples

The following example shows how to enable MCSA:

```
Device# configuration terminal
Device(config) ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain) exit
Device(config) ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag) sessionmgr
Device(config-ipv6-pmipv6-mag) exit
Device(config) mcsa
```

The following example shows how to disable MCSA:

```
Device# configuration terminal
Device(config) ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain) exit
Device(config) ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag) no sessionmgr
Device(config-ipv6-pmipv6-mag) exit
Device(config) no mcsa
```

Related Commands

Command	Description
show mcsa statistics	Displays the MCSA notification statistics.

platform subscriber template

To enable policy templates in the Intelligent Services Gateway (ISG), use the **platform subscriber template** command in the global configuration mode. To disable policy templates in the ISG, use the **no** form of this command.

platform subscriber template

no platform subscriber template

Command Default

By default, this command disables policy templates in the ISG.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The router has to be reloaded after this command is configured for the command to take effect.

Examples

The following example shows how to enable policy templates in the ISG:

```
Router# configure terminal
Router(config)# platform subscriber template

A system RELOAD is required before policy templating will be enabled.
```

sessionmgr

To enable mobile access gateway (MAG) to process the notifications it receives through the mobile client service abstraction (MCSA) from Intelligent Services Gateway (ISG), use the **sessionmgr** command in MAG configuration mode. To disable this function, use the **no** form of this command.

sessionmgr

no sessionmgr

Syntax Description

This command does not have any arguments or keywords.

Command Default

MAG does not process the notification it receives through MCSA from the ISG.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

This command is not supported in standalone MAG configuration. Use this command only when a MAG is configured to coexist with an ISG.

Examples

The following example shows how to enable the MAG to process the notifications it receives through MCSA from the ISG:

```
Device> enable
Device# configuration terminal
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# exit
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# sessionmgr
```

show mcsa statistics

To display the mobile client service abstraction (MCSA) notification statistics, use the **show mcsa statistics** command in privileged EXEC mode.

show mcsa statistics{**sint**| **cint**}

Syntax Description

sint	Specifies the service interface notification statistics.
cint	Specifies client interface notification statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced

Usage Guidelines

Enable MCSA by using the **mcsa** command before you enter the **show mcsa statistics** command.

Examples

The following is sample output from the **show mcsa statistics sint** command:

```
Device# show mcsa statistics sint

Session Create Req              : 1
Session Create Res              : 1
Session Update Req              : 0
Session Update Res              : 0
Session Update Ind              : 0
Session Update Rep Success      : 0
Session Update Rep Failed       : 0
Session Delete Req              : 0
Session Delete Res              : 0
Session Delete Ind              : 0
Session Delete Rep Success      : 0
Session Delete Rep Failed       : 0
```

The following is sample output from the **show mcsa statistics cint** command:

```
Device# show mcsa statistics cint

Protocol : PMIPV6
Set Interest list               : 1
Attach Indication               : 1
Attach Rep Success              : 1
Attach Rep Failed               : 0
Detach Indication               : 0
Detach Rep Success              : 0
Detach Rep Failed               : 0
Cleanup Req                     : 0
Cleanup Res                     : 0
Attach Update Req               : 0
```

```
Attach Update Res               : 0
Attach Update Ind               : 0
Attach Update Rep Success       : 0
Attach Update Rep Failed        : 0

Protocol : GTP

Set Interest list               : 1
Attach Indication               : 0
Attach Rep Success              : 0
Attach Rep Failed               : 0
Detach Indication               : 0
Detach Rep Success              : 0
Detach Rep Failed               : 0
Cleanup Req                     : 0
Cleanup Res                     : 0
Attach Update Req               : 0
Attach Update Res               : 0
Attach Update Ind               : 0
Attach Update Rep Success       : 0
Attach Update Rep Failed        : 0
```

Related Commands

Command	Description
mcsa	Enables the MCSA.
clear mcsa statistics	Clears the MCSA notifications statistics.

show gtp apn

To display detailed statistics pertaining to the access points on the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) of the Intelligent Wireless Access Gateway (iWAG) feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each access point name (APN), use the **show gtp apn** command in the privileged EXEC mode.

show gtp apn {*apn-index*| **statistics** [*apn-index*| **all**]| **all**}

Syntax Description

apn-index	Index number of the access point that identifies an APN within the Cisco Gateway GPRS Support Node (Cisco GGSN) configuration. The range is from 1 to 65535.
statistics	Specifies detailed statistics pertaining to a particular access point.
all	Displays detailed statistics pertaining to all the access points on the GTP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show gtp apn** command displaying detailed statistics pertaining to all the access points on the GTP:

```
Router# show gtp apn all
There are 1 Access-Points configured
Index   AccessPointName                 PDP Count
-----------------------------------------------
1       starent.com                     31244
The following is sample output from the show gtp apn
 command displaying detailed statistics pertaining to a particular access point on the GTP:
Router# show gtp apn statistics all
There are 1 Access-Points activated
Index   AccessPointName                 PDP Count
-----------------------------------------------
1       starent.com                     31244
    PDP activation initiated by iWAG              : 0
```

```
    Successful PDP activation initiated by iWAG   : 0
    PDP deactivation initiated by iWAG            : 0
    Successful PDP deactivation initiated by iWAG : 0
    PDP deactivation initiated by GGSN            : 0
    Successful PDP deactivation initiated by GGSN : 0
    Current Active Sessions                       : 31244
```

The following is sample output from the **show gtp apn** command displaying statistics pertaining to the access points based on an APN index:

```
Router# show gtp apn 1
apn_index  : 1
apn_name : starent.com
GGSN Addr   : 192.170.10.2
Primary DNS : 192.165.1.1
DHCP Addr   : 192.168.10.1
DHCP Lease : 30000
Tunnel MTU  : 1460
Number of active PDPs in this APN: 31244
Default GW      Prefix Length Name              MAC Address PDP Count
192.168.10.1     16           IFNAME_GTP_VIF0 0000.0000.0000  1
```

The following table describes the significant fields shown in the displays.

Table 1: show gtp apn Field Descriptions

Field	Description
Index	Number assigned to an access point.
AccessPointName	Name of the access point.
DHCP Addr	Dynamic Host Configuration Protocol (DHCP) address of the APN.
DHCP Lease	DHCP lease time, in seconds.
Tunnel MTU	Maximum transmission unit of a tunnel.
Default GW	IP address of the default gateway, if configured.
Prefix Length	Prefix length of the default gateway.
MAC Address	MAC address of the APN.
PDP Count	Number of Packet Data Protocol contexts active for this access point name.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.

Command	Description
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.
show subscriber session	Displays the summary of either authenticated or unauthenticated subscriber sessions.

show gtp mcsa statistics

To display detailed statistics pertaining to mobile client service abstraction on the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) of the Intelligent Wireless Access Gateway (iWAG) feature in the Cisco ASR 1000 Series Aggregation Services Routers, use the **show gtp mcsa statistics** command in the privileged EXEC mode.

show gtp mcsa statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show gtp mcsa statistics** command:

```
Router# show gtp mcsa statistics
iWAG MCSA Statistics:
Attach Indications : 16          Attach Replies    : 16
Detach Indications : 0           Detach Replies    : 0
Update Indications : 0           Update Replies    : 0
Cleanup Requests   : 16          Cleanup Responses : 0
```

The following table describes the significant fields shown in the display.

Table 2: show gtp mcsa statistics Field Descriptions

Field	Description
Attach Indications	Indicates session establishment initiated by mobile client service abstraction.
Attach Replies	Displays the iWAG replies to the Attach Indications field.
Detach Indications	Indicates session deletion initiated by mobile client service abstraction.
Detach Replies	Displays the iWAG replies to the Detach Indications field.
Update Indications	Indicates session updates initiated by mobile client service abstraction.

Field	Description
Update Replies	Displays the iWAG replies to the Update Indications field.
Cleanup Requests	Indicates session deletion initiated by the iWAG.
Cleanup Responses	Displays the replies from mobile client service abstraction to the Cleanup Requests field.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.
show subscriber session	Displays the summary of either authenticated or unauthenticated subscriber sessions.

show gtp path

To display the path information for the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) of the Intelligent Wireless Access Gateway (iWAG) feature in the Cisco ASR 1000 Series Aggregation Services Routers, use the **show gtp path** command in the privileged EXEC mode.

show gtp path {**all**| **remote-address remote-address** [**vrf vrf-name**]| **statistics remote-address remote address** [**vrf vrf-name**]}

Syntax Description

all	Displays detailed statistics pertaining to all the GTP paths.
remote-address	Specifies the GTP path statistics according to IP address.
remote-address	Remote address of a GTP path.
vrf	Specifies the virtual routing and forwarding (VRF) instance containing the remote address.
vrf-name	Name of the VRF.
statistics	Specifies detailed statistics pertaining to a particular GTP path.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show gtp path** command displaying detailed statistics pertaining to all the GTP paths:

```
Router# show gtp path all
Total number of path: 2
VRF Name    Local address         Remote address        State  Version  PDP Count
default     192.170.10.1(2123)    192.170.10.2(2123)    UP     1        1
default     192.170.10.1(2152)    192.170.10.2(2152)    UP     1        1
The following is sample output from the show gtp path
 command displaying the GTP path statistics according to IP address:
Router# show gtp path remote-address 192.170.10.2
VRF Name    Local address         Remote address        State  Version  PDP Count
```

```
default     192.170.10.1(2123)    192.170.10.2(2123)    UP     1        1
default     192.170.10.1(2152)    192.170.10.2(2152)    UP     1        1
```

The following is sample output from the **show gtp path** command displaying detailed statistics pertaining to a particular GTP path:

```
Router# show gtp path statistics remote-address 192.170.10.2
VRF Name    Local address         Remote address        State  Version  PDP Count
default     192.170.10.1(2123)    192.170.10.2(2123)    UP     1        1
iWAG GTP Path Statistics:
  Number of short messages           : 0
  Number of unknown messages         : 0
  Unexpected signalling message      : 0
  Unsupported extension hdr recvd   : 0
  Signaling msg received             : 0
  Signaling msg sent                 : 2
  Signaling msg dropped              : 0
  Path failures                      : 0
  Path restart                       : 0
  Number of PDPs created             : 0
  Number of PDPs deleted             : 0
VRF Name    Local address         Remote address        State  Version  PDP Count
default     192.170.10.1(2152)    192.170.10.2(2152)    UP     1        1
iWAG GTP Path Statistics:
  Number of short messages           : 0
  Number of unknown messages         : 0
  Unexpected signalling message      : 0
  Unsupported extension hdr recvd   : 0
  Signaling msg received             : 0
  Signaling msg sent                 : 0
  Signaling msg dropped              : 0
  Path failures                      : 0
  Path restart                       : 0
  Number of PDPs created             : 0
  Number of PDPs deleted             : 0
```

The following table describes the significant fields shown in the displays.

Table 3: show gtp path Field Descriptions

Field	Description
VRF Name	Name of the corresponding VRF instance with which the access point is associated.
Local address	IP address and port number of the local end of the GTP path.
Remote address	IP address and port number of the remote end of the GTP path.
State	State information of the GTP path. Possible states are Up or Down.
Version	Displays the GTP paths according to the GTP version.
PDP Count	Number of Packet Data Protocol contexts that are active for this access point name.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.
show subscriber session	Displays the summary of either authenticated or unauthenticated subscriber sessions.

show gtp parameters

To display the summary of the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) parameters of the Intelligent Wireless Access Gateway (iWAG) feature in the Cisco ASR 1000 Series Aggregation Services Routers, use the **show gtp parameters** command in the privileged EXEC mode.

show gtp parameters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show gtp parameters** command:

```
Gn Prime Parameters:
    GTP path echo interval                        = 60
    GTP signal wait time T3_response              = 10
    GTP signal absolute max wait time (in seconds)= 70
    GTP max retry N3_request                      = 3
MCSA Parameters:
    MCSA Handle                                   = 0xFE000003
    MCSA Context                                  = 0x0
Tunnel Parameters:
    Tunnel Hold Down Timer                        = 70
    Tunnel MTU                                    = 1480
```

The following table describes the significant fields shown in the display.

Table 4: show gtp parameters Field Descriptions

Field	Description
GTP path echo interval	Interval, in seconds, that the GGSN waits for before resending echo responses.
GTP signal absolute max wait time T3_response	Interval, in seconds, that the GGSN waits for before responding to a T3 request.
GTP max retry N3_request	Maximum retry setting for N3 requests.
Tunnel MTU	Maximum transmission unit of a tunnel.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.
show subscriber session	Displays the summary of either authenticated or unauthenticated subscriber sessions.

show gtp pdp-context

To display the list of Packet Data Protocol contexts that are active on the Intelligent Wireless Access Gateway (iWAG) feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name (APN), International Mobile Subscriber Identity (IMSI), mobile subscriber address, Mobile Station International Subscriber Directory Number (MSISDN), or tunnel endpoint identifier (TEID), use the **show gtp pdp-context** command in the privileged EXEC mode.

show gtp pdp-context {**all**| **apn**| **imsi** *imsi-value*| **ms-address** *ip-address* [**detail**| **vrf** *vrf-name*]| **msisdn** *msisdn-value*| **teid-u** *teid-u value*}

Syntax Description

all	Displays detailed statistics pertaining to all the GTP Packet Data Protocol contexts.
apn	Displays GTP Packet Data Protocol contexts based on the APN.
imsi	Displays GTP Packet Data Protocol contexts based on the IMSI.
imsi-value	Value assigned to the IMSI.
ms-address	Displays GTP Packet Data Protocol contexts based on the mobile subscriber address.
ip-address	IP address assigned to the mobile subscriber.
detail	Displays detailed GTP Packet Data Protocol context information.
vrf	Specifies the virtual routing and forwarding (VRF) instance containing the remote address.
vrf-name	Name of the VRF instance.
msisdn	Displays GTP Packet Data Protocol contexts based on the MSISDN value.
msisdn-value	Value assigned to the MSISDN.
teid-u	Displays GTP Packet Data Protocol contexts based on the TEID value in the GPRS Tunnelling Protocol User Plane (GTP-U).
teid-u value	Value assigned to the TEID in the GTP-U.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

```
The following is sample output from the show gtp pdp-context
 command displaying detailed statistics pertaining to all the GTP Packet Data Protocol
contexts:
Router# show gtp pdp-context all
TEID-C    TEID-U    MS Addr         IMSI             GGSN Sig Addr   Fwd VRF     APN
0020F43F  0020F440  192.168.10.5    262020000000485  192.170.10.2    default starent.com
```

The following is sample output from the **show gtp pdp-context** command displaying the GTP Packet Data Protocol contexts based on APN:

```
Router# show gtp pdp-context apn 1
TEID-C    TEID-U    MS Addr         IMSI             GGSN Sig Addr   Fwd VRF     APN
0020F43F  0020F440  192.168.10.5    262020000000485  192.170.10.2    default starent.com
```

The following is sample output from the **show gtp pdp-context** command displaying the GTP Packet Data Protocol contexts based on IMSI:

```
Router# show gtp pdp-context imsi 262020000000485
TEID-C    TEID-U    MS Addr         IMSI             GGSN Sig Addr   Fwd VRF     APN
0020F43F  0020F440  192.168.10.5    262020000000485  192.170.10.2    default starent.com
    current time         : Oct 12 2012 11:57:22
    PDP State            : IWAG_GTP_PDP_IN_SERVICE
    Internal Flags       : 0x40011
    Fwd VRF              : default
    Trans VRF            : default
    user_name (IMSI)     : 262020000000485      MS address  : 192.168.10.5
    MS International PSTN/ISDN Number (MSISDN): 123456789
    control teid local   : 0x0020F43F
    control teid remote  : 0x000F4240
    data teid local      : 0x0020F440
    data teid remote     : 0x001E8480
    primary pdp          : Y
    nsapi                : 5
    signal_sequence      : 0
    ggsn_addr_signal     : 192.170.10.2
    ggsn_addr_data       : 192.170.10.2
    default-gw           : 192.168.10.1         prefix-len  : 16
    dhcp-addr            : 192.168.10.1         dhcp-lease  : 30000
    DNS-addr             : 0.0.0.0
    mcsa ctx             : 0x20000A5
    pdp_create_time      : Oct 12 2012 11:43:08
    pdp_setup_time       : Oct 12 2012 11:43:19
    Requested QOS        : 2001F2004040004040100
    Negotiated QOS       : 2001F2004040004040100
    Virtual Interface    : IFNAME_GTP_VIF0
    Tunnel Interface     : Tunnel0
    Radio Access Technology type: WLAN

The following is sample output from the show gtp pdp-context
 command displaying the GTP Packet Data Protocol contexts based on mobile subscriber address:
Router# show gtp pdp-context ms-address 192.168.10.5
TEID-C    TEID-U    MS Addr         IMSI             GGSN Sig Addr   Fwd VRF     APN
0020F43F  0020F440  192.168.10.5    262020000000485  192.170.10.2    default starent.com
```

```
    current time         : Oct 12 2012 11:57:39
    PDP State            : IWAG_GTP_PDP_IN_SERVICE
    Internal Flags       : 0x40011
    Fwd VRF              : default
    Trans VRF            : default
    user_name (IMSI)     : 262020000000485      MS address  : 192.168.10.5
    MS International PSTN/ISDN Number (MSISDN): 123456789
    control teid local   : 0x0020F43F
    control teid remote  : 0x000F4240
    data teid local      : 0x0020F440
    data teid remote     : 0x001E8480
    primary pdp          : Y
    nsapi                : 5
    signal_sequence      : 0
    ggsn_addr_signal     : 192.170.10.2
    ggsn_addr_data       : 192.170.10.2
    default-gw           : 192.168.10.1         prefix-len  : 16
    dhcp-addr            : 192.168.10.1         dhcp-lease  : 30000
    DNS-addr             : 0.0.0.0
    mcsa ctx             : 0x20000A5
    pdp_create_time      : Oct 12 2012 11:43:08
    pdp_setup_time       : Oct 12 2012 11:43:18
    Requested QOS        : 2001F2004040004040100
    Negotiated QOS       : 2001F2004040004040100
    Virtual Interface    : IFNAME_GTP_VIF0
    Tunnel Interface     : Tunnel0
    Radio Access Technology type: WLAN
```

The following is sample output from the **show gtp pdp-context** command displaying the GTP Packet Data Protocol contexts based on an MSISDN value:

```
Router# show gtp pdp-context msisdn 123456789
TEID-C    TEID-U    MS Addr         IMSI             GGSN Addr       MSISDN
Fwd VRF     APN
0020F43F  0020F440  192.168.10.5    262020000000485  192.170.10.2    default    starent.com

    current time         : Oct 12 2012 11:58:02
    PDP State            : IWAG_GTP_PDP_IN_SERVICE
    Internal Flags       : 0x40011
    Fwd VRF              : default
    Trans VRF            : default
    user_name (IMSI)     : 262020000000485      MS address : 192.168.10.5
    MS International PSTN/ISDN Number (MSISDN): 123456789
    control teid local   : 0x0020F43F
    control teid remote  : 0x000F4240
    data teid local      : 0x0020F440
    data teid remote     : 0x001E8480
    primary pdp          : Y
    nsapi                : 5
    signal_sequence      : 0
    ggsn_addr_signal     : 192.170.10.2
    ggsn_addr_data       : 192.170.10.2
    default-gw           : 192.168.10.1         prefix-len  : 16
    dhcp-addr            : 192.168.10.1         dhcp-lease  : 30000
    DNS-addr             : 0.0.0.0
    mcsa ctx             : 0x20000A5
    pdp_create_time      : Oct 12 2012 11:43:09
    pdp_setup_time       : Oct 12 2012 11:43:19
    Requested QOS        : 2001F2004040004040100
    Negotiated QOS       : 2001F2004040004040100
    Virtual Interface    : IFNAME_GTP_VIF0
    Tunnel Interface     : Tunnel0
    Radio Access Technology type: WLAN
```

The following table describes the significant fields shown in the displays.

Table 5: show gtp pdp-context Field Descriptions

Field	Description
TEID-C	The TEID value of a GPRS Tunnelling Protocol Control Plane (GTP-C) message.

Field	Description
TEID-U	The TEID value of a GTP-U message.
MS Addr	IP address of the mobile station.
IMSI	IMSI for the Packet Data Protocol context.
GGSN Addr	IP address of the GGSN that is associated with the network-initiated procedure for this Packet Data Protocol context.
MSISDN	International Services Digital Network (ISDN) number of the mobile station.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.
show subscriber session	Displays the summary of either authenticated or unauthenticated subscriber sessions.

show gtp tunnel

To display tunnel-related information pertaining to the General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **show gtp tunnel** command in privileged EXEC mode.

show gtp tunnel Tunnel *tunnel-interface number*

Syntax Description

Tunnel	Specifies the GTP tunnel interface.
tunnel-interface number	Interface number assigned to the GTP tunnel.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show gtp tunne**l command:

```
Router# show gtp tunnel Tunnel0
LocalAddr        RemoteAddr       FwdVRF      TransVRF    UsageCount SeqNum    Checksum
192.170.10.1     192.170.10.2     default     default     1          Disabled  N
```

The following table describes the significant fields shown in the display.

Table 6: show gtp tunnel Field Descriptions

Field	Description
LocalAddr	IP address and port number of the local end of the GTP path.
RemoteAddr	IP address and port number of the remote end of the GTP path.
FwdVRF	Forwarding VRF value.
TransVRF	Transport VRF value.
UsageCount	Number of Packet Data Protocol counts.
SeqNum	Sequence number of the GTP packet.

Field	Description
Checksum	Checksum operations used to perform tunnelling.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.
show subscriber session	Displays the summary of either authenticated or unauthenticated subscriber sessions.

show platform subscriber template

To display the list of Intelligent Services Gateway (ISG) policy templates, use the **show platform subscriber template** command in the privileged EXEC mode.

show platform subscriber template [state]

Syntax Description

state	Specifies the state of ISG policy templating.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.10	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the show platform subscriber template command displaying the state of ISG policy templating:

```
Router# show platform software subscriber template state
Templating is turned ON, 1 template, 32000 sessions
```

show subscriber session

To display the summary of either authenticated or unauthenticated subscriber sessions, use the **show subscriber session** command in the privileged EXEC mode.

show subscriber session {**detailed| feature| identifier| uid| username**}

Syntax Description

detailed	Displays detailed session information.
feature	Displays specific feature information.
identifier	Specifies the session identifier.
uid	Displays session information based on unique ID.
username	Displays session information based on username.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

```
The following is sample output from the show subscriber session
 command:
Router# show subscriber session
Codes: Lterm - Local Term, Fwd - forwarded, unauth - unauthenticated,
authen - authenticated, TC Ct. - Number of Traffic Classes on the main session
Current Subscriber Information: Total sessions 1
Uniq ID Interface    State    Service     Up-time  TC Ct. Identifier
198     DHCP/IP      authen   Lterm       02:23:02 1      0001.0000.0001
The following is sample output from the show subscriber session
 command displaying detailed session information:
Router# show subscriber session detailed
Current Subscriber Information: Total sessions 1
-------------------------------------------------
Type: DHCP/IP, UID: 198, State: authen, Identity: 0001.0000.0001
IPv4 Address: 192.168.10.5
Session Up-time: 02:22:54, Last Changed: 02:22:54
Switch-ID: 5256
Policy information:
  Context 7F6F46F89740: Handle 9D000507
  AAA_id 00007C3E: Flow_handle 0
  Authentication status: authen
  Downloaded User profile, excluding services:
    username             0   "0001.0000.0001"
    service-type         0   5 [Outbound]
    reply-message        0   "Default "
```

```
  cisco-mn-service     0   1 [ipv4]
  cisco-mpc-protocol-i 0   2 [gtpv1]
  cisco-service-select 0   "starent.com"
  cisco-msisdn         0   "49123456789"
  imsi                 0   "262020000000485"
  tunnel-if-handle     0   <bad format for type>(1214)
  if-adjacency-handle  0   <bad format for type>(1216)
  teid-enable          0   True
  cisco-uplink-gre-key 0   2000000 (0x1E8480)
  cisco-downlink-gre-k 0   2159680 (0x20F440)
  cisco-mn-service     0   0 [none]
  pmip6-encap-type     0   4 [gre-in-ipv6]
  wins-server-primary  0   192.168.10.5
  default-ipv4-gateway 0   192.168.10.1
  primary-dns          0   192.165.1.1
  dhcp-server          0   192.168.10.1
  wins-server-secondar 0   255.255.0.0
  default-ipv4-gateway 0   192.168.10.1
  lease-duration       0   30000 (0x7530)
  default-gw-mac       0   ""
  domain-name          0   ""
  domain-name          0   ""
Downloaded User profile, including services:
  traffic-class        0   "input access-group name ip_tc1_in_ipv4_acl priority 1"
  traffic-class        0   "output access-group name ip_tc1_out_ipv4_acl priority 1"
  idletime             0   10800 (0x2A30)
  username             0   "0001.0000.0001"
  service-type         0   5 [Outbound]
  reply-message        0   "Default"
  cisco-mn-service     0   1 [ipv4]
  cisco-mpc-protocol-i 0   2 [gtpv1]
  cisco-service-select 0   "starent.com"
  cisco-msisdn         0   "49123456789"
  imsi                 0   "262020000000485"
  tunnel-if-handle     0   <bad format for type>(1214)
  if-adjacency-handle  0   <bad format for type>(1216)
  teid-enable          0   True
  cisco-uplink-gre-key 0   2000000 (0x1E8480)
  cisco-downlink-gre-k 0   2159680 (0x20F440)
  cisco-mn-service     0   0 [none]
  pmip6-encap-type     0   4 [gre-in-ipv6]
  wins-server-primary  0   192.168.10.5
  default-ipv4-gateway 0   192.168.10.1
  primary-dns          0   192.165.1.1
  dhcp-server          0   192.168.10.1
  wins-server-secondar 0   255.255.0.0
  default-ipv4-gateway 0   192.168.10.1
  lease-duration       0   30000 (0x7530)
  default-gw-mac       0   ""
  domain-name          0   ""
  domain-name          0   ""
Config history for session (recent to oldest):
  Access-type: DHCP Client: SM
   Policy event: Service Selection Request
    Profile name: 0001.0000.0001, 2 references
      username             0   "0001.0000.0001"
      service-type         0   5 [Outbound]
      reply-message        0   "Default"
      cisco-mn-service     0   1 [ipv4]
      cisco-mpc-protocol-i 0   2 [gtpv1]
      cisco-service-select 0   "starent.com"
      cisco-msisdn         0   "49123456789"
      imsi                 0   "262020000000485"
      tunnel-if-handle     0   <bad format for type>(1214)
      if-adjacency-handle  0   <bad format for type>(1216)
      teid-enable          0   True
      cisco-uplink-gre-key 0   2000000 (0x1E8480)
      cisco-downlink-gre-k 0   2159680 (0x20F440)
      cisco-mn-service     0   1 [ipv4]
      pmip6-encap-type     0   4 [gre-in-ipv6]
      wins-server-primary  0   192.168.10.5
      default-ipv4-gateway 0   192.168.10.1
      primary-dns          0   192.165.1.1
```

```
        dhcp-server          0   192.168.10.1
        wins-server-secondar 0   255.255.0.0
        default-ipv4-gateway 0   192.168.10.1
        lease-duration       0   30000 (0x7530)
        default-gw-mac       0   ""
        domain-name          0   ""
        domain-name          0   ""
    Access-type: DHCP Client: SM
     Policy event: Service Selection Request (Service)
      Profile name: ip_tc1_ipv4_srvc1, 3 references
        password             0   <hidden>
        username             0   "ip_tc1_ipv4_srvc1"
        traffic-class        0   "input access-group name ip_tc1_in_ipv4_acl priority 1"
        traffic-class        0   "output access-group name ip_tc1_out_ipv4_acl priority 1"
        idletime             0   10800 (0x2A30)
  Active services associated with session:
    name "ip_tc1_ipv4_srvc1", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map ctrl_pmap
      condition always event session-start
        1 service-policy type service name ip_tc1_ipv4_srvc1
        10 authorize identifier mac-address
Classifiers:
Class-id    Dir   Packets    Bytes                 Pri.  Definition
0           In    155803     44236245              0    Match Any
1           Out   0          0                     0    Match Any
60          In    0          0                     1    Match ACL ip_tc1_in_ipv4_acl
61          Out   0          0                     1    Match ACL ip_tc1_out_ipv4_acl
Features:
Idle Timeout:
Class-id   Dir  Timeout value   Idle-Time            Source
61         Out  10800           02:22:54             ip_tc1_ipv4_srvc1
Forced Flow Routing:
Class-id   FFR Tunnel Details Source
0
Tunnel-If-Handlle: 44
Adj-Handle: 7F6F43670A18
TEID Enable: TRUE
Upstream Key: 2000000
Downstream Key: 2159680

1
Configuration Sources:
Type  Active Time  AAA Service ID  Name
SVC   02:22:54     -               ip_tc1_ipv4_srvc1
USR   02:22:54     -               Peruser
INT   02:22:54     -               GigabitEthernet1/3/3
```

The following table describes the significant fields shown in the displays.

Table 7: show subscriber session Field Descriptions

Field	Description
lease-duration	Length of time for which the allocated IP address is valid.
domain-name	Specifies the domain name of the GTP.
default-gw-mac	MAC address of the default gateway, if configured.
dhcp-server	IP address of the Dynamic Host Configuration Protocol (DHCP) server.
primary-dns	IP address of the primary Domain Name System (DNS) server.

Field	Description
wins-server-primary	IP address of the primary Windows Internet Naming Service (WINS) server.
wins-server-secondar	IP address of the secondary WINS server.
cisco-msisdn	Displays the Cisco Mobile Station International Subscriber Directory Number (MSISDN) value for the subscriber session.
imsi	Displays the International Mobile Subscriber Identity (IMSI) value for the subscriber session.

Related Commands

Command	Description
debug gtp	Enables debugging of the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
gtp	Configures the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp apn	Displays detailed statistics pertaining to the access points on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and the Packet Data Protocol count information for each APN.
show gtp mcsa statistics	Displays detailed statistics pertaining to mobile client service abstraction on the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp parameters	Displays the summary of the GTP parameters of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp path	Displays the path information for the GTP of the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers.
show gtp pdp-context	Displays the list of Packet Data Protocol contexts that are active on the iWAG feature in the Cisco ASR 1000 Series Aggregation Services Routers, and are based on Access Point Name, IMSI, mobile subscriber address, MSISDN, or TEID.

Command	Description
show gtp tunnel	Displays tunnel-related information pertaining to the GTP.

vrfid (proxy mobile IPv6)

To specify a Virtual Private Network (VPN) Route Forwarding (VRF) for a local mobility access (LMA) peer that is configured under a mobile access gateway (MAG), use the **vrfid** command in MAG-LMA configuration mode. To disassociate a VRF from an LMA peer that is configured under a MAG, use the **no** form of this command.

vrfid

no vrfid

Syntax Description

This command has no arguments or keywords.

Command Default

No VRF is specified for an LMA peer that is configured under a MAG.

Command Modes

MAG-LMA configuration mode (config-ipv6-pmipv6mag-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	The command was introduced.

Usage Guidelines

This command is not supported in standalone MAG configuration. Use this command only when a MAG is configured to coexist with the Intelligent Services Gateway (ISG). Configure a VRF routing table instance using **vrf definition** command prior to using the **vrfid** command.

Examples

The following example shows how to specify a VRF for an LMA peer that is configured under a MAG:

```
Device# enable
Device# configuration terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# rd 100:20
Device(config-vrf)# exit
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# lma lma1
Device(config-ipv6-pmipv6mag-lma) vrfid vrf1
Device(config-ipv6-pmipv6mag-lma) end
```

Related Commands

Command	Description
vrf definition	Configures a VRF table instance.