Direct Tunnel for 3G Networks

This chapter briefly describes the 3G UMTS direct tunnel (DT) feature, indicates how it is implemented on various systems on a per call basis, and provides feature configuration procedures.

Products supporting direct tunnel include:

- 3G devices (per 3GPP TS 23.919 v8.0.0):
  - the Serving GPRS Support Node (SGSN)
  - the Gateway GPRS Support Node (GGSN)

Important Direct tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

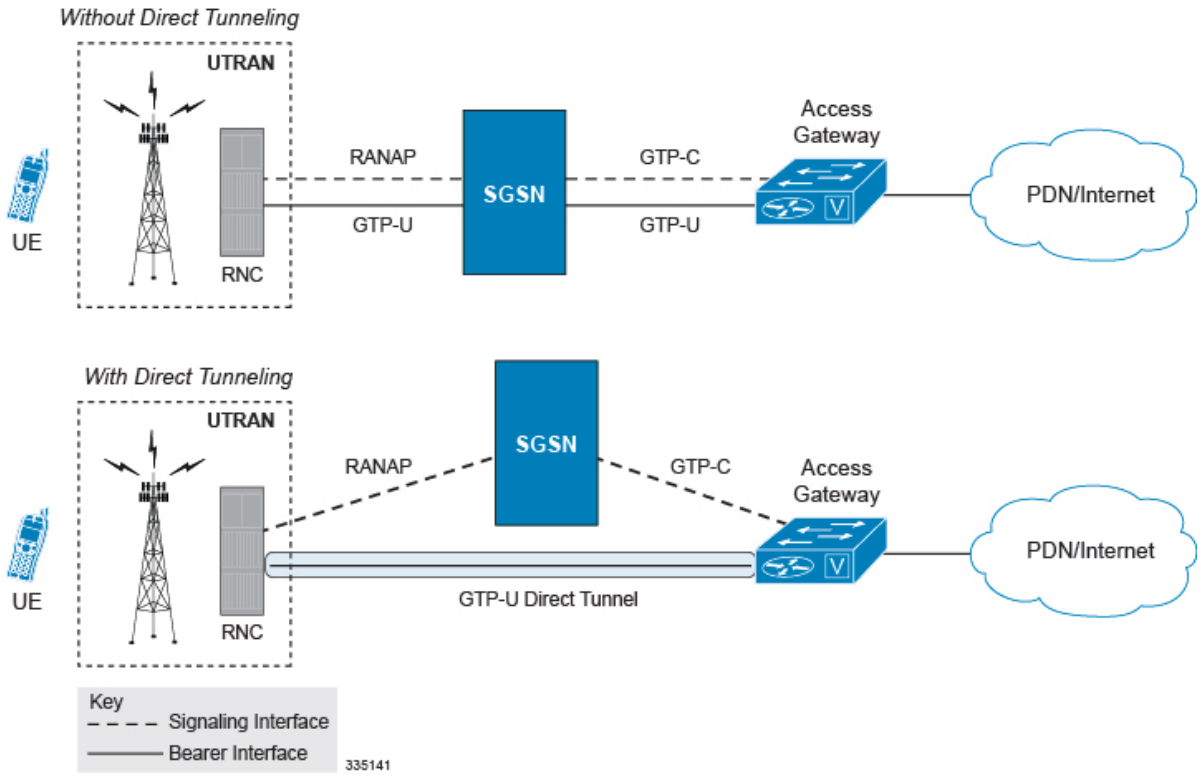
The SGSN determines if setup of a direct tunnel is allowed or disallowed. Currently, the SGSN is the only product that provide configuration commands for this feature. All other products that support direct tunnel do so by default.

Direct Tunnel Feature Overview

The direct tunnel architecture allows the establishment of a direct *user plane* (GTP-U) tunnel between the radio access network equipment (RNC) and a GGSN.

Once a direct tunnel is established, the SGSN continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDP context activation.

Figure 1: GTP-U Direct Tunneling

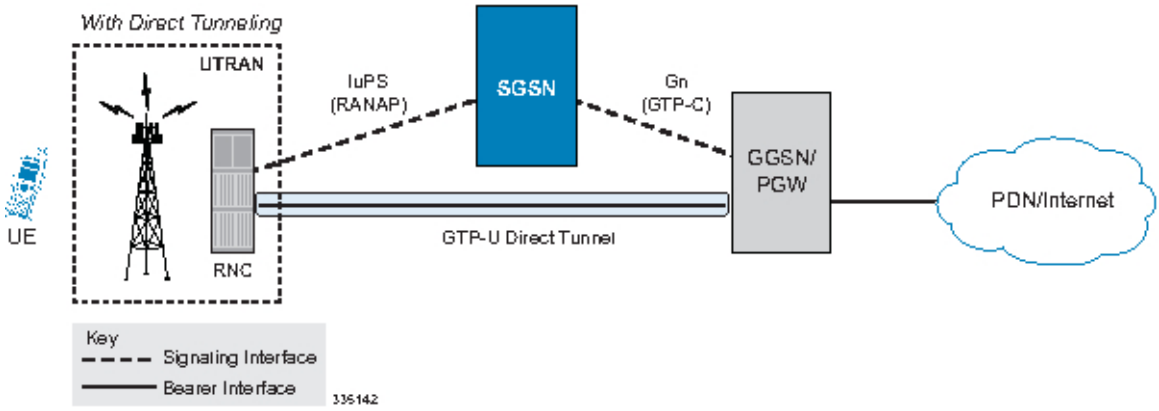


A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN to handle the user plane processing.

A direct tunnel is achieved upon PDP context activation in the following ways:

- **Gn/Gp Interface towards GGSN:** The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN, using an Updated PDP Context Request toward the GGSN or the GGSN service of a collocated GGSN/P-GW.

Figure 2: Direct Tunneling - 3G Network

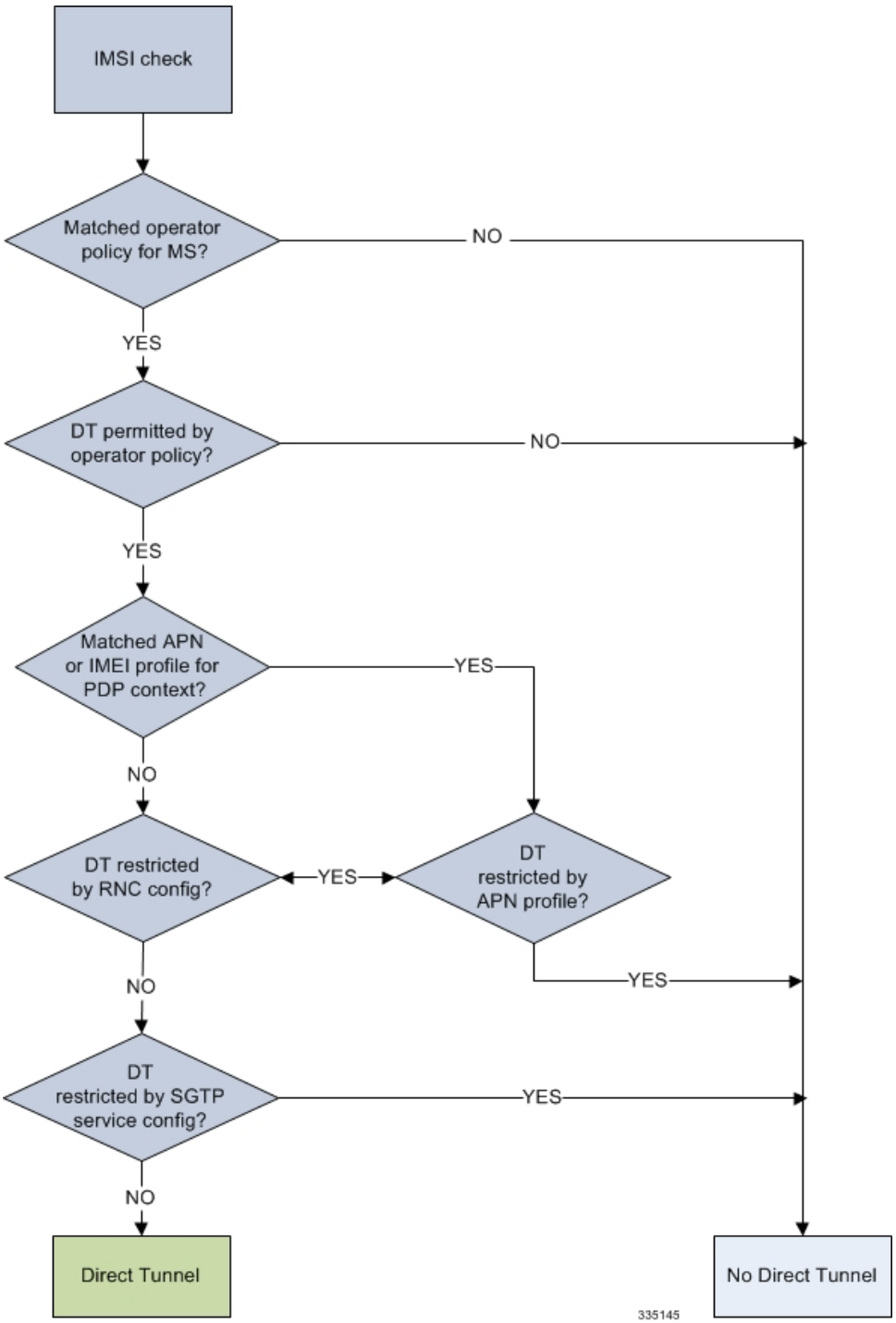


- **Gn/Gp Interface towards P-GW** When Gn/Gp interworking with pre-release 8 (3GPP) SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality. The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the collocated PGW, using an Update PDP Context Message toward the GGSN/P-GW.

A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. Hence, deployment requires highly scalable GGSNs since the volume and frequency of Update PDP Context messages to the GGSN will increase substantially. The SGSN platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

The following figure illustrates the logic used within the SGSN to determine if a direct tunnel will be setup.

Figure 3: Direct Tunneling - Establishment Logic



Direct Tunnel Configuration

The following configurations are provided in this section:

- Configuring Direct Tunnel Support on the SGSN, on page 5

The SGSN direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the system operator policy named *default*.

By default, direct tunnel support is

- *disallowed* on the SGSN
- *allowed* on the GGSN/P-GW

Important If direct tunnel is allowed in the *default* operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel *allowed*.

For more information about operator policies and configuration details, refer to *Operator Policy*.

Configuring Direct Tunnel Support on the SGSN

The following is a high-level view of the steps, and the associated configuration examples, to configure the SGSN to setup a direct tunnel.

Before beginning any of the following procedures, you must have completed (1) the basic service configuration for the SGSN, as described in the *Cisco ASR Serving GPRS Support Node Administration Guide*, and (2) the creation and configuration of a valid operator policy, as described in the *Operator Policy* chapter in this guide.

Step 1 Configure the SGSN to setup GTP-U direct tunnel between an RNC and an access gateway by applying the example configuration presented in the Enabling Setup of GTP-U Direct Tunnels, on page 6.

Step 2 Configure the SGSN to allow GTP-U direct tunnels to an access gateway, for a call filtered on the basis of the APN, by applying the example configuration presented in the Enabling Direct Tunnel per APN , on page 6.

Important It is only necessary to complete either step 2 or step 3 as a direct tunnel can not be setup on the basis of call filtering matched with both an APN profile and an IMEI profile.

Step 3 Configure the SGSN to allow GTP-U direct tunnels to a GGSN, for a call filtered on the basis of the IMEI, by applying the example configuration presented in the Enabling Direct Tunnel per IMEI , on page 7.

Step 4 Configure the SGSN to allow GTP-U direct tunnel setup from a specific RNC by applying the example configuration presented in the Enabling Direct Tunnel to Specific RNCs, on page 7.

Step 5 *(Optional)* Configure the SGSN to disallow direct tunnel setup to a single GGSN that has been configured to allow it in the APN profile. This command allows the operator to restrict use of a GGSN for any reason, such as load balancing. Refer to the **direct-tunnel-disabled-ggsn** command in the *SGTP Service Configuration Mode* chapter of the *Command Line Interface Reference*.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 7 Check that your configuration changes have been saved by using the sample configuration found in the Verifying the SGSN Direct Tunnel Configuration, on page 9.

Enabling Setup of GTP-U Direct Tunnels

The SGSN determines whether a direct tunnel can be setup and by default the SGSN doesn't support direct tunnel.

Example Configuration

Enabling direct tunnel setup on an SGSN is done by configuring direct tunnel support in a call-control profile.

```
config
  call-control-profile policy_name
    direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]
    end
```

Notes:

- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Beginning with Release 19.3.5, **to-ggsn** and **to-sgw** options have been added to the **direct-tunnel** command to enable the operator to select the interface the SGSN will use for its direct tunnel. For a collocated Gn/GP-SGSN and an S4-SGSN,
  - Use the keyword **attempt-when-permitted** without a filter to enable both interface types: GTP-U towards the GGSN and S12 towards the SGW.
  - Use the keyword **attempt-when-permitted** with the **to-ggsn** keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
  - Use the keyword **attempt-when-permitted** with the **to-sgw** keyword filter to enable only the S4's S12 interface between the RNC and the SGW.
- To remove the direct tunnel settings from the configuration, use the following command: **direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]**
- Direct tunnel is allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel per APN

In each operator policy, APN profiles are configured to connect to one or more GGSNs and to control the direct tunnel access to that GGSN based on call filtering by APN. Multiple APN profiles can be configured per operator policy.

By default, APN-based direct tunnel functionality is *allowed* so any existing direct tunnel configuration must be removed to return to default and to ensure that the setup has not been restricted.

Example Configuration

The following is an example of the commands used to ensure that direct tunneling, to a GGSN(s) identified in the APN profile, is enabled:

```
config
  apn-profile profile_name
    remove direct tunnel
    end
```

Notes:

- An APN profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Direct tunnel is now allowed for the APN but will only setup if also allowed on the RNC.

Enabling Direct Tunnel per IMEI

Some operator policy filtering of calls is done on the basis of international mobile equipment identity (IMEI) so the direct tunnel setup may rely upon the feature configuration in the IMEI profile.

The IMEI profile basis its permissions for direct tunnel on the RNC configuration associated with the IuPS service.

By default, direct tunnel functionality is *enabled* for all RNCs.

Example Configuration

The following is an example of the commands used to enable direct tunneling in the IMEI profile:

```
config
  imei-profile profile_name
    direct-tunnel check-iups-service
    end
```

Notes:

- An IMEI profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Direct tunnel is now allowed for calls within the IMEI range associated with the IMEI profile but a direct tunnel will only setup if also allowed on the RNC.

Enabling Direct Tunnel to Specific RNCs

SGSN access to radio access controllers (RNCs) is configured in the IuPS service.

Each IuPS service can include multiple RNC configurations that determine communications and features depending on the RNC.

By default, direct tunnel functionality is *enabled* for all RNCs.

Example Configuration

The following is an example of the commands used to ensure that restrictive configuration is removed and direct tunnel for the RNC is enabled:

```
config
  context ctx_name
    iups-service service_name
      rnc id rnc_id
        default direct-tunnel
        end
```

Notes:

- An IuPS service must have been previously created, and configured.
- An RNC configuration must have been previously created within an IuPS service configuration.
- Command details for configuration can be found in the *Command Line Interface Reference*.

Restricting Direct Tunnels

By default, GGSNs and RNCs are assumed to be capable of direct tunneling. The SGSN's direct tunnel functionality can be fine tuned to:

Disable direct tunneling for a specified GGSN(s). GGSNs are identified by their IP address, either IPv4 or IPv6. The command listed below can be repeated to disable direct tunneling for multiple GGSNs, thereby creating a 'disabled GGSN' list. Checking for a GGSN that is direct-tunnel-disabled is actually the last step in the PDP Activation procedure.

```
config
  context context_name
    sgtp-service service_name
      direct-tunnel-disabled-ggsn ip_address
      end
```

Restrict direct tunneling for an entire APN. The following configuration scenario prohibits direct tunneling setup to a GGSN for an entire APN - the APN associated with the profile.

```
config
  apn-profile profile_name
    direct-tunnel not-permitted-by-ggsn
    end
```

Restrict direct tunneling by a specific RNC. The following configuration scenario restricts the SGSN from attempting to setup a direct tunnel when a call originates from a specific RNC.

```
config
  context context_name
    iups-service service_name
      rnc id rnc_id
        direct-tunnel not-permitted-by-rnc
```

```
end
```

Verifying the SGSN Direct Tunnel Configuration

Enabling the setup of a GTP-U direct tunnel on the SGSN is not a straight forward task. It is controlled by an operator policy with related configuration in multiple components. Each of these component configurations must be checked to ensure that the direct tunnel configuration has been completed. You need to begin with the operator policy itself.

Verifying the Operator Policy Configuration

For the feature to be enabled, it must be allowed in the call-control profile, and the call-control profile must be associated with an operator policy. As well, either an APN profile or an IMEI profile must have been created/configured and associated with the same operator policy. Use the following command to display and verify the operator policy and the association of the required profiles:

show operator-policy full name *policy_name*

The output of this command displays profiles associated with the operator policy. The output also includes some values just as illustrative examples:

```
show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1
Call Control Profile Name               : ccprofile1
  Validity                              : Valid
IMEI Range 99999999999990  to 99999999999995
  IMEI Profile Name                     : imeiprofile1
  Validity                              : Invalid
APN NI homers1
  APN Profile Name                      : apnprofile1
  Validity                              : Valid
APN NI visitors2
  APN Profile Name                      : apnprofile2
  Validity                              : Invalid
```

Notes:

- Validity refers to the status of the profile. Valid indicates that profile has been created and associated with the policy. Invalid means only the name of the profile has been associated with the policy.
- The operator policy itself will only be valid if one or more IMSI ranges have been associated with it - refer to the *Operator Policy* chapter, in this guide, for details.

Verifying the Call-Control Profile Configuration

Use the following command to display and verify the direct tunnel configuration for the call-control profiles:

show call-control-profile full name *profile_name*

The output of this command displays all of the configuration, including direct tunnel for the specified call-control profile.

```
Call Control Profile Name = ccprofile1
...
Re-Authentication                   : Disabled
Direct Tunnel                       : Not Restricted
GTPU Fast Path                      : Disabled
...
```

Verifying the APN Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the APN profile:

show apn-profile full name *<profile_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified APN profile.

```
Call Control Profile Name = apnprofile1
...
IP Source Validation                          : Disabled
Direct Tunnel                                 : Not Restricted
Service Restriction for Access Type > UMTS    : Disabled
...
```

Verifying the IMEI Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the IMEI profile:

show imei-profile full name *<profile_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified IMEI profile.

```
IMEI Profile Name = imeiprofile1
Black List                          : Disabled
GGSN Selection                      : Disabled
Direct Tunnel                       : Enabled
```

Verifying the RNC Configuration

Use the following command to display and verify the direct tunnel configuration in the RNC configuration:

show iups-service name *service_name*

The output of this command displays all of the configuration, including direct tunnel for the specified IuPS service.

```
IService name              : iups1
...
Available RNC:
   Rnc-Id                        : 1
   Direct Tunnel                 : Not Restricted
```