Configuring the SaMOG Gateway

This chapter provides configuration instructions for the SaMOG (S2a Mobility Over GTP) Gateway. Information about the commands in this chapter can be found in the *Command Line Interface Reference.*

Configuring the System to Perform as a SaMOG Gateway

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a SaMOG Gateway in a test environment.

Required Information

The following sections describe the minimum amount of information required to configure and make the SaMOG Gateway operational in the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

The following table lists the information that is required to configure the SaMOG Gateway context and service.

Table 1: Required Information for SaMOG Configuration

Required Information	Description
SaMOG Context and MRME, CGW and SaMOG Service Configuration	
SaMOG context name	The name of the SaMOG context, which can be from 1 to 79 alpha and/or numeric characters.
MRME service name	The name of the MRME service, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IP address to which you want to bind the MRME service.
context DNS	The name of the context to use for PGW DNS.
IPV4_address/subnetmask	The IPv4 address and subnetmask for the destination RADIUS client the MRME service will use.

Required Information	Description
Key	The name of the encrypted key for use by the destination RADIUS server.
Port Number	The port number for RADIUS disconnect messages.
IPv4 address	The IPv4 address of the RADIUS client
Key	The encrypted key name for use by the RADIUS client.
Port	The port number used by the RADIUS client.
CGW service name	The name of the CGW service, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IPv4 address to which the CGW service will bind.
Egress EGTP service name	The name of the egress EGTP service that the CGW service will use. This name must match the name of the EGTP service configured later in this procedure.
Timeout	The session delete delay timeout setting for use by CGW service.
SaMOG service name	The name of the SaMOG service, which can be from 1 to 63 alpha and/or numeric characters.
MRME service name	The name of the MRME service to associate with this SaMOG service. This is the MRME service name configured previously in this procedure.
CGW service name	The name of the CGW service to associate with this SaMOG service. This is the CGW service name configured previously in this procedure.
Subscriber map name	The subscriber map name to associate with the SaMOG service. This name must match the subscriber map name configured later in this procedure.
LTE Policy Configuration	
Subscriber map name	The name of the subscriber map to associate with the LTE policy, which can be from which can be from 1 to 64 alpha and/or numeric characters.
Precedence priority	Specifies the prcedence for the subscriber map. Must be an integer from 1 to 1024.
Service criteria type	Specifies the service criteria that must be matched for the subscriber map. Must be one of **imsi**, **service-plmnid** or **all**.
MCC number	The Mobile Country Code for use in this LTE policy.

Required Information	Description
MNC	The Mobile Network code for use in this LTE policy.
Operator policy name	The name of the operator policy use with the subscriber map, which can be from 1 to 64 alpha and/or numeric characters.
TAI mgmt db name	The name of the Tracking Area Identifier database for use with the LTE policy, which can be from 1 to 64 alpha and/or numeric characters.
GTPU and EGTP Service Configuration	
SaMOG context name	The name of the SaMOG context configured previously.
EGTP service name	The name for this EGTP service, which can be from 1 to 63 alpha and/or numeric characters.
EGTP service name	The name of the EGTP service name that you want to associate with the GTPU service. This is the EGTP service name configured previously.
IPv4 address	The IPv4 address to which you want to use to bind the EGTP service to the GTPU service.
GTPU service name	The name of the GTPU service, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IP address to which the GTPU service will bind.
AAA and Diameter Endpoint Configuration	
AAA context name	The name assigned to the AAA context, which can be from 1 to 79 alpha and/or numeric characters.
AAA interface name	The name assigned to the AAA interface, which can be from 1 to 79 alpha and/or numeric characters.
IPv4 address/subnetmask	The primary IPv4 address and subnetmask for use by the AAA interface.
IPv4 address subnetmask	The secondary IPv4 address and subnetmask for use by the AAA interface.
SaMOG context name	The name of the SaMOG context configured earlier.
AAA DIAMETER STa1 group name	The primary AAA group name for use over the STa interface, which can be from 1 to 63 alpha and/or numeric characters.
DIAMETER endpoint name	The DIAMETER authentication endpoint name for use with this AAA group.

Required Information	Description
AAA DIAMETER STa2 group name	The secondary AAA group name for use over the STa interface, which can be from 1 to 63 alpha and/or numeric characters.
DIAMETER endpoint name	The DIAMETER authentication endpoint name for use with the secondary AAA group.
AAA Accounting Group Name	The name of the AAA Accounting group, which can be from 1 to 63 alpha and/or numeric characters.
Diameter authentication dictionary	The name of the Diameter dictionary used for authentication. This must be configured as the aaa-custom13 dictionary.
DIAMETER endpoint name	The name of the DIAMETER endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server.
STa endpoint name	The name of the DIAMETER endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server.
Origin real name	Name of the local Diameter realm, which can be a a string from 1 to 127 alpha and/or numeric characters.
Origin host STa endpoint IPv4 address	The IPv4 address of the origin host STa endpoint.
IPv4 address	The IPv4 address used for the origin host STa endpoint.
Port	The port used for the origin host STa endpoint.
Peer name	The name of the Diameter peer, which can be from 1 to 63 alpha and/or numeric characters.
SaMOG realm name	The name of the peer Diameter realm, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IPv4 address for the peer STa endpoint.
Port	The port used for the peer STa endpoint.
DNS Configuration	
DNS context name	The name of the context in which DNS will be configured, which can be from 1 to 79 alpha and/or numeric characters.
DNS interface name	The name of the DNS interface, which can be from 1 to 79 alpha and/or numeric characters.
IPv4 address	The IPv4 address of the DNS server.

Required Information	Description
IP name server IP address	The IP name server IPv4 address.
DNS client	The name of the DNS client, which can be from 1 to 63 alpha and/or numeric characters.
IPv4 address	The IPv4 address to which you want to bind the DNS client service.
Configuring and Binding the Interfaces	
SaMOG service Interface port/slot	The slot and port number to which you want to bind the SaMOG service.
GTP SaMOG interface name and context	The SaMOG interface and context name that will be bound to the SaMOG interface port/slot.
STa Accounting service interface port/slot	The slot and port number to which you want to bind the STa accounting interface.
STa Accounting service name and context	The name and context name of the STa accounting interface that you want to bind to the STa accounting port/slot.
DNS service Interface slot/port	The slot and port number that to which you want to bind the DNS service.
DNS service interface name and context.	The name and context name that you want to bind to the DNS interface slot/port.
Radius PMIP-side service interface port/slot.	The slot and port number to which you want to bind the PMIP-side RADIUS interface.
Radius PMIP-side service interface name and context.	The name and context name of the PMIP side RADIUS interface you want to bind to the RADIUS interface port/slot.
Radius SaMOG-side service interface port/slot.	The slot and port number to which you want to bind the SaMOG-side RADIUS interface.
GTPU interface port/slot.	The slot and port number to which you want to bind the GTPU-interface.

SaMOG Gateway Configuration

The high-level steps below summarize the SaMOG gateway configuration tasks. Steps 1 through 8 are mandatory. Steps 8 through 11 are optional. Note that the SaMOG Gateway is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, see "Managing License Keys" in the *System Administration Guide.*

Step 1 Set system configuration parameters such as activating PSC2s, ports, and enabling session recovery by following the configuration examples in the *System Administration Guide*.

Step 2 Create the SaMOG context by applying the example configuration in Creating the SaMOG Gateway Context , on page 6.

Step 3 Configure the MRME, CGW, and SaMOG services by applying the example configuration in Configuring the MRME, CGW and SaMOG Services, on page 7.

Step 4 Configure the LTE policy by applying the example configuration in Configuring the LTE Policy, on page 8.

Step 5 Create the GTPU and EGTP services by applying the example configuration in Configuring the GTPU and EGTP Services, on page 8.

Step 6 Create MAG services for a PMIPv6-based S2a interface by applying the example configuration in Configuring MAG Services, on page 9.

Step 7 Optional. Configure the IP over GRE (IPoGRE) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration in Configuring IPoGRE, on page 9.

Step 8 Optional. Configure the IP over VLAN (IPoVLAN) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration in Configuring IPoVLAN, on page 10.

Step 9 Create and configure the AAA group for Diameter and AAA authentication and accounting by applying the example configuration in Configuring AAA, on page 11.

Step 10 Configure the GTPP group consisting of the GTPP dictionary and CDR attributes, to be used for SGW and SGSN CDRs, and associate the GTPP group to the SaMOG Call Control Profile by applying the example configuration in Configuring GTPP Dictionary and CDR Attributes, on page 11.

Step 11 Configure the DNS service by applying the example configuration in Configuring DNS, on page 12.

Step 12 Optional. Enable Local breakout for an APN by applying the example configuration in Configuring Local Breakout, on page 12.

Step 13 Optional. Enable web-based authorization by applying the example configuration in Configuring Web-based Authorization, on page 15.

Step 14 Configure and bind interfaces to the relevant interfaces by applying the example configuration in Configuring and Binding the Interfaces, on page 18.

Step 15 Optional. Enable event logging by applying the example configuration in Enabling Logging, on page 18.

Step 16 Optional. Enable the sending of CGW and SaMOG SNMP traps by applying the example configuration in Enabling SNMP Traps, on page 19.

Step 17 Optional. Configure the system to gather and transfer bulk statistics by applying the example configuration in Configuring Bulk Statistics, on page 19.

Step 18 Save the completed configuration by following the instructions in Saving the Configuration, on page 20.

Creating the SaMOG Gateway Context

Create the context in which the SaMOG service will reside. The MRME, CGW, SaMOG and other related services will be configured in this context. Create the SaMOG context by applying the configuration example below.

```
config
    context  samog_context_name
    end
```

Configuring the MRME, CGW and SaMOG Services

The MRME and CGW services provide the SaMOG functionality. They must be configured in the SaMOG context and then associated with a SaMOG service name. Configure the MRME, CGW, and SaMOG services by applying the example configuration below.

```
            context context_name
                twan-profile twan_profile_name
                    radius client {  ipv4/ipv6_address [/mask ] } [ encrypted
 ] key value [ disconnect-message [ dest-port destination_port_number ] ] [
dictionary { custom70 | custom71 } ]
                    ue-address [ dhcp | twan ]
            exit
            mrme-service  mrme_service_name
# Release 18 and earlier:
                  bind address   ip4_address
# Release 19 and later:
                bind { ipv4-address  ipv4_address [ ipv6-address ipv6_address
 ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }
                  associate twan-profile twan_profile_name
                  dns-pgw context dns
 radius client  ip4_address/subnetmask encrypted key key  disconnect-message
dest-port  port_no
                  exit
            cgw-service  cgw_service_name
                bind { ipv4-address  ipv4_address [ ipv6-address ipv6_address
 ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }
                  associate egress-egtp_service egress-egtp_service_name
                  revocation enable
                  session-delete-delay timeout  timeout_msecs
                  exit
            samog-service samog_service_name
 associate mrme-service  mrme_service_name
                  assoicate cgw-service  cgw_service_name
                  associate subscriber-map  subscriber_map_name
                  associate dhcp-service  dhcp_service_name [ level { system
 | user } ]
                 # Associate a DHCPv6 service
                  associate dhcpv6-service  dhcpv6_service_name
                  exit
```

Important Configure the custom71 dictionary when Cisco WLC is used with PMIPv6 as the access-type. Configuring the custom71 dictionary enables attributes like the UE's permanent identity (NAI), subscribed APN, network protocol (PMIPv6), and LMA address (CGW service's bind address) to be sent in the Cisco Vendor-specific attributes to WLC. The WLC uses this information to build the PMIPv6 PBU to the SaMOG gateway when the **aaa-override** option is enabled on the Cisco WLC. These attributes are not sent when the custom70 dictionary is configured.

Notes:

- Use the **ue-address** command to configure Layer 3 IP access-type only.

- When the **associate dhcpv6-service** *dhcpv6_service_name* is configured, SaMOG will use the bind address configured under the DHCPv6 Service Configuration Mode for DHCPv6 server functionality.

Configuring the LTE Policy

Configure the LTE policy by applying the example configuration below.

```
config
      operator-policy policy-name
            apn network-identifier  apn_net_id apn-profile apn_profile_name
            associate call-control-profile   profile_id
            exit
      call-control-profile profile_name
            accounting mode gtpp
            authenticate context context_name aaa-group aaa_group_name
            accounting context context_name aaa-group aaa_group_name
            accounting context context_name gtpp-group gtpp_group_name
            assocaite accounting-policy  policy_name
            exit
      apn-profile profile_name
            accounting mode none
            local-offload
            address-resolution-mode local
            pgw-address IP_address
            qos default-bearer qci qci_id
            qos default-bearer arp arp_value preemption-capability may
vulnerability not-preemptable
            qos apn-ambr max-ul mbr-up max-dl mbr-dwn
            pdp-type-ipv4v6-override ipv4
            virtual-mac { mac_address | violation drop }
            twan default-gateway ipv4/ipv6_address/mask
            exit
      lte-policy
            subscriber-map   subscriber_map_name
                  precedence precedence_priority  match-criteria
service_criteria_type  mcc  mcc_number  mnc  mnc_number  operator-policy-name
operator_policy_name
                  precedence precedence_priority  match-criteria
service_criteria_type  operator-policy-name  operator_policy_name
                  exit
            tai-mgmt-db  tai_mgmt_db_name
           exit
```

Configuring the GTPU and EGTP Services

Configure the GTPU and EGTP services by applying the example configuration below.

```
config
      context samog_context_name
            egtp-service  egtp_service_name
            associate gtpu-service  egtp_service_name
            gtpc bind ipv4-address  ipv4_address
            exit
      gtpu-service  gtpu_service_name
            bind ipv4-address  ipv4_address
            exit
```

Configuring MAG Services

Create MAG services to configure a PMIPv6-based S2a interface by applying the example configuration below.

```
config
     context context_name
          cgw-service cgw_service_name
               bind ipv4-address ipv4_address
               associate mag-service mag_service_name
               exit
          mag-service mag_service_name
               bind ipv4-address ipv4_address
               reg-lifetime  max_reg_duration
               mobility-option-type-value standard
               end
```

Configuring IPoGRE

Important The IP over GRE functionality requires an additional GRE Interface Tunneling license to create IP-GRE tunnels. For more information, contact your Cisco account representative.

Configure IP over GRE (IPoGRE) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration below.

```
config
     context context_name
          ip vrf vrf_name
          exit
     interface  interface_name
          ip address  ip_address[/mask ]ipv4/v6_address
          exit
     interface  interface_name1
          ip address  ip_address[/mask ]ipv4/v6_address
          exit
     interface  interface_tunnel_name tunnel
          ip vrf forwarding  gre_vrf_name
          ip address  ip_address[/mask ]ipv4/v6_address
          tunnel-mode gre
               source interface interface_name
               destination address ipv4_address
               exit
          exit
     ip route ipv4_address ipv4_address tunnel interface_tunnel_name
     port ethernet  port_number
          no shutdown
          bind interface   interface_name1 context_name
          vlan vlan_number
               no shutdown
               ingress-mode
               bind interface interface_name context_name
               end
```

Notes:

- Use the **interface** *interface_name1* configuration only if a VRF-GRE tunnel is required.
- Use the **ip vrf forwarding** command to associate a GRE tunnel with the VRF.

Configuring IPoVLAN

Configure IP over VLAN (IPoVLAN) encapsulation for processing DHCP Layer 3 IP packets by applying the example configuration below.

```
config
     context context_name
          ip vrf vrf_name
          exit
     interface interface_name
          ip address ip_address ip_address
          exit
     interface interface_name1
          ip vrf forwarding  vrf_name
          ip address ip_address ip_address
          exit
     ip route ip_address[/mask ] next-hop ip_address interface_name1 vrf vrf_name
     ip route ip_address[/mask ] next-hop ip_address interface_name1 vrf vrf_name
     port ethernet  port_number
          no shutdown
          ingress-mode
          bind interface   interface_name context_name
          vlan vlan_number
               ingress-mode
               bind interface interface_name1 context_name
               no shutdown
               end
config
     context context_name
          twan-profile twan_profile_name
               ue-address dhcp
               access-type client ipv4_address[/mask ] ip
               access-type ip vrf  vrf_name
               radius ip vrf  vrf_name
               radius client   ipv4_address[/mask ] key shared_secret_key
disconnect-message dest-port port_number dictionary custom71
               end
```

Notes:

- Use the **ip vrf forwarding** command to associate a GRE tunnel with the VRF.
- Use the **ingress-mode** command to process UL user packets for L3IP access-type.
- Each TWAN Profile creates a "aaa group" in all AAAMgrs with the name **samog_rad_grp_***twan_profile_name*.

Configuring AAA

Create the AAA group for DIAMETER authentication and then configure AAA accounting and authentication by applying the example configuration below.

```
config
      contextaaa_context_name
            interface  aaa_interface_name
                  ip address  ipv4_address/subnetmask
                  ip address  ipv4_address/subnetmask  secondary
                  end
config
      context  samog_context_name
            aaa group aaa_diameterSTa1_group_name
                  diameter authentication dictionary aaa-custom13
                  diameter authentication endpoint  endpoint_name
                  exit
            aaa group  aaa_group_diameter_STa2_name
                  diameter authentication dictionary aaa-custom13
                  diameter authentication endpoint   endpoint_name
                  exit
            aaa group  aaa_acct_group_name
                  radius attribute nas-ip-address address  ipv4-address
                  radius accounting server ipv4_address  encrypted key  key
  port  port_no
                  exit
            aaa group default
            exit
      gtpp group default
      exit
diameter endpoint  STA_endpoint_name
      origin realm  realm_name
      use-proxy
      origin host STa_endpoint_ipv4_address  address  ipv4_address  port  port_no
      no watchdog-timeout
      peer  peer_name  realm  samog_realm_name address  ipv4_address port  port_no
      exit
```

Configuring GTPP Dictionary and CDR Attributes

Configure the GTPP dictionary to be used for SGW and SGSN CDRs and the CDR attributes for the SaMOG gateway by applying the example configuration below.

```
config
      context  samog_context_name
            gtpp group gttp_group_name
                  gtpp charging-agent IPv4/IPv6_Address
                  gtpp server Server_IPv4/IPv6_Address max Maximum_GTPP_Messages
                  gtpp trigger volume-limit
                  gtpp trigger time-limit
                  gtpp dictionary custom24
                  gtpp attribute local-record-sequence-number
                  gtpp attribute local-record-sequence-number
                  gtpp attribute msisdn
                  gtpp attribute diagnostics
                  gtpp attribute dynamic-flag
                  gtpp attribute record-type sgsnpdprecord
                  gtpp attribute record-type sgwrecord
                  gtpp attribute qos max-length qos_max_length
                  end
config
      call-control-profile call_control_profile_name
            accounting context samog_context_name gtpp group gtpp_group_name
```

Configuring DNS

Configure DNS for the SaMOG gateway by applying the example configuration below.

```
config
      context  dns_context_name
            interface  dns_interface_name
                  ip address  ipv4_address/subnetmask
 exit
            subscriber default
            exit
      aaa group default
      exit
      gtpp group default
      ip domain-lookup
      ip name-servers ipv4-address
      dns-client dns_client_name
            bind address ipv4_address
      exit
```

Configuring Local Breakout

Optionally, configure the local breakout - enhanced, or local breakout - basic, or flow-based (with or without external NAT) local breakout model for an APN (assuming that a P-GW service is configured) by applying the appropriate example configuration below:

Important The Local Breakout (LBO) feature is license dependent. Each LBO models require separate feature licenses. While the LBO - Basic and Flow-based LBO licenses can co-exist, they are mutually exclusive with the LBO - Enhanced license. Contact your local Cisco account representative for licensing requirements.

Local Breakout - Enhanced

```
config
      context  context_name
            cgw-service service_name
                  associate pgw-service  service_name
                  exit
            exit
      apn-profile  profile_name
            local-offload
            end
```

Local Breakout - Basic

```
config
     apn-profile apn_profile_name
         local-offload
         ip address pool name pool_name
         ip context-name vpn_context_name
         dns primary  ipv4_address
         dns secondary ipv4_address
         ip access-group access_list_name [ in | out ]
         active-charging rulebase rulebase_name
         exit
    context context_name
        ip pool  pool_name ip_address/mask public priority subscriber-gw-address
 router_ip_address
         ip access-list access_list_name
              redirect css service acs_service_name any
              exit
         exit
    active-charging service acs_service_name
         access-ruledef access_ruledef_name
              ip any-match = TRUE
              exit
         fw-and-nat policy policy_name
             access-rule priority  priority access-ruledef access_ruledef_name
 permit nat-realm nat_realm_name
              exit
         rulebase rulebase_name
              fw-and-nat default-policy policy_name
              end
```

Flow-based Local Breakout

```
config
     apn-profile apn_profile_name
         local-offload flow
         ip context-name vpn_context_name
         ip access-group access_list_name [ in | out ]
         active-charging rulebase rulebase_name
         exit
    context context_name
         ip access-list access_list_name
              redirect css service acs_service_name any
              exit
         exit
```

After applying the above initial configuration for Flow-based LBO, you can configure either a flow-based LBO whitelist or a blacklist.

Flow-based LBO with External NAT

SaMOG can also perform flow-based LBO with external NAT devices based on nex-hop. Configure flow-based LBO with an external NAT by applying the example configuration below:

```
config
 active-charging service acs_service_name
 rulebase rulebase_name
 action priority action_priority_1 ruledef ruledef_name_1 charging-action
charging_action_name
 action priority action_priority_2 ruledef ruledef_name_2 charging-action
charging_action_name
 exit
 ruledef ruledef_name_1
 ip dst-address = ipv6_address[/mask ]
 exit
 ruledef ruledef_name_2
 ip dst-address = ipv4_address[/mask ]
 exit
 charging-action charging_action_name
 nexthop-forwarding-address ipv4_address
 exit
 exit
    # To configure IPv6 Access List
 context context_name
 ipv6 access-list ipv6_acl_name
 redirect css service css_service_name any
 exit
 exit
    # To configure the APN profile to use the IPv6 access list
 apn-profile apn_profile_name
 ip access-group ipv6_acl_name in
 ip access-group ipv6_acl_name out
        # To configure IPv6 DNS servers for GTPv2 sessions on flow-based LBO
 dns ipv6 { primary | secondary } ipv6_address
 end
```

Flow-based LBO Whitelist

```
    active-charging service  acs_service_name
         access-ruledef access_ruledef_name
              ip dst-address = ipv4_destination_address[/mask ]
              exit
         fw-and-nat policy policy_name
             access-rule priority  priority access-ruledef access_ruledef_name
 permit bypass-nat
            access-rule no-ruledef-matches uplink action permit nat-realm
 nat_realm_name
              access-rule no-ruledef-matches downlink action permit
nat-realm nat_realm_name
              exit
         rulebase rulebase_name
              fw-and-nat default-policy policy_name
              end
```

Notes:

- The *nat_realm_name* is the IP pool used by the NAT service for dynamic NATting. This IP pool may have one-to-one or many-to-one users mapping to conserve IP addresses.

Flow-based LBO Blacklist

```
    active-charging service  acs_service_name
         access-ruledef access_ruledef_name
              ip dst-address = ipv4_destination_address[/mask ]
              exit
         fw-and-nat policy policy_name
             access-rule priority  priority access-ruledef access_ruledef_name
 permit nat-realm nat_realm_name
              access-rule no-ruledef-matches uplink action permit
bypass-nat
              access-rule no-ruledef-matches downlink action permit
bypass-nat
              exit
         rulebase rulebase_name
              fw-and-nat default-policy policy_name
              end
```

Notes:

- The *nat_realm_name* is the IP pool used by the NAT service for dynamic NATting. This IP pool may have one-to-one or many-to-one users mapping to conserve IP addresses.

Configuring Web-based Authorization

Important The Web Authorization feature is license dependent. Contact your local Cisco account representative for licensing requirements.

Optionally, configure the SaMOG web-based authorization by applying the example configuration below.

HTTP Redirection for Web-based Authorization

For HTTP redirection, apply the following rulebase, ruledef and charging action example:

```
config
      active-charging service acs_service_name
             #Rule to analyze HTTP packets
             ruledef http_ruledef_name
                    tcp either-port = 80
                    tcp either-port = 8080
                    rule-application routing
                    exit
             #Rule to check if packet is a DNS packet
             ruledef is_DNS_ruledef_name
                    udp either-port = port_number
                    tcp either-port = port_number
                    multi-line-or all-lines
                    exit
            #Rule to check if packet is destined to HTTP portal (to avoid
 redirect loop)
             ruledef is_redirected_ruledef_name
                    ip server-ip-address = http_web_portal_ipv4_address/mask
                    exit
             #Rule for HTTP redirection to HTTP portal
             ruledef http_redirect_ruledef_name
                    http any-match = TRUE
                    ip any-match = TRUE
                    multi-line-or all-lines
                    exit
             #Action to allow packets without throttling at ECS
             charging-action allow_charging_action_name
                    content-id content_id_2
                    exit
             #Action to perform HTTP 302 redirection
             charging-action page_redirect_charging_action_name
                    content-id content_id_3
                    flow action redirect-url http_web_portal_url
                    exit
             #Rulebase with all above rules and actions
             rulebase rulebase_name
                    retransmissions-counted
                    #Run protocol analyzers
                    route priority route_priority ruledef http_ruledef_name
analyzer http
                    #Take action based on protocol analyzer result
                    action priority action_priority ruledef is_DNS_ruledef_name
 charging-action allow_charging_action_name
                    action priority action_priority ruledef
is_redirected_ruledef_name charging-action allow_charging_action_name
                    action priority action_priority ruledef
```

```
http_redirect_ruledef_name charging-action page_redirect_charging_action_name
                           end
```

HTTPS Redirection for Web-based Authorization

For HTTPS redirection, as the HTTPS packets are encrypted using SSL/TLS between the client and server, the ACS service will not be able to perform HTTP request inspection. All HTTPS packets are redirected to an external web portal using Layer 3/Layer 4 redirection rules. The web portal performs an SSL handshake with the UE and redirects for authenticaiton.

Apply the following rulebase, ruledef and charging action example for HTTPS redirection:

```
config
      active-charging service acs_service_name
             #Rule to allow DNS packets
             ruledef is_dns_ruledef_name
                    udp either-port = 53
                    tcp either-port = 53
                    multi-line-or all-lines
                    exit
             #Rule to check if the packet is destined to the web portal,
 to avoid redirect loop
             ruledef is_redirect_ruledef_name
                    ip server-ip-address = web_portal_ip_address
                    exit
             #Rule to check if the packet is an HTTPS packet
             ruledef is_https_ruledef_name
                    tcp either-port = 443
                    multi-line-or all-lines
                    exit
             #Action to allow packets without throttling at ECS
             charging-action allow_charging_action_name
                    content-id content_id_1
                    exit
             #Charging action to redirect all HTTPS packets (including
initial TCP SYN/SYNACK/ACK) to web portal
             charging-action l4_redirect_charging_action_name
                    content-id content_id_2
                    flow action readdress server web_portal_ip_address port
port_number
                    exit
             rulebase rulebase_name
                    action priority priority ruledef is_dns_ruledef_name
charging_action allow_charging_action_name
                    action priority priority ruledef
is_redirect_ruledef_namecharging_action allow_charging_action_name
                    action priority priority ruledef is_https_ruledef_name
charging_action l4_redirect_charging_action_name
```

Once the ruledef, charging action and rulebase are configured based on HTTP or HTTPS redirection, apply the rest of the configuration for web authorization as specified below:

```
configure
    operator-policy  { default | name  policy_name }
```

```
         apn  webauth-apn-profile apn_profile_name
         exit
    apn-profile  profile_name
         active-charging rulebase rulebase_name
         dns { primary | secondary } IPv4_address
         dhcp lease { short duration | time duration }
         ip address pool name  pool_name
         ip context-name  context_name
         ip access-group group_name [ in | out ]
         ipv6 address prefix-pool pool_name
         exit
    call-control-profile  profile_name
         timeout imsi cache  timer_value
         subscriber  multi-device
         authenticate context context_name auth-method { [ eap ] [non-eap]
}
         end
```

Configuring and Binding the Interfaces

The interfaces created previously now must be bound to physical ports. Bind the system interfaces by applying the example configuration below.

```
config
      port ethernet  slot no/port no
            no shutdown
            bind interface gtp_samog_interface_name  gtp_samog_context name
            exit
      port ethernet  slot no/port no
            bind interface interface  STa_acct_interface_name STa_acct_context_name
            exit
      port ethernet  slot no/port no
            bind interface dns_interface_name  dns_context name
            exit
      port ethernet  slot no/port no
            bind interface wlc_pmip_side_interface_name wlc_pmip_side_context_name
            exit
      port ethernet  slot no/port no
            bind interface wlc_side_samog_interface_name wlc_side_samog_context name

      port ethernet  slot no/port no
            bind interface gtpu_interface_name gtpu/gtpc_context name
            end
```

Enabling Logging

Optional. Enable event logging for the SaMOG Gateway by applying the example configuration below from the Command Line Interface Exec Mode.

```
[local]asr5000#  logging filter active facility mrme level  error_reporting_level
[local]asr5500#  logging filter active facility cgw level  error_reporting_level
```

```
[local]asr5500# logging filter active facility ipsgmgr level
error_reporting_level
[local]asr5500# logging filter active facility radius-coa level
error_reporting_level
[local]asr5500# logging filter active facility radius-auth level
error_reporting_level
[local]asr5500# logging filter active facility radius-acct level
error_reporting_level
[local]asr5500# logging filter active facility diabase level
error_reporting_level
[local]asr5500# logging filter active facility diameter-auth level
error_reporting_level
[local]asr5500# logging filter active facility aaamgr level error_reporting_level
[local]asr5500# logging filter active facility aaa-client level
error_reporting_level
[local]asr5500# logging filter active facility diameter level
error_reporting_level
[local]asr5500# logging filter active facility mobile-ipv6 level
error_reporting_level
[local]asr5500# logging filter active facility hamgr level  error_reporting_level
[local]asr5500# logging filter active facility ham diameter-ecs  level
error_reporting_level
[local]asr5500# logging filter active facility egtpc level error_reporting_level
[local]asr5500# logging filter active facility egtpmgr level
error_reporting_level
```

Enabling SNMP Traps

Optional. Enable the sending of SaMOG gateway-related SNMP traps by applying the example configuration below.

```
config
      context  samog_context_name
            snmp trap enable SaMOGServiceStart
            snmp trap enable SaMOGServiceStop
            snmp trap enable CGWServiceStart
            snmp trap enable CGWServiceStop
            end
```

To disable the generation of an SNMP trap:

```
config
      contextsamog_context_name
            snmp trap suppress  trap_name
            end
```

Configuring Bulk Statistics

Use the following configuration example to enable SaMOG bulk statistics:

```
config
      bulkstats collection
      bulkstats mode
 sample-interval minutes
```

```
            transfer-interval  minutes
            file  no
                  remotefile format  format
/localdisk/bulkstats/bulkstat%date%%time%.txt
                 receiver  ipv4_or_ipv6_address  primary mechanism sftp login
  login_name  encrypted password samog schema  schema_name  format  schema_format
```

Notes:

- The **bulkstats collection** command in this example enables bulk statistics, and the system begins collecting pre-defined bulk statistical information.
- The **bulkstats mode** command enters Bulk Statistics Configuration Mode, where you define the statistics to collect.
- The **sample-interval** command specifies the time interval, in minutes, to collect the defined statistics. The *minutes* value can be in the range of 1 to 1440 minutes. The default value is 15 minutes.
- The **transfer-interval** command specifies the time interval, in minutes, to transfer the collected statistics to the receiver (the collection server). The *minutes* value can be in the range of 1 to 999999 minutes. The default value is 480 minutes.
- The **file** command specifies a file in which to collect the bulk statistics. A bulk statistics file is used to group bulk statistics schema, delivery options, and receiver configuration. The *number* can be in the range of 1 to 4.
- The **receiver** command in this example specifies a primary and secondary collection server, the transfer mechanism (in this example, ftp), and a login name and password.
- The **samog schema** command specifies that the SaMOG schema is used to gather statistics. The *schema_name* is an arbitrary name (in the range of 1 to 31 characters) to use as a label for the collected statistics defined by the **format** option. The **format** option defines within quotation marks the list of variables in the SaMOG schema to collect. The format string can be in the range of 1 to 3599.

For descriptions of the SaMOG schema variables, see "SaMOG Schema Statistics" in the *Statistics and Counters Reference.* For more information on configuring bulk statistics, see the *System Administration Guide.*

Saving the Configuration

Save the SaMOG configuration file 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, see the *System Administration Guide* and the *Command Line Interface Reference.*