Configuring Control Plane in CUPS

Important For information related to following configurations, refer the *Ultra Packet Core CUPS Sx Interface Administration and Reference Guide*:

- *Configuring Sx Service for CUPS*
- *Configuring Sx-u Interface for CUPS*
- *Configuring Sx Demux for CUPS*

Important

- The following configuration limit applies in CUPS:
  - Rulebase - 512
  - Ruledef - 2500
  - Charging-action - 2048
- The following CLI command is not recommended to be used, with active subscriber sessions, in production environment: **no active-charging service** *service_name*

The SAEGW Service can be configured to support Control Plane in CUPS behavior, which provides Control Plane functionality through Sxa, Sxb, and Sxab interfaces. The following table highlights minimum configurations required for enabling CUPS Control Plane mode.

SAEGW Service Configuration Mode - Configuration Dependencies	Non-CUPS	CUPS (Control Plane)
cups-enabled	Not Required.	eGTP-C Services of S-GW and P-GW must be associated with **cups-enabled** CLI to enable CUPS Control Plane Mode. **Note** Refer to the *Configuring SAEGW Service in CUPS Mode* section for configuration details. **Important** For GGSN, all eGTP-C services (of P-GW associated with GGSN service) and GGSN services should be configured with **cups-enabled** CLI command. For details, refer the *GGSN in CUPS* feature chapter.
GTP-U Service (Under eGTP-C Service)	eGTP-C Services of S-GW and P-GW must be associated with GTP-U Service.	Not Required
Sx Service	Not Required.	The SAEGW Service must be associated with Sx Service for communication with the User Plane. The Sx Service is capable of handling all possible interfaces like Sxa, Sxb, and Sxab, which is required for Pure-S, Pure-P, and Collapsed PDN respectively. **Important** Refer to the *Ultra Packet Core CUPS Sx Interface Administration and Reference Guide* for more details.
GTP-U Service (Under SAEGW Service)	Not Required.	The SAEGW Service must be associated with GTP-U Service for Sending/Receiving the Router Advertisement(RA)/Router Solicitation (RS) messages between Control Plane and User Plane. The RA/RS signaling is required for both IPv6 and IPv4v6 Pure-P/Collapsed PDN. **Important** Refer to the *Ultra Packet Core CUPS Sx Interface Administration and Reference Guide* for more details.
User-Plane Profile	Not Required.	• **Pure-P/Collapsed PDN**: IP Pool must be associated with User-Plane Profile, which contains information related to User Plane IP address and User Plane capabilities. • **Pure-S PDN**: APN Profile must be configured with associated User Plane Profile, which contains information related to User Plane IP address and User Plane capabilities.

Enabling CUPS in eGTP-C Service for SAEGW

Use the following commands to configure eGTP-C service with CUPS mode that is applicable only for SAEGW service.

```
configure
  context context_name
    egtp-service service_name
      [ no ] cups-enabled
      end
```

The following services should be in STARTED state, and associated under SAEGW service for SAEGW service to move to STARTED state:

1. All eGTP-C services should be configured with **cups-enabled** CLI.
   - S-GW Ingress Service (which is configured as part of SAEGW S-GW Service)
   - S-GW Egress Service (which is configured as part of SAEGW S-GW Service)
   - P-GW Ingress Service (which is configured as part of SAEGW P-GW Service)
2. Other dependent Services like:
   - Sx Service
   - GTP-U Service

NOTES:

- There is no requirement to configure GTP-U service under eGTP-C service, in case **cups-enabled** CLI is enabled. If GTP-U service is configured along with **cups-enabled** CLI, then it will not have any affect.
- There is no change in non-CUPS behavior.
- Any deviation from the above mentioned configuration of SAEGW service will not get the Service in STARTED state. The same would be displayed in **show configuration errors** CLI command.
- The **show egtp-service all** for eGTP-C and **show saegw-service all** for SAEGW will display if the services are CUPS enabled.
- The **cups-enabled** CLI must not be used for standalone P-GW and S-GW service.

Verifying CUPS in EGTPC Service for SAEGW

You can use the following commands to verify if CUPS is enabled:

- **show configuration**
- **show configuration verbose**

- **show egtp-service { all | name** *service_name* **}**
- **show saegw-service { all | name** *service_name* **}**

Use the following command to verify the associated User Plane IP address:

- **show subscribers saegw-only full all**

Recommended Timers

The following table provides the recommended timer values for CLI commands related to IPSec, Sx, and SRP.

IPSEC	**CP**	**UP**
ikev2-ikesa max-retransmission	*3*	*3*
ikev2-ikesa retransmission-timeout	*1000*	*1000*
keepalive	**interval** *4* **timeout** *1* **num-retry** *4*	**interval** *5* **timeout** *2* **num-retry** *4*
Sx	**CP**	**UP**
sx-protocol heartbeat interval	*10*	*10*
sx-protocol heartbeat retransmission-timeout	*5*	*5*
sx-protocol heartbeat max-retransmissions	*4*	*4*
sxa max-retransmissions	*4*	*4*
sxa retransmission-timeout-ms	*5000*	*5000*
sxb max-retransmissions	*4*	*4*
sxb retransmission-timeout-ms	*5000*	*5000*
sxab max-retransmissions	*4*	*4*
sxab retransmission-timeout-ms	*5000*	*5000*
sx-protocol association reattempt-timeout	*60*	*60*
SRP	**CP**	**UP**
hello-interval	*3*	*3*
dead-interval	*15*	*15*

Recommended Configurations

Following are the recommended configurations and restrictions related to Sx and SRP over IPSec:

- The multihop BFD timer between CP and UP must be seven seconds (for Data UPs).
- The singlehop BFD must be enabled on all the contexts (CP GW/Billing and UP Gn/Gi).
- Inter-chassis multihop BFD must be enabled for CP-CP ICSR and UP-UP ICSR (IMS UP).
- The SRP-IPSec ACL must be configured for TCP protocol instead of IP protocol.
- The Sx-IPSec ACL must be configured for UDP protocol instead of IP protocol.

Example Configurations in CP

Multihop BFD Configuration VPC-DI

The following is an example of multihop BFD configuration with seven seconds timer.

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.225 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 350 min_rx 350 multiplier 20
    #exit
```

Multihop BFD Configuration VPC-SI

The following is an example of multihop BFD configuration with three seconds timer.

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.225 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 150 min_rx 150 multiplier 20
    #exit
```

BGP Configuration

The following is an example of BGP configuration with recommended timers.

```
router bgp 1111
      router-id 209.165.200.225
      maximum-paths ebgp 15
      neighbor 209.165.200.250 remote-as 1000
      neighbor 209.165.200.250 ebgp-multihop
      neighbor 209.165.200.250 update-source 209.165.200.225
      neighbor 1111:2222::101 remote-as 1000
      neighbor 1111:2222::101 ebgp-multihop
      neighbor 1111:2222::101 update-source 1111:2222::1
      bgp graceful-restart restart-time 120
      bgp graceful-restart stalepath-time 300
      timers bgp keepalive-interval 30 holdtime-interval 90 min-peer-holdtime-interval 0
server-sock-open-delay-period 10
      address-family ipv4
        redistribute connected
      #exit
```

```
    address-family ipv6
      neighbor 1111:2222::101 activate
      redistribute connected
    #exit
  #exit
```

Singlehop BFD Configuration

The following is an example of singlehop BFD configuration with three seconds timer.

```
interface bgp-sw1-2161-10
    ip address 209.165.200.233 209.165.200.255
    ipv6 address 1111:222::9/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-11
    ip address 209.165.200.234 209.165.200.255
    ipv6 address 1111:222::10/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-12
    ip address 209.165.200.235 209.165.200.255
    ipv6 address 1111:222::11/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-3
    ip address 209.165.200.226 209.165.200.255
    ipv6 address 1111:222::2/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-4
    ip address 209.165.200.227 209.165.200.255
    ipv6 address 1111:222::3/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-5
    ip address 209.165.200.228 209.165.200.255
    ipv6 address 1111:222::4/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-6
    ip address 209.165.200.229 209.165.200.255
    ipv6 address 1111:222::5/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-7
    ip address 209.165.200.230 209.165.200.255
    ipv6 address 1111:222::6/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-8
    ip address 209.165.200.231 209.165.200.255
    ipv6 address 1111:222::7/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-9
    ip address 209.165.200.232 209.165.200.255
    ipv6 address 1111:222::8/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
```

Static Route for Multihop BFD Configuration

The following is an example of static route multihop BFD configuration.

```
ip route static multihop bfd UP-5 209.165.200.240 209.165.200.245
    ip route static multihop bfd UP-6 209.165.200.240 209.165.200.246
    ip route static multihop bfd UP-9 209.165.200.240 209.165.200.247
    ip route static multihop bfd UP-10 209.165.200.240 209.165.200.248
    ip route static multihop bfd UP-7 209.165.200.240 209.165.200.249
    ip route static multihop bfd UP-8 209.165.200.240 209.165.200.250
```

Static Route for Singlehop BFD Configuration

The following is an example of static route singlehop BFD configuration.

```
ip route static bfd bgp-sw1-2161-3 209.165.200.230
    ip route static bfd bgp-sw1-2161-4 209.165.200.230
    ip route static bfd bgp-sw1-2161-5 209.165.200.230
    ip route static bfd bgp-sw1-2161-6 209.165.200.230
    ip route static bfd bgp-sw1-2161-7 209.165.200.230
    ip route static bfd bgp-sw1-2161-8 209.165.200.230
    ip route static bfd bgp-sw1-2161-9 209.165.200.230
    ip route static bfd bgp-sw1-2161-10 209.165.200.230
    ip route static bfd bgp-sw1-2161-11 209.165.200.230
    ip route static bfd bgp-sw1-2161-12 209.165.200.230
```

IPSec ACL Configuration

The following is an example IPSec ACL configuration in CP.

```
ip access-list UP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec Transform Set Configuration

The following is an example of IPSec Transform Set configuration in CP.

```
ikev2-ikesa transform-set ikesa-UP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256

    ipsec transform-set A-UP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14
```

IPSec Crypto Map Configuration

The following is an example of IPSec Crypto Map configuration in CP.

```
crypto map UP-1 ikev2-ipv4
      match address UP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-UP-1
      ikev2-ikesa rekey
      keepalive interval 4 timeout 1 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-UP-1
        lifetime 300
        rekey keepalive
```

```
      #exit
      peer 192.1.1.1
      ikev2-ikesa policy error-notification
    #exit
```

Sx Configuration

The following is an example of Sx configuration in CP.

```
sx-service SX-1
      instance-type controlplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
      sx-protocol supported-features load-control
      sx-protocol supported-features overload-control
    exit
end
```

Example Router Configurations

Static Routes for Interface

The following is an example configuration of static route for interface.

```
ip route 209.165.200.224/27 Vlan1111 209.165.200.225
ip route 209.165.200.224/27 Vlan1111 209.165.200.226
ip route 209.165.200.224/27 Vlan1111 209.165.200.227
ip route 209.165.200.224/27 Vlan1111 209.165.200.228
ip route 209.165.200.224/27 Vlan1111 209.165.200.229
ip route 209.165.200.224/27 Vlan1111 209.165.200.230
ip route 209.165.200.224/27 Vlan1111 209.165.200.231
ip route 209.165.200.224/27 Vlan1111 209.165.200.232
ip route 209.165.200.224/27 Vlan1111 209.165.200.233
ip route 209.165.200.224/27 Vlan1111 209.165.200.234
```

Static Routes for Singlehop BFD

The following is an example configuration of static route for singlehop BFD.

```
ip route static bfd Vlan1111 209.165.200.225
ip route static bfd Vlan1111 209.165.200.226
ip route static bfd Vlan1111 209.165.200.227
ip route static bfd Vlan1111 209.165.200.228
ip route static bfd Vlan1111 209.165.200.229
ip route static bfd Vlan1111 209.165.200.230
ip route static bfd Vlan1111 209.165.200.231
ip route static bfd Vlan1111 209.165.200.232
ip route static bfd Vlan1111 209.165.200.233
ip route static bfd Vlan1111 209.165.200.234
```

Interface for Singlehop BFD

The following is an example configuration of interface for singlehop BFD.

```
interface Vlan1111
  no shutdown
  bandwidth 10000000
  bfd interval 999 min_rx 999 multiplier 3
  no bfd echo
  ip address 209.165.200.224/27
  ipv6 address 1111:222::1/112
```

BGP Configuration

The following is an example of BGP configuration with recommended timers.

```
router bgp 1000
  router-id 209.165.200.226
  timers bgp 30 90
  timers bestpath-limit 300
  timers prefix-peer-timeout 30
  timers prefix-peer-wait 90
  graceful-restart
  graceful-restart restart-time 120
  graceful-restart stalepath-time 300
```

Example Configurations in UP

IPSec ACL Configuration

The following is an example of IPSec ACL configuration in UP.

```
ip access-list CP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec Transform Set Configuration

The following is an example of IPSec Transform Set configuration in UP.

```
ipsec transform-set A-CP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14

    ikev2-ikesa transform-set ikesa-CP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256
```

IPSec Crypto Map Configuration

The following is an example of IPSec Crypto Map configuration in UP.

```
crypto map CP-1 ikev2-ipv4
      match address CP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-CP-1
      ikev2-ikesa rekey
      keepalive interval 5 timeout 2 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
```

```
        ipsec transform-set list A-CP-1
      #exit
      peer 209.165.200.230
      ikev2-ikesa policy error-notification
    #exit
```

Sx Configuration

The following is an example of Sx configuration in UP.

```
sx-service SX-1
      instance-type userplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
    exit
```

Example SRP Configurations

IPSec ACL Configuration

The following is an example of IPSec ACL configuration for SRP.

```
ip access-list SRP
      permit tcp host 209.165.200.227 host 209.165.200.228
    #exit
```

SRP Configuration

The following is an example of SRP configuration.

```
configure
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.225 interval 999 min_rx 999 multiplier 3
    #exit
configure
  context srp
    service-redundancy-protocol
      chassis-mode primary
      hello-interval 3
      dead-interval 15
      monitor bfd context srp 209.165.200.226 chassis-to-chassis
      monitor bgp context gi-pgw 209.165.200.245
      monitor bgp context gi-pgw 3333:888::1
      monitor bgp context saegw 209.165.200.245
      monitor bgp context saegw 3333:888::2
      peer-ip-address 209.165.200.227
      bind address 209.165.200.228
    #exit
    ip route static multihop bfd srp 209.165.200.229 209.165.200.245
    ip route 209.165.201.1 209.165.202.129 209.165.200.230 SRP-Physical-2102
    ip route 209.165.201.2 209.165.202.130 209.165.200.231 SRP-Physical-2102
    ip route 209.165.201.3 209.165.202.131 209.165.200.232 SRP-Physical-2102
```

```
    ip igmp profile default
    #exit
  #exit
end
```