Perimeta Configuration for ClearIP Inbound Scenarios

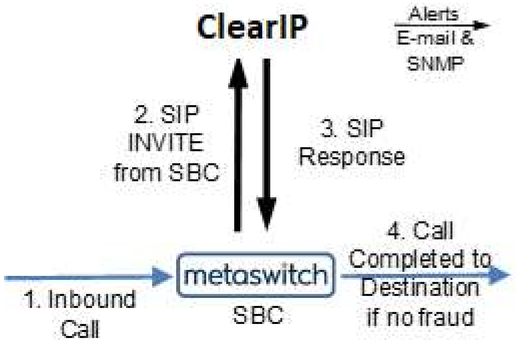
Revision History

Revision	Date of Issue	Changes
1.0.0	March 31, 2017	Initial draft
1.0.1	April 3, 2017	Add to Introduction
1.0.2	April 4, 2017	Update call scenarios description
1.1.0	April 5, 2018	Update for ClearIP
1.2.0	April 23, 2018	Update for TCP connection issue
1.3.0	April 27, 2018	Updated for inbound scenarios
1.3.1	June 28, 2018	Added outbound MMF rules.

Contents

1 Introduction

This documentation provides instructions on how to configure Metaswitch Perimeta Session Border Controller (SBC) with ClearIP for inbound scenarios. The diagram provides an overview of how ClearIP is configured as a SIP end point with Perimeta. SIP INVITEs are sent from Perimeta to ClearIP for fraud and robocall control. If no fraud is detected, ClearIP returns a SIP 404 No Route Found message and Perimeta retries the call to the next route in its local call routing table. If fraud is detected, ClearIP responds with a SIP 603 Decline message indicating that Perimeta should block the call. ClearIP can also return a SIP 302 Redirect message with an alternative destination if the call should be diverted.

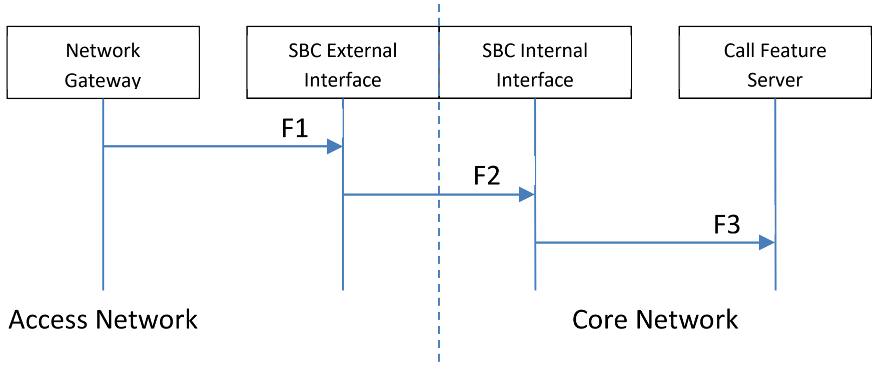


This documentation does not include Perimeta installation instructions, such as installing Perimeta VMware image, configuring network interfaces, configuring Perimeta with DCM, etc. This work should be done by Metaswitch representatives.

2 Inbound Scenarios

ClearIP can be used as the fraud and robocall control solution for either inbound or outbound scenarios. In the inbound call scenarios, Perimeta directly forwards the calls from source devices to ClearIP. In the outbound scenarios, Perimeta forwards the calls from source devices to call feature servers first, then forwards the calls to ClearIP before sending them out. Since it is difficult for ClearIP to get the source device information in the outbound call scenarios, this documentation discusses the inbound call scenarios.

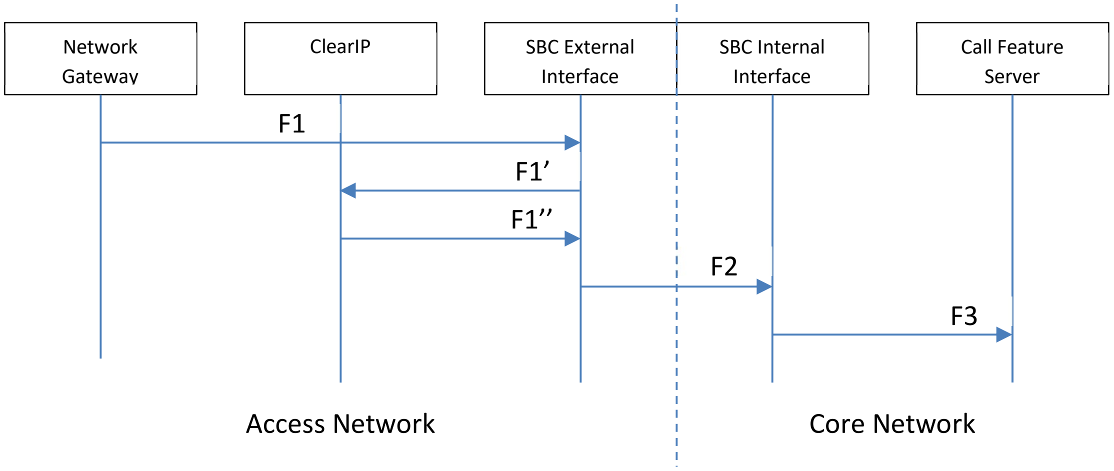
2.1 Original Scenario w/o ClearIP



1. Access Network. The network outside of the domain of the telephone service provider.
2. Core Network. The network inside of the domain of the telephone service provider.
3. Network Gateway. The device in Access Network sends SIP calls to the telephone service provider.
4. SBC External Interface. The external SIP interface configured on SBC to connect Access Network.
5. SBC Internal Interface. The internal SIP interface configured on SBC to connect Core Network.
6. Call Feature Server. The server of the telephone service provider providing routing, billing, etc. features.
7. Routing rules
    a. L1. Local policies configured on SBC for SBC External Interface/Access Network.
    b. L2. Local policies configured on SBC for SBC Internal Interface/Core Network.

    Note: There may be only one local policy. We separate it into two policies logically.
8. Data flow
    a. F1. Network Gateway sends calls to SBC External Interface.
    b. F2. SBC External Interface forwards the calls to SBC Internal Interface based on the local policies configured on SBC for SBC External Interface, L1.
    c. F3. SBC Internal Interface forwards the calls to Call Feature Server based on the local policies configured on SBC for SBC Internal Interface, L2.

2.2 Proposed Scenario w/ ClearIP



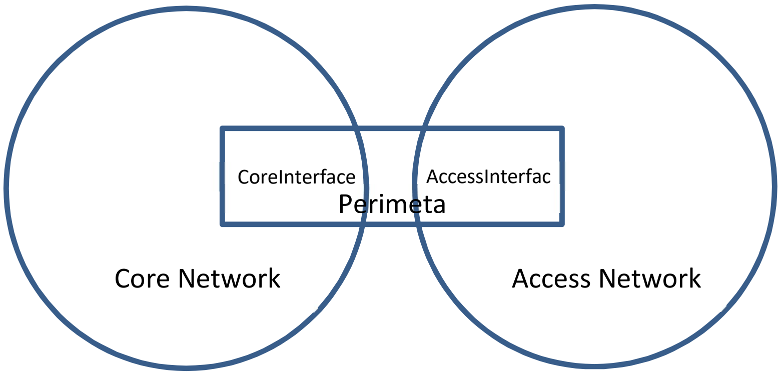
1. Access Network. The network outside of the domain of the telephone service provider. ClearIP typically is in Access Network.
2. Core Network. The network inside of the domain of the telephone service provider.
3. Network Gateway. The device in Access Network sends SIP calls to the telephone service provider.
4. SBC External Interface. The external SIP interface configured on SBC to connect Access Network.
5. SBC Internal Interface. The internal SIP interface configured on SBC to connect Core Network.
6. Call Feature Server. The server of the telephone service provider providing routing, billing, etc. features.
7. Routing rules
    a. L1’+L1. Local policies configured on SBC for SBC External Interface. It includes the routing policy for ClearIP and the original Local policies configured on SBC for SBC External Interface, L1.
    b. L2. Local policies configured on SBC for SBC Internal Interface.

    Note: It is not necessary to change L1 and L2.
8. Data flow
    a. F1. Network Gateway sends calls to SBC External Interface.
    b. F1’. SBC External Interface sends the calls to ClearIP for fraud detection based on the local policies configured on SBC for SBC External Interface for ClearIP, L1’.
    c. F1’’. ClearIP sends response to SBC External Interface. If there is fraud detected, SIP 603 Decline is sent to SBC, SBC External Interface forwards it to Network Gateway and finishes the calls. Otherwise, SIP 404 Not Found is sent.
    d. F2. SBC External Interface forwards the calls to SBC Internal Interface based on the local policies configured on SBC for SBC External Interface, L1.
    e. F3. SBC Internal Interface forwards the calls to Call Feature Server based on the local policies configured on SBC for SBC Internal Interface, L2.

3 Basic Configuration

This section provides the basic standard configuration for Perimeta.

3.1 Network Diagram



Perimeta is configured with 2 network interfaces, CoreInterface and AccessInterface. They connect to Core Network and Access Network respectively. Core Network includes trusted network devices. Access Network includes the devices outside, customer devices and provider devices. To work with the devices identified by FQDN, such as ClearIP (sip.clearip.com), DNS servers should be configured in the service-interface.

Note: CearIP can be treated as a trusted device in Core Network or a normal device in Access Network. In this documentation, ClearIP is treated as a device in Access Network.

3.2 Configuration

```
  system
    service-interface serv1
      description "Core Network"
      service-network 1
      port-group-name CoreNetwork
      ipv4
        ! Probing is disabled for service interface serv1 due to inconsistent
configuration:
        ! - The probe source IP for shelf A interface 1 has not been filled out
        ! - The probe source IP for shelf B interface 1 has not been filled out
        subnet-prefix-length 18
        gateway-ip-address 172.16.4.1
        local-ip-address 172.16.4.232
          service-address CoreIP
        probes-source-style specific-source
        activate
      network-security trusted
      criticality 10
    service-interface serv2
      description "Access Network"
      service-network 2
      port-group-name AccessNetwork
      ipv4
        ! Probing is disabled for service interface serv2 due to inconsistent
configuration:
        ! - The probe source IP for shelf A interface 1 has not been filled out
        ! - The probe source IP for shelf B interface 1 has not been filled out
        subnet-prefix-length 18
        gateway-ip-address 172.16.4.1
        local-ip-address 172.16.4.233
          service-address AccessIP
        probes-source-style specific-source
        activate
      network-security untrusted
      criticality 8
      dns-servers 8.8.8.8
```

Note: At least one DNS server should be configured. In the sample configuration, a Google Public DNS IPv4 server is configured on the access network service interface, serv2, which connects to Access Network. Other DNS servers can be used too. For example, an internal DNS server of the telephone service provider in Core Network can be configured on the core network service interface, serv1, which connects Core Network.

4 Media Configuration

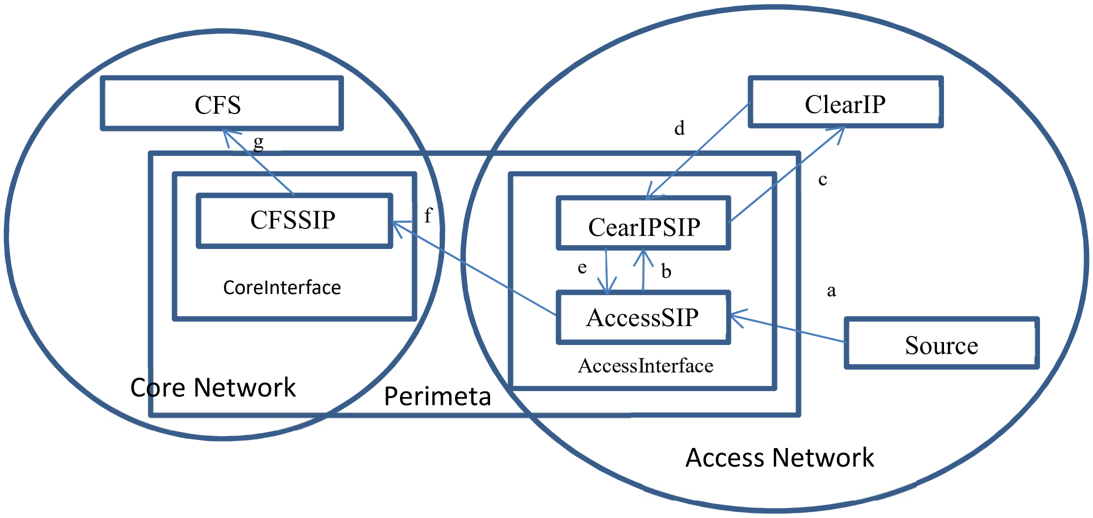
Perimeta can be configured to bypass media traffic between Perimeta and ClearIP.

1. For the calls between the end points in the same network, it needs to configure media bypass in the adjacencies.
2. For the calls between the end points in the different networks, the same media bypass tag can be used to link adjacencies to bypass media.

5 Call Scenarios for Inbound Scenario

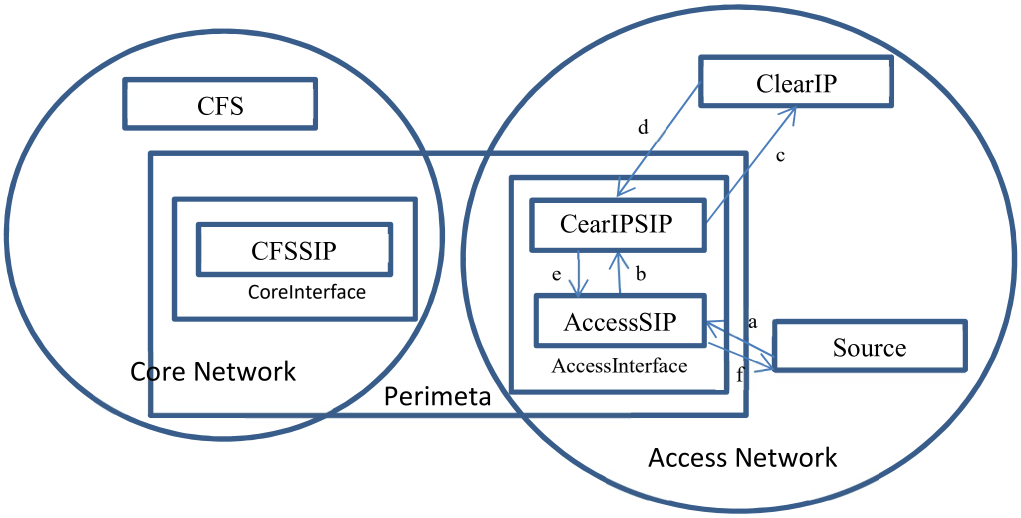
Three different inbound call scenarios are discussed.

5.1 No Fraud Detected



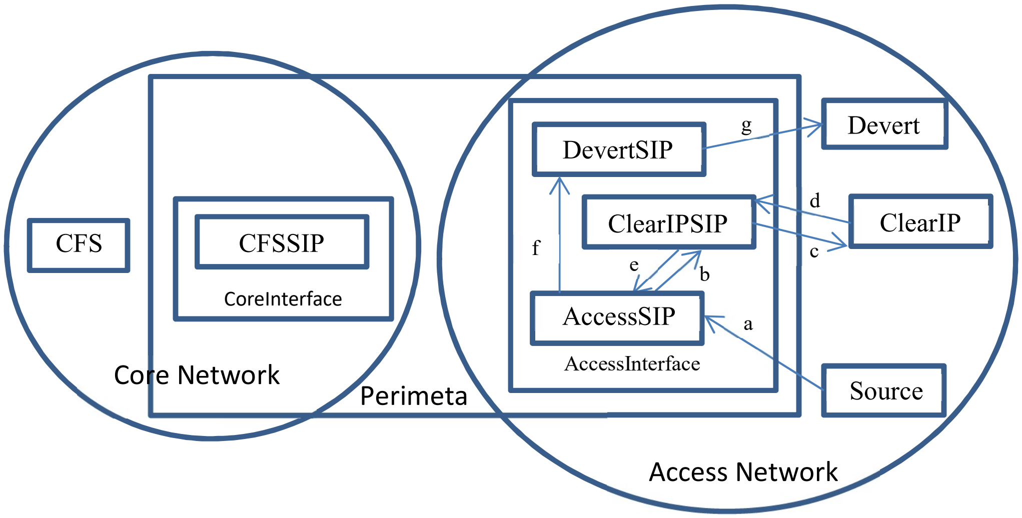
1. Source sends a call to Perimeta (a)
2. Perimeta forwards the call to ClearIP (b, c)
3. ClearIP returns SIP 404 (d,e)
4. Perimeta tries CFS, the original target device, call feature server (f, g)

5.2 Fraud Detected



1. Source sends a call to Perimeta (a)
2. Perimeta forwards the call to ClearIP (b, c)
3. ClearIP returns SIP 603 (d, e)
4. Perimeta drops the call (f)

5.3 Diverted



1. Source sends a call to Perimeta (a)
2. Perimeta forwards the call to ClearIP (b, c)
3. ClearIP returns SIP 3xx with Destination, the diversion device (d, e)
4. Perimeta tries Devert (f, g)

6 Perimeta Configuration for ClearIP

This section provides details on the Perimeta configuration settings for operation with ClearIP for the inbound scenario that is discussed in the documentation.

6.1 High Level Description

1. The basic idea is to insert ClearIP into normal configuration.
2. Perimeta should be configured to do hunting (route advance) if ClearIP returns SIP 404. The call routing policy rule for this part should be
    a. Try ClearIP first.
    b. Try other destinations.

   The ClearIP adjacency should be configured with hunting-trigger code 404.
3. Perimeta should drop the call if the ClearIP return SIP 603. It is the default behavior of Perimeta, it is not necessary to configure anything for it.
4. The adjacency of ClearIP should be configured to handle SIP 302 messages. Several different behaviors may be configured
    a. Try the destinations in SIP 3xx from the same or different interface of the ClearIP.
    b. Prevent SIP 404 from being replied from the destinations. Otherwise Perimeta tries the original destinations.
5. MMF (Message Manipulation Framework) rules are configured to provide information, such as IP address, of the call source device to ClearIP.

6.2 Instructions

1. MMF addInvitePSourceDeviceHeader rule is configured to add P-Source-Device header with source device IP address into the SIP INVITE sent to ClearIP.

```
sip message-manipulation
  header-profile addPSourceDeviceHeader
    description "Copies IP from Via header to P-Source-Device header"
    header P-Source-Device
      action add-header value ${msg.rmt_ip_addr}
  header-profile delPSourceDeviceHeader
    description "Deletes P-Source-Device header"
    header P-Source-Device
      action strip
  method-profile addInvitePSourceDeviceHeader
    method INVITE
      action pass
      header-profile addPSourceDeviceHeader
  method-profile delInvitePSourceDeviceHeader
    method INVITE
      action pass
      header-profile delPSourceDeviceHeader
```

2. ClearIPSIP adjacency is configured for ClearIP.
    a. Hunting trigger code 404
    b. Ping-enable
    c. Timer
    d. Media-bypass-tages mbtag
    e. Redirect-mode recurse-route
    f. listen-transports tcp
    g. mandated-transport tcp
    h. signaling-peer sip.clearip.com

```
adjacency sip ClearIPSIP
  description "ClearIP SIP Adjacency"
  interop
    hunting-trigger 404
    ping-enable
      fail-count 1
      interval 10
      lifetime 5
    timer
      prov-resp-timeout 5 seconds
  media-bypass-tags mbtag
  listen-transports tcp
  adjacency-type preset-peering
  mandated-transport tcp
  redirect-mode recurse-route
  service-address AccessIP
    # service-network 2
    # signaling-local-address ipv4 172.16.4.233
  signaling-peer sip.clearip.com
  signaling-peer-port 5060
  activate
```

Note:

i. ping-enable should be configured to allow Perimeta to detect the state of ClearIP instead of waiting for the long timeout of establishing TCP connection.

ii. timer should be configured to allow Perimeta to quickly fail a call attempt. It is very useful for the scenario that ClearIP is down and the SBC timeout of establishing TCP connection is long.

Note: TLS is optional

i. signaling-peer-port 5061

ii. tls fqdn sip.clearip.com

```
adjacency sip ClearIPSIP
  description "ClearIP SIP Adjacency"
  interop
    hunting-trigger 404
    ping-enable
      fail-count 1
      interval 10
      lifetime 5
    timer
      prov-resp-timeout 5 seconds
  media-bypass-tags mbtag
  listen-transports tcp
  adjacency-type preset-peering
  mandated-transport tcp
  redirect-mode recurse-route
  tls fqdn sip.clearip.com
  service-address AccessIP
    # service-network 2
    # signaling-local-address ipv4 172.16.4.233
  signaling-peer sip.clearip.com
  signaling-peer-port 5061
  activate
```

Note: Important

i. Do not replace “sip.clearip.com” with a static IP address. The IP addresses for ClearIP will change for load balancing and maintenance. Using a static IP address for ClearIP will cause a service interruption.

ii. CearIP does not respond to UDP or ICMP (ping) messages

3. DevertSIP adjacency is configured for the destination device returned in SIP 3xx from ClearIP.
    a. Media-bypass-tages mbtag

```
adjacency sip DevertSIP
  description "Deverted SIP Adjacency"
  media-bypass-tags mbtag
  adjacency-type preset-peering
  service-address AccessIP
    # service-network 2
    # signaling-local-address ipv4 172.16.4.233
  remote-address-range ipv4 172.16.4.32 prefix-len 29 trusted
  signaling-peer 172.16.4.38
  signaling-peer-port 5060
  activate
```

4. CSFSIP adjacency is configured for the original target device, such as call feature server.
    a. Media-bypass-tages mbtag

```
adjacency sip CFSSIP
  description "Call Feature Server SIP Adjacency"
  media-bypass-tags mbtag
  adjacency-type preset-core
  service-address CoreIP
    # service-network 1
    # signaling-local-address ipv4 172.16.4.232
  signaling-peer 172.16.4.19
  signaling-peer-port 5060
  activate
```

5. AccessSIP adjacency is configured for the source device.
    a. Media-bypass-tages mbtag
    b. Edit-profiles inbound addInvitePSourceDeviceHeader

```
adjacency sip AccessSIP
  description "Access SIP Adjacency"
  interop
    message-manipulation
      edit-profiles inbound addInvitePSourceDeviceHeader
  media-bypass-tags mbtag
  adjacency-type preset-peering
  service-address AccessIP
    # service-network 2
    # signaling-local-address ipv4 172.16.4.233
  remote-address-range ipv4 172.16.4.128 prefix-len 25 trusted
  signaling-peer 172.16.4.139
  signaling-peer-port 5060
  activate
```

6. Call-policy-set
    a. All calls from AccessSIP adjacency should be sent to ClearIPSIP adjacency first
    b. All calls from AccessSIP adjacency should be sent to CFSSIP adjacency if ClearIPSIP (adjacency for ClearIP) fails with SIP 404

```
  rtg-src-adjacency-table srcAdjTable
    entry 1
      match-adjacency AccessSIP
      dst-adjacency ClearIPSIP
      action complete
    entry 2
      match-adjacency AccessSIP
      dst-adjacency CFSSIP
      action complete
```

6.3 Configuration

```
sbc
  signaling
      header-profile addPSourceDeviceHeader
        description "Copies IP from Via header to P-Source-Device header"
        header P-Source-Device
          action add-header value ${msg.rmt_ip_addr}
      header-profile delPSourceDeviceHeader
        description "Deletes P-Source-Device header"
        header P-Source-Device
          action strip
      method-profile addInvitePSourceDeviceHeader
        method INVITE
          action pass
          header-profile addPSourceDeviceHeader
      method-profile delInvitePSourceDeviceHeader
        method INVITE
          action pass
          header-profile delPSourceDeviceHeader
    adjacency sip ClearIPSIP
      description "ClearIP SIP Adjacency"
      interop
        hunting-trigger 404
        ping-enable
          fail-count 1
          interval 10
          lifetime 5
        timer
          prov-resp-timeout 5 seconds
      media-bypass-tags mbtag
      listen-transports tcp
      adjacency-type preset-peering
      mandated-transport tcp
      redirect-mode recurse-route
      service-address AccessIP
        # service-network 2
        # signaling-local-address ipv4 172.16.4.233
      signaling-peer sip.clearip.com
      signaling-peer-port 5060
      activate
    adjacency sip DevertSIP
      description "Deverted SIP Adjacency"
      media-bypass-tags mbtag
      adjacency-type preset-peering
      service-address AccessIP
        # service-network 2
        # signaling-local-address ipv4 172.16.4.233
      remote-address-range ipv4 172.16.4.32 prefix-len 29 trusted
      signaling-peer 172.16.4.38
      signaling-peer-port 5060
      activate
    adjacency sip CFSSIP
      description "Call Feature Server SIP Adjacency"
      media-bypass-tags mbtag
      adjacency-type preset-core
      service-address CoreIP
        # service-network 1
        # signaling-local-address ipv4 172.16.4.232
      signaling-peer 172.16.4.19
      signaling-peer-port 5060
      activate
    adjacency sip AccessSIP
      description "Access SIP Adjacency"
      interop
        message-manipulation
          edit-profiles inbound addInvitePSourceDeviceHeader
          edit-profiles outbound delInvitePSourceDeviceHeader
      media-bypass-tags mbtag
      adjacency-type preset-peering
      service-address AccessIP
        # service-network 2
        # signaling-local-address ipv4 172.16.4.233
      remote-address-range ipv4 172.16.4.128 prefix-len 25 trusted
      signaling-peer 172.16.4.139
      signaling-peer-port 5060
      activate
    call-policy-set 1
      description "Routing policy for ClearIP"
      first-call-routing-table srcAdjTable
      rtg-src-adjacency-table srcAdjTable
        entry 1
          match-adjacency AccessSIP
          dst-adjacency ClearIPSIP
          action complete
        entry 2
          match-adjacency AccessSIP
          dst-adjacency CFSSIP
          action complete
      complete
    active-call-policy-set 1
  activate
```