Common Components

The following components of the Cisco Unified Border Element are common to all of the configuration profile examples in this document.

- Secure Media
- Adjacencies
- Call Policies
- CAC Policies
- SIP Profiles

Secure Media

The secure media segment provides secure transportation of unsignaled, encrypted data streams between two networks.

Secure media is disabled by default. To enable secure media, you configure it at the global level in the the SBC configuration. Once enabled, it applies to all calls.

When secure media is enabled, the Cisco Unified Border Element assumes that all endpoints can handle encrypted data streams regardless of the actual capabilities of the endpoints.

Secure media can apply to any of the following types of addresses:

- Physical address of an interface
- Logical address of an interface
- Service Virtual Interface (SVI) address

The following example shows how to enable secure media:

```
sbc MY_SBC
    sbe
    secure-media
    …
    …
```

All connections configured after the **secure-media** command are secure connections.

Adjacencies

The connection between a Cisco Unified Border Element and a customer, network, business, or service provider is called an adjacency. An adjacency configuration contains the local IP address and the remote IP address for the adjacency that provides the connection between a Cisco Unified Border Element and a customer, network, business, or service provider.

There are two types of adjacencies:

- Session Initiation Protocol (SIP) adjacency, which acts as a back-to-back user agent
- H.323, which acts as an H.323 gateway

Adjacencies can be grouped together in accounts. Accounts enable you define call policies and CAC polices based on customer.

A signaling address must be configured for each adjacency, and each signaling address must be paired with a signaling port. SBC uses the IP-address/port-number pair to receive signaling and control packets.

For a SIP adjacency, the signaling address is specified as an outbound proxy address to a remote device.

A signaling address can be any of the following types of addresses:

- Loopback address configured on the router
- Physical address of an interface
- Logical address of a subinterface
- Static Virtual Address (SVI)

The following examples show the adjacency configurations for Business-to-Business TelePresence Configuration Profile Example:

```
adjacency sip CUCM1
    vrf CUCM1
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1
    preferred-transport tcp
    security trusted-unencrypted
    signaling-address ipv4 23.61.1.1
        statistics method summary
    signaling-port 5160
    remote-address ipv4 175.181.0.10 255.255.255.255
    signaling-peer 175.181.0.10
    signaling-peer-port 5160
    account CUCM1
    attach

adjacency sip CUCM2
    vrf CUCM2
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1
    preferred-transport tcp
    security trusted-unencrypted
    signaling-address ipv4 23.61.2.1
    statistics method summary
```

```
signaling-port 5160
remote-address ipv4 175.182.0.12 255.255.255.255
signaling-peer 175.182.0.12
signaling-peer-port 5160
account CUCM2
attach
```

Note For examples of creating VRFs, see the "VRF Examples" section on page 111

Call Policies

A call policy is a set of rules that define how SBC responds to new call events. A call policy includes number analysis and routing.

A call policy set contains one or more tables, which contain entries, such as adjacency names, source numbers, and destination numbers. SBC uses these tables to match the fields in incoming and outgoing call packets with the entries in these tables. Based on these matches, SBC can perform the following tasks.

- Jump to another table
- Select the adjacencies
- Complete the call

Call Policy Configuration

This example shows how to configure a call policy with table entries and entry commands that connect 2 CUCM adjacencies: CUCM1 and CUCM2.

```
sbc MY_SBC
    sbe
    secure-media
        ….
        ….
        ….
    call-policy-set 1
        first-call-routing-table start-table
        rtg-src-adjacency-table start-table
        entry 1
            match-adjacency CUCM2
            dst-adjacency CUCM1
            action complete
        entry 2
            match-adjacency CUCM1
            dst-adjacency CUCM2
            action complete
        complete
    active-call-policy-set 1
```

Number Analysis

A number analysis call policy compares incoming and outgoing call numbers with numbers in a Cisco Unified Border Element table of valid telephone numbers.

SBC does number analysis by matching dialed numbers with the configured entries in a call policy entry table. A number analysis call policy is applied only to new call events. If the dialed number does not match any of the entries in the call policy, SBC rejects the call.

A number analysis call policy can perform the following functions:

- Number Validation
- Number Categorization
- Digit Manipulation

Number analysis is done by matching dialed numbers with valid numbers in the following types of call policy tables:

- dst-number—Tables of this type contain entries whose match values represent complete numbers of Destination. In such tables, an entry matches an event if the entire dialed digit string exactly matches the match value of the entry.
- dst-prefix—Tables of this type contain entries whose match values represent number prefixes of Destination. In such tables, an entry matches an event if there exists a subset of the dialed digit string, consisting of consecutive digits taken from the front of the dialed digit string, that exactly matches the match value of the entry.
- src-number—Tables of this type contain entries whose match values represent complete numbers of Source. In such tables, an entry matches an event if the entire source digit string exactly matches the match value of the entry.
- src-prefix—Tables of this type contain entries whose match values represent number prefixes of Source. In such tables, an entry matches an event if there exists a subset of the source digit string, consisting of consecutive digits taken from the front of the source digit string, that exactly matches the match value of the entry.

Note During number analysis, only the destination number can be modified. The source number cannot be modified. The source number can be modified during Routing.

The format of an entry in a call policy table is a limited-form, regular expression representing a string of dialed digits. The format syntax used is described in Table 1.

Table 1 Number Analysis Expressions

Expression	Description
X	Any numerical digit 0 – 9.
( )	The digit within the parentheses is optional. For example, (0)XXXX represents 0XXXX and XXXX.
[ ]	One of the digits within the square brackets is used. For example, [01]XXX represents 0XXX and 1XXX. A range of values can be represented within the square brackets. For example, [013-5]XXX represents 0XXX, 1XXX, 3XXX, 4XXX and 5XXX.
*	The * key on the telephone.
#	The # key on the telephone.
-	Digit delimiter
,	Digit delimiter
a-f/A-F	Hexadecimal digits

For more detailed information on number and prefix matching, see Chapter 12, “Implementing Cisco Unified Border Element (SP Edition) Policies” of the *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model.*

Number Validation

A number validation call policy verifies whether the dialed number matches a valid telephone number in the call policy table. The following example shows the configuration of a call policy that does number validation:

```
sbc MY_SBC
    sbe
        call-policy-set 2
            first-number-analysis-table VALIDATE-DEST-PREFIX
            na-dst-prefix-table VALIDATE-DEST-PREFIX
            entry 1
                match-prefix 8XX
                action accept
                exit
            entry 2
                match-prefix 911
                action accept
                exit
            entry 3
                match-prefix 1XX
                action accept
                exit
            entry 4
                match-prefix X
                action reject
                exit
            complete
        active-call-policy-set 2
```

Number Categorization

With number categorization, call events can be placed into user-defined categories during processing. Events that are placed into categories can be referred to during the CAC policy stage. The following example shows the configuration of a call policy that does number categorization:

```
sbc MY_SBC
    sbe
        call-policy-set 3
            first-number-analysis-table VALIDATE-DEST-PREFIX
            na-dst-prefix-table VALIDATE-DEST-PREFIX
            entry 1
                match-prefix 8X
                category Non-emergency
                action accept
                exit
            entry 2
                match-prefix 1XX
                category Non-Emergency
                action accept
                exit
            entry 3
                match-prefix 911
                category Emergency
                action accept
                exit
            entry 4
                match-prefix X
                action reject
                exit
        complete
    active-call-policy-set 3
```

Digit Manipulation

Digit manipulation is the process of reformatting a call number into a canonical form, such as the E.164 format. In the following example, the **edit-dst del-prefix 1** command in entry 1 removes the leading 1 digit from the dialed number and deletes the entire string.

The following example shows the configuration of a call policy that does digit manipulation:

```
sbc MY_SBC
    sbe
        call-policy-set 4
            first-number-analysis-table VALIDATE-DEST-PREFIX
            na-dst-prefix-table VALIDATE-DEST-PREFIX
            entry 1
                match-prefix 8X
                category Non-emergency
                edit-dst del-prefix 1
                action accept
                exit
            entry 2
                match-prefix 1XX
                category Non-Emergency
                action accept
                exit
            entry 3
                match-prefix 911
                category Emergency
                action accept
                exit
            entry 4
                match-prefix X
                action reject
                exit
        complete
    active-call-policy-set 4
```

Routing

Routing is also handled in a call policy table. Routing is the process of determining the next-hop and VoIP-signaling entities, to which signaling requests are to be sent.

A routing call policy is applied to new call events and subscriber registration events.

A routing call policy is applied in two stages:

1. Digit manipulation
2. Selection of a destination adjacency (or group of adjacencies for load balancing)

You can configure routing rules using regular expressions to match entities such as:

- User name
- Domain name (that is part of a source or destination SIP URI)

The digits in a call number can be modified or replaced during the routing process.

Note If a new call event matches an existing subscriber registration, the new call is automatically routed to the source IP address and port of the existing subscriber registration. No configured policy is required for this. The configured policy does not effect the routing of such calls.

Note Routing call policies are not applied to call update events, such as update signaling messages. Call update events are automatically routed to the destination adjacency of the call.

The following configuration shows how to configure a routing call policy table for routing calls based on the prefix number of the call:

```
sbc MY_SBC
    sbe
        call-policy-set 5
        first-call-routing-table ROUTE-ON-DEST-NUM
        rtg-dst-address-table ROUTE-ON-DEST-NUM
        entry 1
            match-address 212
            prefix
            edit add-prefix 1
            dst-adjacency CUCM1
            action complete
            exit
        entry 2
            match-address 215
            prefix
            dst-adjacency CUCM1
             action complete
            entry 3
            match-address 732
            prefix
            dst-adjacency CUCM2
            action complete
            exit
        entry 4
            match-address 908
            prefix
            dst-adjacency CUCM2
            edit replace 609
            action complete
            exit
        complete
    active-call-policy-set 5
```

CAC Policies

Call Admission Control (CAC) policies determine whether a call event should be allowed or rejected, based on the limits that are configured in the CAC policy for a particular network.

The primary uses of a CAC policy are:

- Preventing DoS attacks
- Implementing service-level agreements (SLAs)

Preventing DoS Attacks

CAC policies are used to defend load-sensitive network elements against potentially harmful levels of load, such as DoS attacks and mass media phone-ins.

Implementing SLAs

CAC policies are used to police the SLAs between organizations and ensure that the network utilization levels are not exceeded.

A CAC policy can be applied to any type of call event. If an event is not granted by a CAC policy, the Cisco Unified Border Element rejects the call event and returns the appropriate error code.

Note Only call admission events are configured in CAC policies. Other call events, such as number analysis and routing are configured in call policies.

The following example shows how to configure a CAC policy to ignore the bandwidth field of media streams. Ignoring the bandwidth field allows the Cisco Unified Border Element to downgrade a media stream from Secure Real-Time Transport Protocol (SRTP) to Real-Time Transport Protocol (RTP).

```
sbc MY_SBC
    sbe
    secure-media
        ….
        ….
        ….
    cac-policy-set 1
        description Ignore the  bandwidth field in SDP
        first-cac-table BW
        first-cac-scope call
        cac-table BW
        table-type policy-set
        entry 1
            media bandwidth-field ignore
            action cac-complete
    active-cac-policy-set 1
```

SIP Profiles

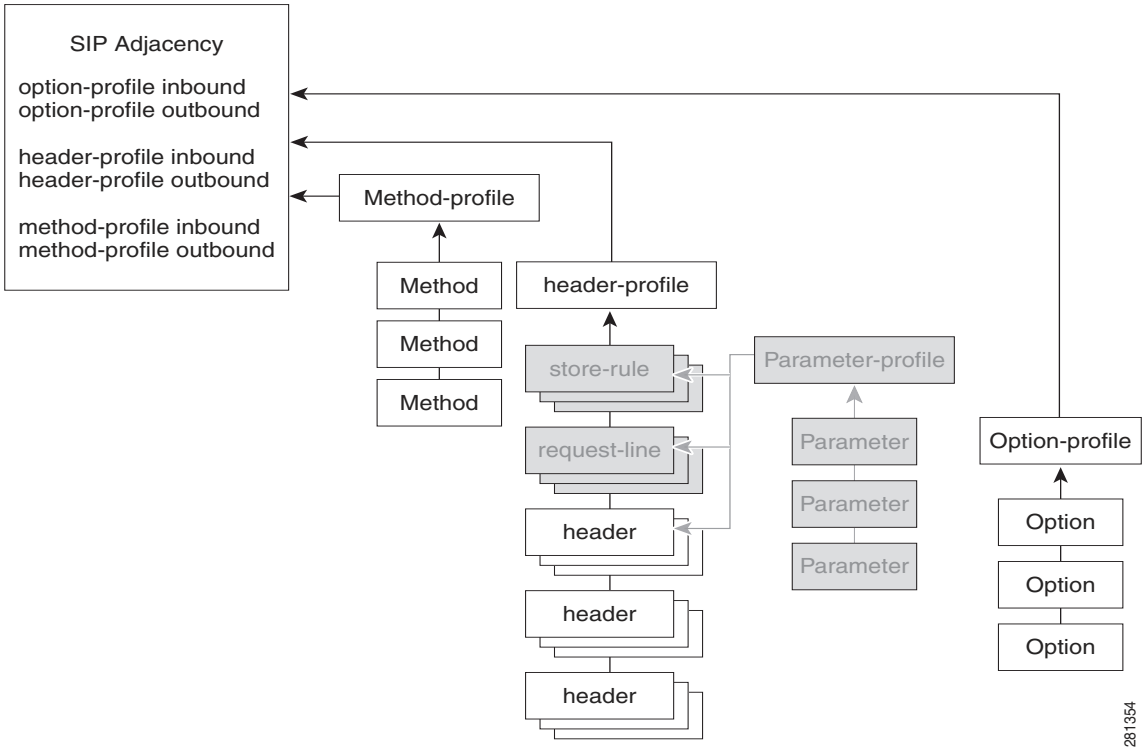
A SIP profile can be used to create a whitelist or a blacklist that contains a list headers or methods, and the actions to be performed on them. Whitelists are used to accept requests. Blacklists are used to reject requests.

The following types of SIP profiles are possible for use in whitelists or blacklists:

- Header profile
- Method profile
- Parameter profile
- Option profile

Figure 2 shows the various profiles and how they are attached to a SIP adjacency. Header-profiles can be associated with individual methods also, but in our example, the header-profile is associated directly to the SIP adjacency. Profiles must be associated to an ingress SIP adjacency and to an egress SIP adjacency.

Figure 2 Method, Header, Option Profiles Attached to an Adjacency



Note Parameter-profiles are associated directly to headers, but a parameter-profile is not used in the Telepresence example in this document. Thus, parameters are grayed out in Figure 2.

The Telepresence example in this document uses the following two whitelists and no blacklists:

- Method profile whitelist
- Header profile whitelist

Each header or method entry in the list may optionally be assigned one of the following actions:

- Pass
- Reject

Whitelists use only the pass action. Blacklists use only the reject action.

A header profile is a list of predefined headers that are passed or rejected using a whitelist or blacklist.

A method profile is a list of predefined methods that are passed or rejected using a whitelist or blacklist.

An option-profile is a list of predefined options that can be passed or rejected by placing it in a whitelist or blacklist. In our Telepresence example, the required Telepresence options, TIMER and REPLACES, are passed in the method-profile whitelist.

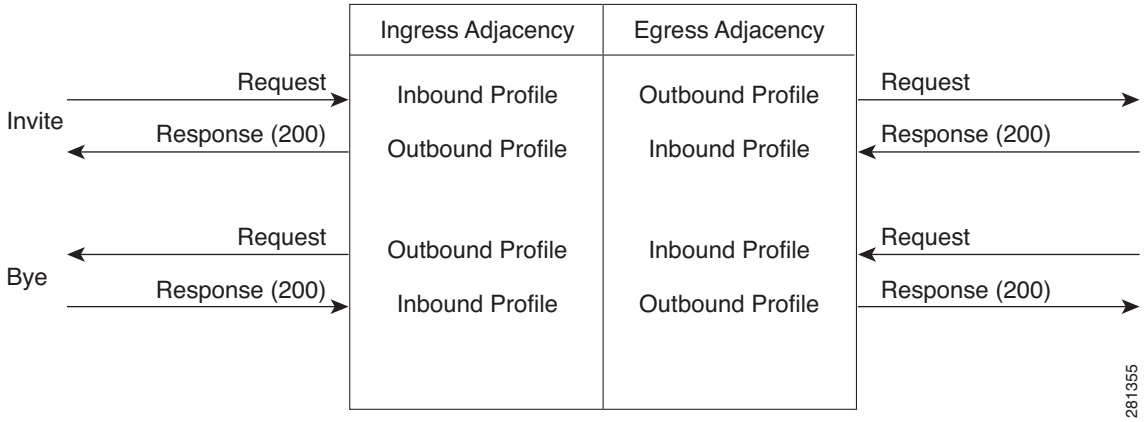
A whitelist is created using the **sip header-profile** command, adding the headers or methods as entries, and then assigning the pass action to each entry.

A method profile whitelist applies to an entire SIP message. Method-profile actions override default profile behavior.

A header profile whitelist applies only to single lines in a SIP message. A header-profile can match any part of the header, but it can only replace the entire header.

Profiles must be applied on both the inbound and outbound sides of each adjacency. Figure 3 shows the flow of profiles between adjacencies during a call.

Figure 3 Flow of Profiles During a Call



All headers are passed, stripped, or modified before they are processed by the Bye Reponse(200) on the ingress adjacency. All messages are passed, stripped, or modified after they are processed by the Bye Reponse(200) on the egress adjacency, before they are sent to the line.

Note For the header and method actions to be able to act on messages arriving on the ingress side, the headers and methods must first be passed from the inbound profile on the ingress side.

The following example shows how to attach whitelists to the inbound and outbound profiles.

```
adjacency sip CUCM1
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1

adjacency sip CUCM2
    header-profile inbound PASS-HEADERS
    header-profile outbound PASS-HEADERS
    method-profile inbound method1
    method-profile outbound method1
    option-profile ua inbound option1
    option-profile ua outbound option1
```

A profile cannot be deleted while it is attached to any adjacency. You can see which adjacencies are using a profile by entering the following show commands:

- show sbc sbe sip method-profile
- show sbc sbe sip essential-methods

Header Profile

In the following header profile white list, all the listed headers are configured to be passed.

```
sbc MY_SBC
    sbe
    secure-media
        …
    sip header-profile PASS-HEADERS
        description "pass non-essential headers"
        header Allow entry 1
            action pass
        header Min-SE entry 1
            action pass
        header Reason entry 1
            action pass
        header SERVER entry 1
        action pass
        header DIVERSION entry 1
        action pass
        header Allow-Events entry 1
        action pass
        header Remote-Party-ID entry 1
        action pass
        header Session-Expires entry 1
        action pass
        header session-expiry entry 1
        action pass
        header RESOURCE-PRIORITY entry 1
        action pass
```

Table 2 provides a description of three of the PASS-HEADERS white list header entries.

Table 2 Description of Three Entries in the PASS-HEADERS White List

Header	Description
header SERVER entry	Contains information about the software used by the user agent server (UAS) to handle the request.
header DIVERSION entry	Allows implementation of feature logic based on who diverted the call.
header RESOURCE-PRIORITY entry	Helps prioritize access to SIP-signaled resources during periods of emergency-induced resource scarcity.

Method Profile

In the following method profile white list, the methods are configured with actions and the profile is configured with options:

```
sbc MY_SBC
    sbe
    secure-media

    sip method-profile method1
        description "pass default methods"
        pass-body
        method INFO
            action pass
        method OPTION
            action pass
        method UPDATE
            action pass
    sip option-profile option1
        description "pass default options plus TIMER"
        option TIMER
        option REPLACES
    …
```