CHAPTER 10

Dial Plan

Revised: June 08, 2010; OL-19142-02

The dial plan is one of the key elements of a Unified Communications system, and an integral part of all call processing agents. Generally, the dial plan is responsible for instructing the call processing agent on how to route calls. Specifically, the dial plan performs the following main functions:

- Endpoint addressing

  Reachability of internal destinations is provided by assigning directory numbers (DNs) to all endpoints.

- Path selection

  Depending on the calling device, different paths can be selected to reach the same destination.

- Calling privileges

  Different groups of devices can be assigned to different classes of service, by granting or denying access to certain destinations.

- Digit manipulation

  In some cases, it is necessary to manipulate the dialed string before routing the call.

- Call coverage

  Special groups of devices can be created to handle incoming calls for a certain service according to different rules (top-down, circular hunt, longest idle, or broadcast).

For general dial plan guidance and design considerations, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

IPv6 and Unified CM Dial Plans

The deployment of IPv6 with Cisco Unified Communications Manager (Unified CM) affects two areas of dial plan functionality:

- IPv6 addressing for SIP route patterns
- Path selection considerations for IPv6 calls over IPv6-capable networks

SIP IPv6 Route Patterns

Cisco Unified CM can use SIP route patterns to route or block both internal and external calls to SIP endpoints. SIP route patterns can use the destination domain name, an IPv4 address, or an IPv6 address to provide a match for call routing.

A SIP request to call a device can take either of the following forms:

- Using an address:

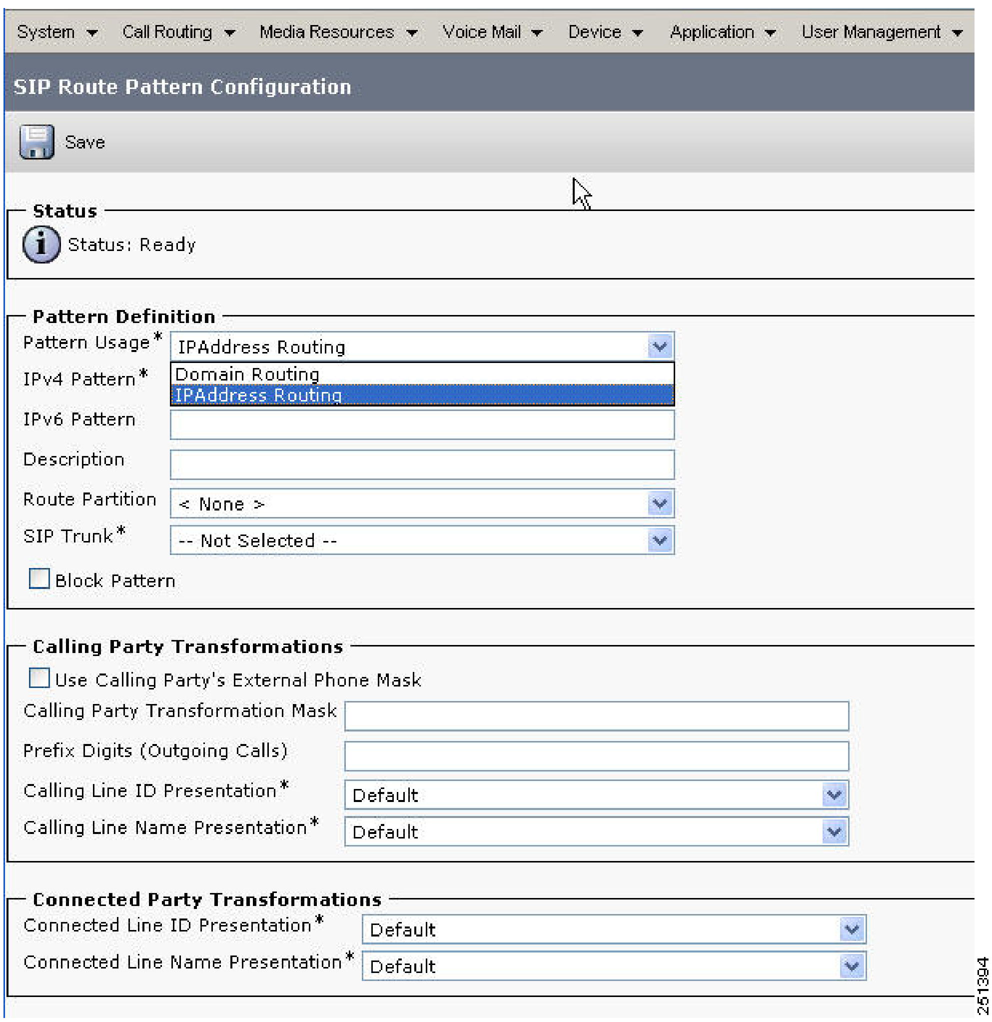
  INVITE sip:5001@2001:0db8:2::1 5060 SIP/2.0

- Using a domain name:

  INVITE sip:5001@example.com 5060 SIP/2.0

To process the SIP request, the Unified CM administrator can add domains, IP addresses, and IP network addresses, and associate them to SIP trunks (only), as shown in Figure 10-1. This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.

Figure 10-1 SIP Route Pattern Configuration in Unified CM



The following guidelines and examples apply to SIP route patterns:

- Domain name examples:
  - example.com
  - my-pc.example.com
  - *.com
  - rtp-ccm[1-5].example.com
- Valid characters for domain names:

  [, -, ., 0-9, A-Z, a-z, *, and]
- If domains names are used, then DNS must be configured in the Unified CM cluster.
- IPv4 address examples:
  - 192.168.201.119 (explicit IP host address)
  - 192.168.0.0/16 (IP network)
- IPv6 address examples:
  - 2001:0db8:2::1 (explicit IPv6 host address)
  - 2001::/16 (IPv6 network)
- Valid characters for IPv6 addresses:

  0-9, A-F, :, and /

Path Selection Considerations for IPv6 Calls

If you create an IPv6 route pattern, then that route pattern must be associated with an IPv6-capable SIP trunk. Likewise, the campus network or WAN that the IPv6 call traverses must be IPv6-capable.

Call Routing in Cisco IOS with SIP IPv6 Dial Peers

The following example shows a typical Cisco IOS IPv6 dial peer. Note that Alternative Network Address Types (ANAT) has been configured on this dial peer, thus allowing either an IPv4 address or IPv6 address to be negotiated for media. The session target can be configured with only one address, either IPv4 or IPv6.

```
dial-peer voice 1 voip
 description **** SIP Trunk to CUCM ****
 destination-pattern 5...
 voice-class sip anat
 session protocol sipv2
 session target ipv6:[2001:db8:caf0:101:21b:78ff:fe7a:5d86]
 session transport tcp
 dtmf-relay rtp-nte
 no vad
```

For a complete example of Cisco IOS ANAT configuration and IPv6 dial peers, see Configuring Cisco IOS Gateways, page D-1

Emergency Services

Cisco Emergency Responder is used to locate (by access switch or IPv4 subnet) IP devices that make emergency calls. Cisco Emergency Responder supports IPv4 only. Cisco Emergency Responder can support dual-stack devices by using the IPv4 address of the device. IPv6-only devices are not supported.

Cisco Emergency Responder interfaces with the following components:

- A Unified CM cluster by the following methods:
  - SNMP, to collect information about its configured phones
  - JTAPI, to allow for the call processing associated with redirection of the call to the proper PSAP gateway
- The access switches (through SNMP) where the phones associated with Unified CM are connected.