Dial Plan

Dial Plan Overview

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

  Sometimes, 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 Collaboration Solution Reference Network Design (SRND), available at Link.

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

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:

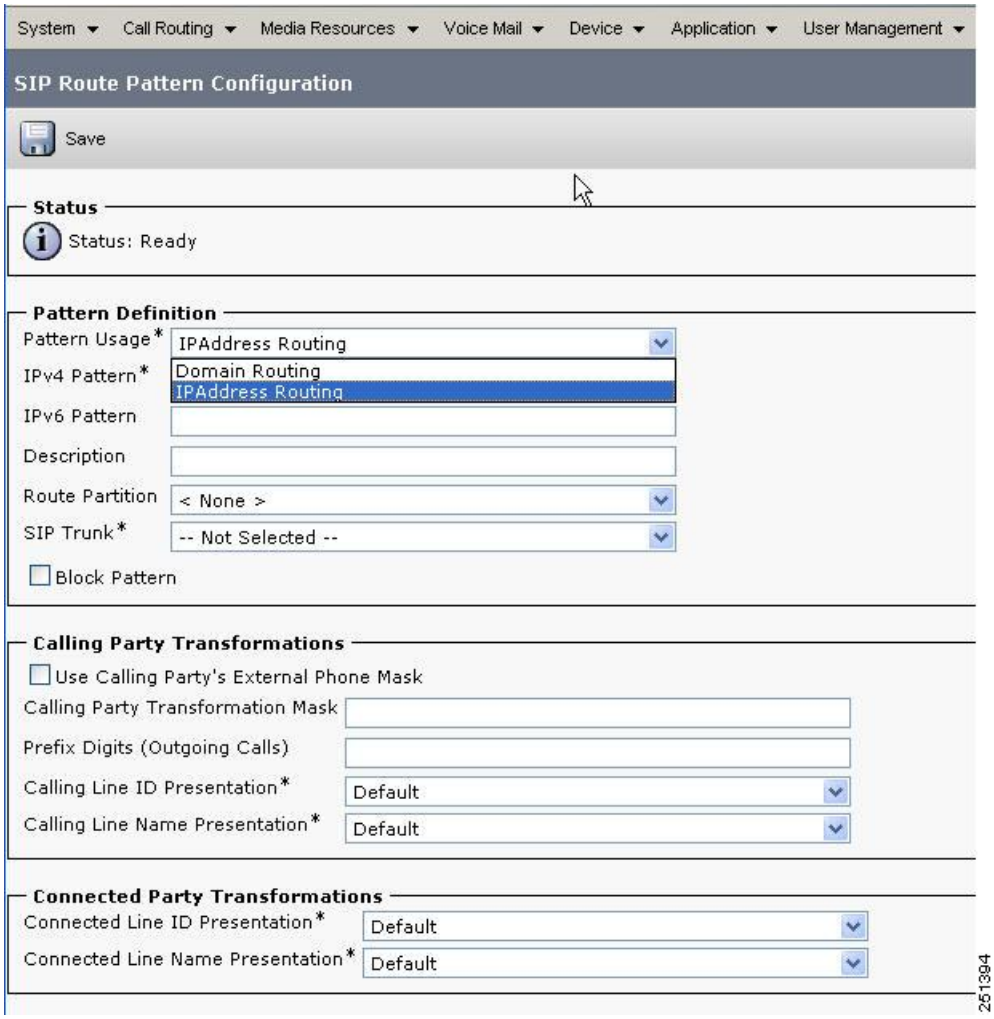
  INVITE sip:5001@2001:0db8:2::1 5060 SIP/2.0

- 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 the following figure. This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.

Figure 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.

Emergency Services

Cisco Emergency Responder (Emergency Responder) can track the IPv6-only phones through the switch port-based tracking, or access point-based tracking, or as manually configured phones. For the switch port-based tracking, Emergency Responder can talk to Cisco switches configured as the IPv4 address or IPv6 address through the SNMP protocol. Access point-based tracking requires the IPv6-only phone to communicate its upstream infrastructure information to Unified CM. For more information on Access Point Configuration and Discovery, refer to the Cisco Emergency Responder Administration Guide.

Emergency Responder tracks registered endpoints in Unified CM and provides Emergency Call Treatment for reaching correct PSAP and with correct Location information.

Emergency Responder interfaces with the following components:

- A Unified CM cluster by the following methods:
  - JTAPI, SNMP V3/V2, and AXL using IPv4 interface, to collect IPv6 information about its configured IP Phones. Emergency Responder and Unified CM are IPv6-aware.
  - JTAPI, to allow for the call processing associated with redirection of the call to the proper PSAP gateway.

- The access switches (through SNMP IPv4 or IPv6) where the phones associated with Unified CM are connected. Unified CM is IPv6-aware to communicate with Emergency Responder using IPv4 transport. The Emergency Responder to Switch interface is IPv6, supporting SNMP V3/V2.

Emergency Responder Limitations for IPv6-Only Endpoints

Some limitations for IPv6-only endpoints include:

- A call coming to Emergency Responder from an analog phone must be connected to an IPv4 gateway.
- Teleworker and off-premises features work only with IPv4.