SA 9122: Restrict Public-Private Network Connections (Restrict Toll Bypass) – Application Notes

Contents

I. Overview 4

II. Terminologies and acronyms 4

III. Detailed description 6

a. Fundamental concepts 6

b. Cardinal rules 7

a. Inter-PBX toll compliance 7

b. *Auto* classification 9

IV. Support for resources 9

V. Supported Communication Manager features 11

VI. SA9122 Administration 11

a. Screens to administer SA9122 11

b. Enabling SA9122 13

c. Administering Locations 13

d. Administering Network Regions 13

e. Administering location of stations 14

f. Administering location of trunks and type of trunks 14

VII. Feature limitations 15

VIII. Best Practices 16

a. Administering IP network on Locations 16

b. Setting up Gateways and SBCs 17

c. Setting up Multi-Location Routing Tables 17

d. Configuring Adjuncts 17

e. Configuring Trunks 17

f. Configuring Session Manager 17

g. Tail End hop off 18

h. Multi-geography Communication Manager 18

IX. Configuration scenarios 19

a. Legacy multi-Communication Manager configuration 19

b. Simple Avaya Aura® configuration 23

c. Signaling between Communication Manager, Session Manager and other entities 27

d. Call flow between Communication Manager and Session Manager 30

e. Call flow between Communication Manager and Session Manager (multiple entities and multiple links)..... 31

SA 9122: Restrict Public-Private Network Connections (Toll Bypass) – App Notes

I. Overview

The Restrict Public-Private Network Connections (SA9122) is a Communication Manager Release 6.3 special application feature. Communication Manager 6.3 is delivered as part of Avaya Aura® 6.2 Feature Pack 2. This feature provides a solution to address the toll fraud regulations in certain countries, especially India. When enabled, SA9122 ensures that PSTN trunk and VoIP calls across locations do not merge in a single call, thus, making Communication Manager compliant with toll regulations.

An Avaya Aura® solution is a federated solution. That is, there is no central point of intelligence; the intelligence is distributed across multiple elements. For an Avaya Aura® solution to be compliant, each network element must be compliant.

With SA9122, Communication Manager as a network element is 100% compliant as of 6.2 Feature Pack 2.

In Communication Manager Release 6.3.8, the solution has been enhanced to support limited network compliance. With a network of IP Office V9.1 or later and CM 6.3.8 or later, the Avaya Aura® network supports federated compliance to a limited extent. This allows for inter-PBX calls to be on-net and compliant with the regulation. For more information see the Inter-PBX toll compliance and Federated call scenario sections and for features limitations, see the **Error! Reference source not found.** section.

Note: *This feature is an enabler but not a guarantee of toll compliance. Also, failure to configure the feature as per the guidelines mentioned in this document will increase the risk of toll fraud.*

II. Terminologies and acronyms

Term/Acronym	Meaning
AWOH	Administered Without Hardware. AWOH telephones are virtual stations administered on the server. Useful for certain group or team features, such as pickup and bridging.
CO	Central Office. The place where telephone companies terminate customer lines and locate switching equipment to interconnect those lines with other networks.
CM	Communication Manager. A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media

Term/Acronym	Meaning
	gateways and analog, digital, and IP-based communication devices.
Communication Manager (CM) gateways	CM gateways can be H.248 gateways or traditional gateways. These gateways connect to and are controlled by Communication Manager. These gateways provide station and trunk connectivity.
CUG	Closed User Group. Private groups of telephone subscribers who can make or receive calls within the group.
DECT	Digital Enhanced Cordless Telecommunications (Digital European Cordless Telecommunications) is a digital communication standard, which is primarily used for creating cordless phone systems.
ISDN-PRI	Primary Rate Interface (PRI) is a standardized telecommunications service level within Integrated Services Digital Network (ISDN) to carry multiple DS0 voice and data transmissions between a network and a user.
ISDN-BRI	Basic Rate Interface (BRI, 2B+D, 2B1D) is an Integrated Services Digital Network (ISDN) configuration for subscriber lines that are same as the lines used for plain old telephone service.
H.323	An ITU defined IP based signaling protocol for audio and video communication. Used between Communication Manager and H.323 phones.
PHS	Personal Handy Phone System. A lightweight wireless telephone that functions as a cordless phone at home and as a mobile phone outside. The Personal Handyphone system also handles voice, fax, and video signals.
PSTN gateways	An entity that connects to the PSTN network on one side and to the Aura network on the other. A PSTN gateway can be an SBC, IP Office, or any other Avaya or a 3rd party gateway.
PSTN POI	PSTN Point of Interconnect where the PSTN line is connected to the enterprise. PSTN POI is usually a gateway or an SBC.
REMO	An enterprise or a hosted communication solution provider uses SIP Remote Office Solution (REMO) to provide fully functional Avaya communication services to an employee working from a remote location over the public Internet without VPN connectivity.
SBC	A **s***ession* **b***order* **c***ontroller* (SBC) is network equipment that can also be considered as a SIP-aware firewall. It controls real-time session traffic between networks. SBCs facilitate the transmission of real-time session traffic outside a NAT device or firewall boundaries. SBCs secure voice and video communications, presence information, and instant messaging. SBCs also safeguard SIP signaling elements against threats and data overload.

Term/Acronym	Meaning
SM	Session Manager. A SIP routing and integration server that is the core component within the Avaya Aura® solution.
SIP	Session Initiation Protocol. A very popular signaling standard for voice over IP. Driven by IETF. Avaya Aura® is built on the foundation of SIP.
IPO	IP Office. IP Office version 9.1 is Toll compliant when it operates independently (Branch) or in Centralized or Hybrid mode with Aura core.

III. Detailed description

a. Fundamental concepts

SA9122 is implemented at the connection layer of Communication Manager. SA9122 is built on two fundamental concepts inherent to Communication Manager:

- **Location of a user (party)** – All stations and trunks have locations.
  - For TDM resources, such as analog, DCP, and ISDN devices, the location is inherited from the gateway to which the resources are connected.
  - For IP devices, the location is configured by network mapping or by static administration.
    - Network mapping is mapping a range of IP addresses to a location.
    - Static administration is mapping an individual station or signaling group to a location.

- **Type of a user (party)** – There are two types of users: stations and trunks.
  - Stations are internal users, also known as enterprise users, CUG, or private users.
  - Trunks can be internal (within the enterprise) or external (public network). ISDN, H.323, and SIP trunks are classified as one of the following:
    - Public trunk: used when the far-end connects to the Public PSTN cloud. CO trunks (trunks administered as type CO) are public by default.
    - Private trunk: used when both ends of the trunk are within the enterprise, for example, inter-office trunks.
    - Universal trunk: used when calls across trunks do not require toll compliance checks. This trunk type is available for Communication Manager Release 6.3.
    - Auto trunk: used to indicate whether the calling user is a public user or private user on a per call basis. You can use auto trunk when you want to allow the toll compliance check to be performed at the destination PBX, rather than at the point of exiting from Communication Manager.

Introduced, in Communication Manager Release 6.3.8, the *auto* trunk type is available only for SIP trunks.

b. Cardinal rules

SA9122 works on the following rules:

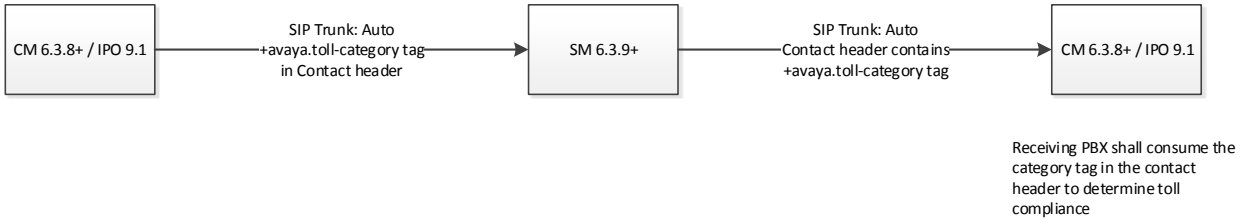
Existing parties in call	New party type	Rules
One or more Public trunks	**Public or Private**	If a public party is already on a call, all parties must belong to the location of the public party. If location of the new party is same as the location of any public trunk already on the call, the calls are allowed. As a corollary to this rule, all public trunks in the call will have the same location.
All Private users	**Public**	If all the parties on a call are private users, a public party can join the call only if the location of the public party is the same as that of all the private parties. If the location of the public party is not the same as that of the private parties, the public party cannot join the call.
All Private users	**Private**	If all the parties in a call are private users, a new private party **can join** the call irrespective of the location of the private party. Calls between private parties are always allowed.

a. Inter-PBX toll compliance

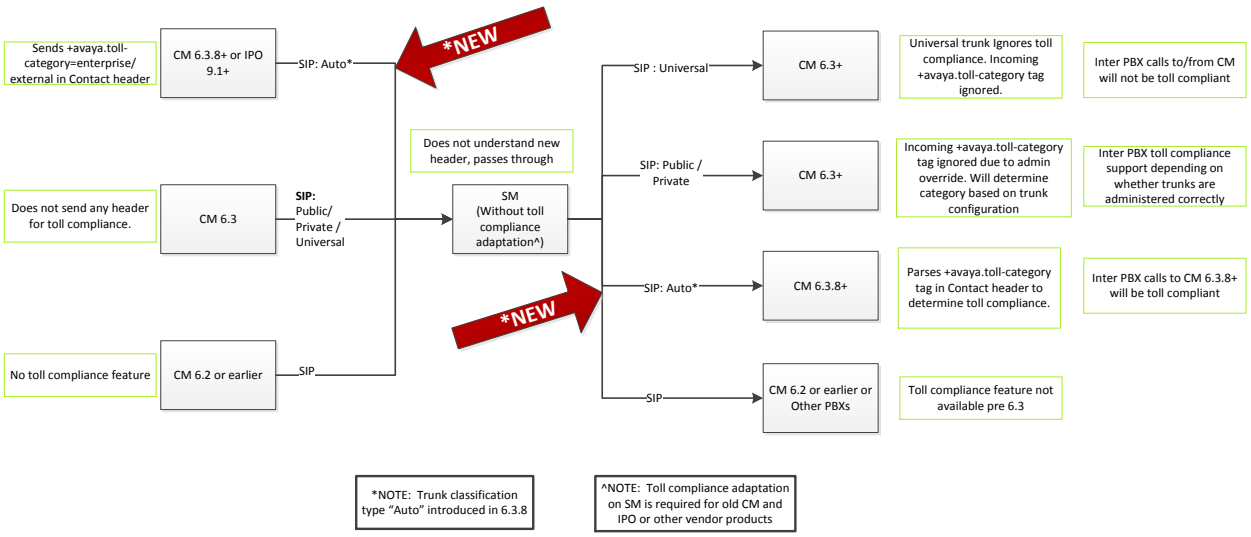
With Communication Manager Release 6.3.8 and later, inter-PBX calls are toll compliant. IP Office Release 9.1 supports inter-PBX toll compliance. Federated compliance is achieved by sending the caller's location and type (enterprise or public) to the far end PBX. With this information, the destination PBX can determine whether the call can be allowed to terminate at a given destination or if certain features can be allowed for this call. Federated compliance has certain limitations. For more information on limitations, please see the limitations section.

In an Avaya Aura® architecture, deploy IP Office 9.1 in any of the following three supported types of deployments: Centralized branch deployment, Distributed branch deployment, or Mixed branch deployment. In all of the above modes, the federated compliance with Aura Core is supported.

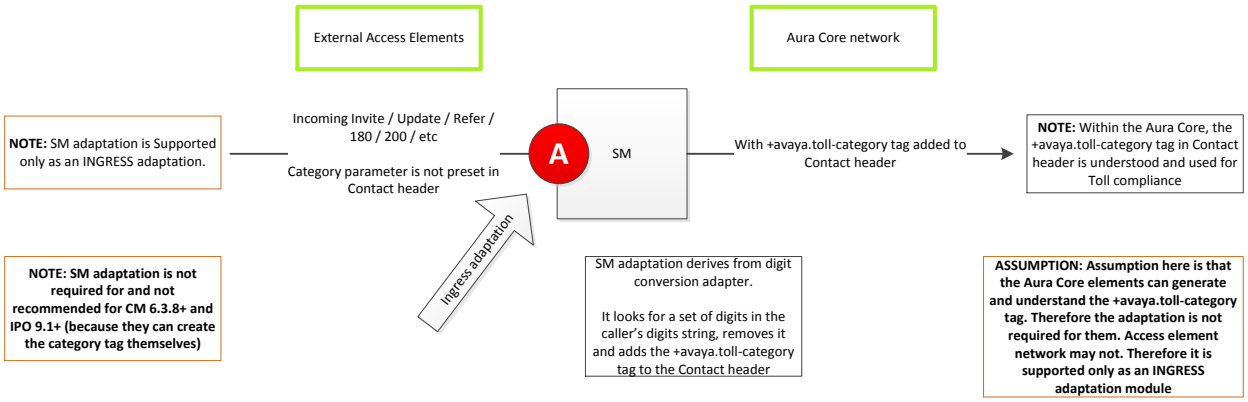
High level multi-PBX toll compliance



Toll compliance in Aura network

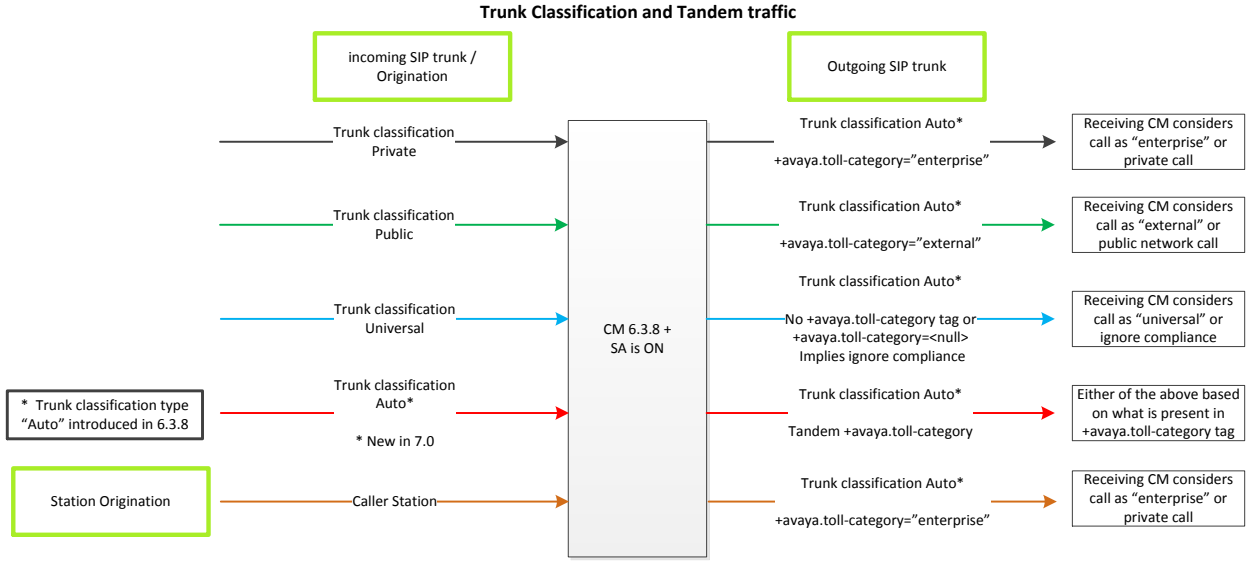


Other PBXs can be included in this "compliance net" if they understand the special SIP signaling used by Communication Manager and IP Office. If they do not, Avaya APS can be engaged to write an adaptation module on SM (using the pluggable adaptation module capability of SM) that will allow them to participate in this federated toll compliance feature. The adaptation module will need to be developed as follows:



b. *Auto* classification

With the new *Auto* classification, the behavior of Communication Manager as for station traffic and as a tandem node is shown in the following image.



IV. Support for resources

Resource type	Supported	Not supported
Stations	• Analog • DCP • H.323 • SIP	• DECT • AWOH • PHS • ISDN BRI

Resource type	Supported	Not supported
Endpoints	• Audio • Video • H.323 soft phones and deskphones • SIP soft phones and deskphones, including Advanced SIP telephony-capable endpoints	Any H.323 or SIP endpoint that can do local conferencing on its own, which means that the media is mixed locally. The endpoints do not involve Communication Manager to set up a conference call.[1]
Gateways	All gateways supported with Communication Manager 6.3	—
PSTN Trunks	• CO • ISDN-PRI • H.323 • SIP	• ISDN-BRI • R2MFC
Enterprise Trunk	• SIP • ISDN-PRI • H.323	• ISDN-BRI • R2MFC • CO
Adjuncts or Application servers	• Messaging servers directly connected to Communication Manager or Session Manager • Network Messaging servers[2] • Conferencing servers[3]	—
Communication Manager or other PBXs	Network of Communication Manager servers or other PBXs connected via ISDN, H.323, or direct SIP[4]	Partial support of federated compliance in an Avaya Aura® network.

Notes:

1. For endpoints with local conferencing capabilities, administer the endpoints in such a way that they are toll compliant. You can configure only a single line appearance on them or enable LNCC or do not allow them access to any PSTN resource by putting them in a remote location. For more information, see Administering location of stations.
2. In a network consisting of a Network Messaging server, messaging calls from other servers to a central Communication Manager server are supported.
3. Since a conference server by itself is not toll compliant, a solution must have two conference servers: one for public calls and the other for CUG calls.
4. Each Communication Manager server or PBX must be compliant with toll regulations independently. As of Communication Manager 6.3.8 and later and IP Office 9.1, limited

federated compliance is possible in the network. For more information, see the Federated call scenario section.

V. Supported Communication Manager features

Feature types	Supported
Station features	• Transfer and Conference • Call forward • Call coverage • Exclusion • Team button • Call pickup
Logical partitioning features	• Tenant • Class of Restriction (COR) • Class of Service (COS)
Contact center features	All features
Mobility features	• EC500 • Enterprise Mobility User (EMU) • 1X Mobile (all modes) • Soft Phone (on any device – cell phone, Tablet or PC)

VI. SA9122 Administration

a. Screens to administer SA9122

Most of these fields already exist in Communication Manager. All the fields are not added for SA9122. The following table provides the information about the fields that are used to administer SA9122.

Screen	Purpose	Fields
Special Applications	To enable the Special Application feature SA9122.	(SA9122) - Restrict Public-Private Network Connections (Toll Bypass)
Locations	To administer locations.	• ARS Prefix 1 Required For 10-Digit NANP Calls • Location No • Name • Timezone Offset • DST • City/Area • Attd FAC • Loc Parm (Location Parameter) • Disp Parm (Display Parameter) • Prefix • Proxy Sel Rte Pat
IP Network Region	To map network regions to locations.	Location
IP Network Map	To classify IP addresses in Network Regions/Locations.	• IP Address (From: To:) • Subnet Bits Network Region • VLAN • Emergency Location
Media Gateway	To assign a location to the media gateway.	Location
Cabinet	To assign a location to the port network.	Location
Trunk Group	To classify the type of trunk as private, public, or universal.	SA9122: For Toll Compliance, Treat As: **Note**: This field is available only when the **(SA9122) - Restrict Public-Private Network Connections (Toll Bypass)** field is set to **y**.
ISDN PRI Signaling Group	To administer the far-end location.	Far-end location **Note**: This field is available only when the **(SA9122) - Restrict Public-Private Network Connections (Toll Bypass)** field is set to **y**. If the **Far-end location** field is left blank, the near-end location shall be considered as a fallback option^.
Signaling Group (SIP	• To administer the far-end network region (NR).	• Far-end Node name • Far-end Network Region

Screen	Purpose	Fields
and H.323)	• To administer Near-end node name.	• Near-end Node-name **Note**: If the **Far-end Network Region** field is blank, then the NR of the near-end node is considered as a fall-back option.

^: The fallback option will be available in a future release.

b. Enabling SA9122

Before you begin

1. Check if you have licenses for the Multilocation feature. This feature is necessary for SA9122 to work. For licenses, contact Avaya Account Representative.
2. When configuring a network of Communication Managers or an Avaya Aura® solution, have a centralized and a unique dial plan. Call routing is much simpler if a unique enterprise-wide dial plan is used.
3. Configure a consistent network location map across entities. For example, for a given IP subnet, Communication Manager and Session Manager must be configured to map the IP subnet to the same location.

Procedure

On the System Parameters Special Applications screen, set the **SA 9122 – Restrict Public- Private Network connections** field to **y**.

c. Administering Locations

Procedure

On the Locations screen, administer the locations as per your network configuration. For example, if you have enterprise users in Pune and Delhi, you can add locations “Pune” and “Delhi”.

d. Administering Network Regions

Procedure

On the IP Network Region screen, administer the location number to which the IP network region belongs.

Note: An IP network region can be a core NR or a stub NR. Communication Manager considers the location of the parties on the call for toll compliance checks. The type of the NR does not matter. For more information about core NR and stub NR, see the Avaya Aura® Feature Description Guide.

e. Administering location of stations

Procedure

- For analog and DCP stations, configure the location of the gateway or port network to which the stations are connected.
  - On the media gateway screen, administer the location of the media gateway. On the cabinet screen, administer the location of the cabinet (port network).
- For H.323 and SIP stations, configure the IP address based on the location. Map the IP ranges to the location of the H.323 or SIP station.
  - On the IP Network Map screen, administer the IP address ranges as according to the network configuration. For. e.g. 10.10.2.2 to 10.10.2.254 in NR1 (NR1 is mapped to Location Pune).

    Note: Do not configure the location on the station screen. Leave the field blank.

- For SIP stations with local conferencing capabilities:
  - If the endpoint is administered as an OPTIM station, administer them in a location that does not have PSTN resource, similar to how VPN users are configured. See Configuring Session Manager.
  - If the endpoint is not administered as an OPTIM station, configure Session Manager to route calls over a private trunk to Communication Manager so that Communication Manager disallows PSTN access to the endpoints.

  Note: Analog conference phones, such as B149, use Communication Manager to do conference calls. These phones do not have local conferencing capabilities. Third-party H.323 endpoints with local conferencing capabilities are not supported with this feature.

  For more information about using B149 conference phone, visit support.avaya.com and see *Avaya B149 Conference Phone*, 16-603923.

f. Administering location of trunks and type of trunks

Procedure

1. Configure the far-end location of trunks. For public trunks, the far-end location must be the location of the city or the gateway to which the trunk is connected.
   a. On the Signaling Group screen, administer the **Far-end Location** field for ISDN PRI.

      Note: This is a new field introduced by SA9122.

   b. On the Signaling group screen, administer the Far-end Node name for SIP and H.323.

Note: If you do not configure the location of trunks, the system uses the near-end location of the trunk. If the trunk is a PRI trunk, the system uses the location of the gateway.

2. Configure the type of trunks.
    a. On the Trunk Group screen, set **SA9122 Restrict Public Private Network Connections, For Toll Compliance, Treat As:** to **public**, **private**, **universal,** or **auto**, depending on the trunk usage.

VII. Feature limitations

SA9122 is **not supported** in the following scenarios:

1. If you have multiple Communication Manager Systems in one location, each Communication Manager must identify the location with a unique name. If not, then the solution might not be toll compliant.
2. Multi-device Access feature is not supported.
3. CM-FS and application sequencing are not supported.
4. When a conference call is distributed between two servers, Communication Manager and another server, calls cannot be toll compliant. Since a conference will have members on either side of the trunk, calls cannot be 100% toll compliant. Assume in a 3-party conference, a user dials a bridge hosted on another server – say another CM or AAC. In this case, the conference has few members on either side of the trunk. This case is not supported.
5. SIP Contact Center features are not supported.
6. Bridge call appearances across locations are not supported, that is, the primary station and the bridge call appearance must be in the same location.
7. Splitting media streams across locations is not supported. The assumption is that all media channels of an IP phone, H.323 and SIP terminate at the same location.
8. Advanced SIP Telephony-2 (AST-2) features are not supported.
   Softphones in the SIP telecommuter mode is not supported because the endpoint hides the topology of the telecommuting leg.

Federated call scenario

(Pune) CM_A ----------SM----------CM_B (Bangalore)

SIP User_B from Bangalore moves to Pune. The network map of Session Manager maps User_B to Pune location. The home Communication Manager of the user is CM_B, and hence, CM_B processes all calls for this user.

1. Call 1
    a. SIP User_B from Bangalore calls SIP User_A in Pune.
    b. The call comes to CM_A via Session Manager.
    c. CM_A rings user_A at desk and at EC500 destination.

d. User answers on EC500 handset.
e. CM_B sees this call as Enterprise user B calling an Auto trunk. It has left the compliance decision to CM_A
f. CM_A receives the call from Enterprise user A in Pune, therefore terminates the call at enterprise user_B in Pune and their EC500 destination.

2. Call 2
    a. User_B calls SIP User_C in Bangalore.
    b. This is an enterprise call, and hence is allowed.
    c. CM_B sees this call as Enterprise user B in Pune calling Enterprise user_C in Bangalore

3. User_B Merges Call 1 and Call 2
    a. This call will be allowed to merge by CM_B because
    b. CM_B sees only part of call1; it does not see that call 1 has a public trunk as one of the parties.
    c. In future releases of Communication Manager, the terminating CM will communicate the far end user's category information to the originating PBX for better federated toll compliance.

VIII. Best Practices

a. Administering IP network on Locations

1. Divide the enterprise network into individual locations. Each location will be considered as an individual unit for toll compliance. The Cardinal rules apply to these locations.
2. Define a network region for individual locations.
3. Assign a location to each IP network region.
4. Configure the IP network and DHCP server so that IP devices, such as deskphones, softphones, and wireless devices, get IP addresses within a range.
5. To classify IP addresses as devices in a network region and, in turn, in a location, configure the range of IP addresses on Communication Manager, in the IP Network Map table.

    Important!
    - Do not administer the **Location** field on the station screen. Leave the field blank.
    - The location names configured in Communication Manager, on the Locations screen, **must exactly** match the location name as configured in Session Manager. The name is case sensitive.

b. Setting up Gateways and SBCs

1. Deploy Session Border Controller (SBC) for each location if the PSTN calls are routed through the SBC. If a location does not have a media gateway or port network, no PSTN termination is possible to users in that location. For information about deploying SBC, see *Installing and Configuring Avaya Aura® Session Border Controller*.

c. Setting up Multi-Location Routing Tables

1. Configure AAR or ARS routing tables for each location of the enterprise. In a multi-location enterprise, it is mandatory to configure multi-location routing to ensure toll compliance. The routing tables facilitate routing through local trunks, thus, enabling toll compliance.

d. Configuring Adjuncts

1. If an adjunct that provides conferencing service, then it needs to be compliant in itself. For Modular Messaging (MM), disable outbound dialing. For Avaya Aura® Conferencing (AAC) and Meeting Exchange (MX), use the outbound dialing with caution and prior verification.
2. A point: Configure the messaging server over a 'universal' trunk if the server is directly connected to Communication Manager.
3. If the server is connected to Communication Manager via Session Manager, configure the CM-SM trunk as **auto**.

e. Configuring Trunks

1. Configure the CM-SM trunk as **auto**.
    i. On the Trunk Group screen, set the **SA9122 Restrict Public-Private Network Connections (Toll Bypass) For Toll Compliance, Treat As:** field to **auto**.
2. Disable TAC dialing of trunk. It is recommended that you allow trunk access via AAR or ARS.
    i. To disable direct trunk dialing, on the Trunk group screen, set the **Dial Access** field to **n**.

    Note: TAC is primarily used for troubleshooting to provide direct access to the trunk group. SIP trunks do not support TAC dialing.

f. Configuring Session Manager

1. Configure Session Manager to do source-based routing. The routing is based on the signaling location of the originator. For detailed information about administering source-based routing, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.
2. Typically, VPN gateways cannot determine the real location of an incoming connection and provides one IP from a global pool of IP addresses. In this case, configure a pool of IPs for the remote location.

3. If the VPN gateways or an SBC provides deterministic IP ranges for connections based on where the user is accessing it, then classify the IP ranges into locations that have PSTN resources.

   Important - Do not assign a PSTN resource to the remote location. There should be no gateway or SBC in the remote location that connects to the public PSTN network. Note that 'Remote' is just a name given to the location. The location name can be any valid name.

g. Tail End hop off

1. SA9122 is the exact opposite of the tail-end-hop-off feature. With the tail-end-hop-off feature, PSTN routing happens at the last enterprise boundary. Therefore, turn on SA9122 only if required.

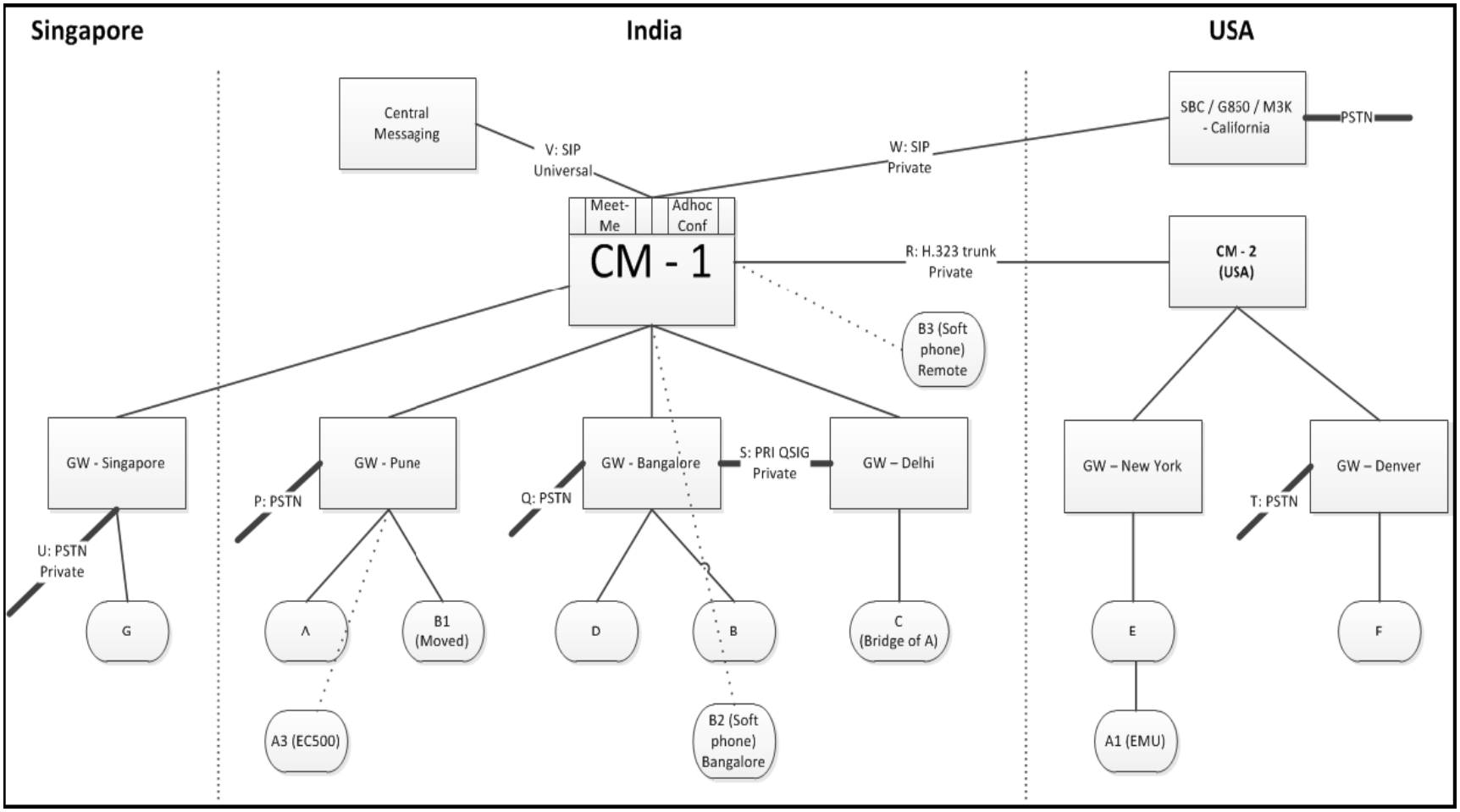
   Note: Toll compliance check might not be required on individual trunks. To not have a toll compliance check on for a trunk, set the **SA9122 Restrict Public-Private Network Connections (Toll Bypass) For Toll Compliance, Treat As:** field to **universal**.

h. Multi-geography Communication Manager

1. When a Communication Manager server controls multiple geographies and SA9122 needs to work only in one location, for example, India, configure all the trunks connected to gateways outside India boundary as **private**.
   i. On the Trunk Group screen, set the **SA9122 Restrict Public-Private Network Connections (Toll Bypass) For Toll Compliance, Treat As:** field to **private**.

IX. Configuration scenarios

a. Legacy multi-Communication Manager configuration



Configuration overview

The above configuration consists of one (or more) Communication Manager in India and one (or more) Communication Manager outside India. In India, the enterprise users are located in different locations, for example, Pune, Bangalore, and Delhi. Each location has a media gateway and a PSTN trunk terminating into that media gateway. Communication Manager-1 is directly connected to Central Messaging server.

Note: The location names are for the purpose of explaining the configuration. A customer setup can have completely different names.

Guidelines

1. Communication Manager-1 or any Communication Manager in India will have the special application enabled to support toll compliance.
2. Communication Manager -2 or any Communication Manager outside India will not have the special application enabled.

Configuring Communication Manager for SA9122

To configure Communication Manager for the SA9122 feature, perform the following steps:

Gateways and Locations

1. On the Locations screen, create multiple locations – Pune, Delhi, Bangalore, Singapore, and Remote.

   Note: The case of letters used for the location names of Communication Manager and Session Manager must be the same. For example, if the location name on Communication Manager is 'Pune', SM should not have the location name as 'pune'.
2. On the Media Gateway screen, add the location of each gateway by assigning the location number that is mapped to the location name.

IP-network map and Locations

1. On the IP Address Mapping screen, configure IP-network map with subnet ranges for each city. For example, the DHCP server is configured to assign IP addresses 10.10.2.2 to 10.10.2.254 to devices in Location 1 and 10.10.3.2 to 10.10.3.254 to devices in Location 2.
   a. Create rows in the IP-network map table.
   b. Configure the IP ranges and the IP network region in the location to which the IP range belongs.
2. Configure IP-network map with subnet ranges for remote users.

Note: VPN gateways or SBCs provide IP addresses to the devices connected to the enterprise from the public network. For example, IP addresses from 10.10.10.2 to 10.10.10.254 are assigned to these remote devices.

3. Configure a network map entry and point it to the remote location.

   Note: A remote location is a logical concept. A location that does not have any Communication Manager PSTN resources is considered as a remote location. There can be multiple remote locations. Also, a remote location can have any name. The name 'Remote' is just an example.

Stations

For DCP and analog stations:
No configuration is required for these stations. These stations inherit their location from the gateway they are connected to.

For H.323 stations:
On the Station screen, leave the **Location** field blank. Based on the IP address of the station, the station obtains a network region and a location.

Trunks

On the Trunk Group screen, set the **SA9122 Restrict Public-Private Network Connections (Toll Bypass) For Toll Compliance, Treat As:** field, to **Private**, **Public**, **Universal,** or **auto** depending on the **Trunk usage**

Scenario-specific trunk administration details are as follows:

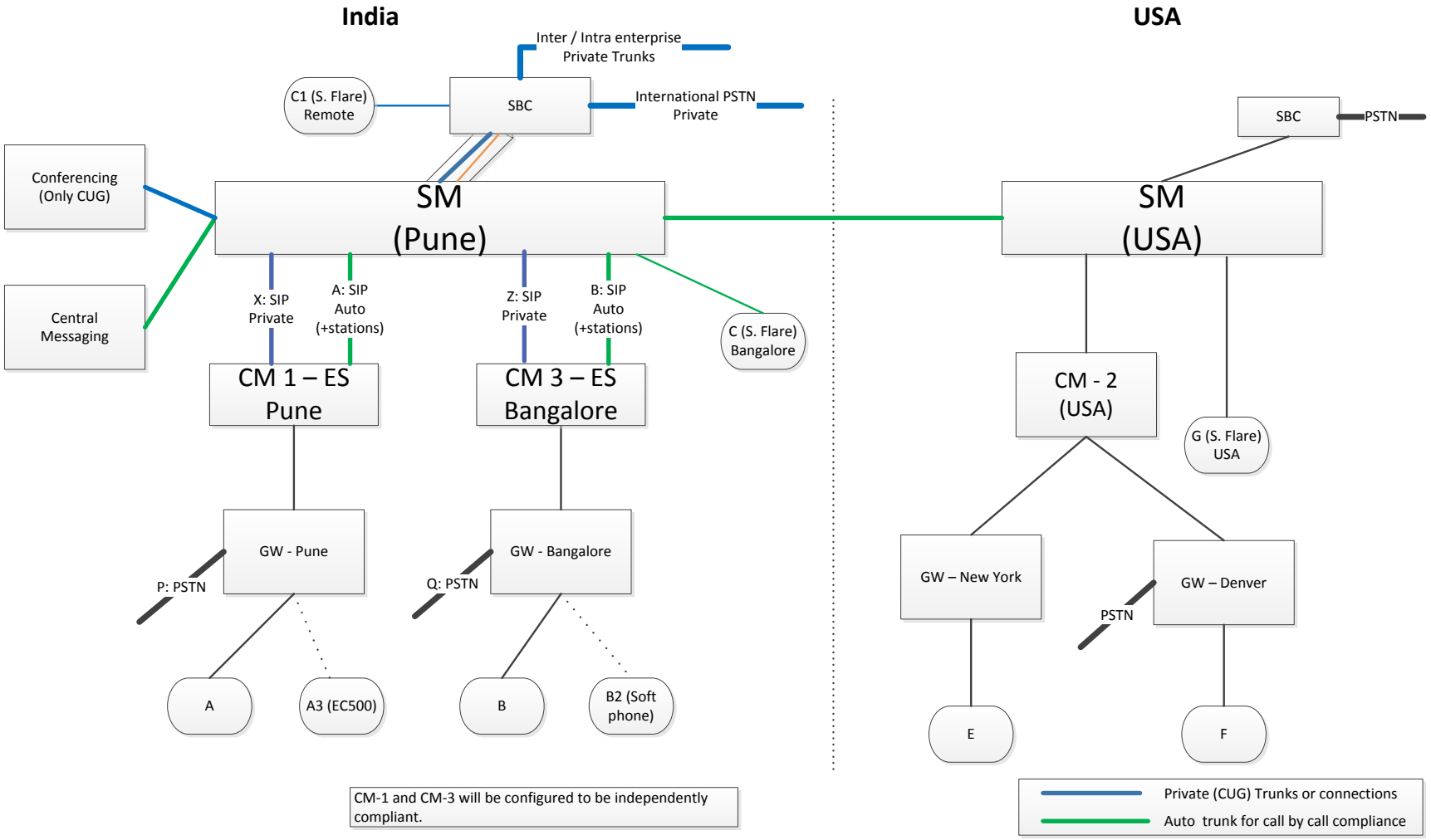
1. Configure the Far-end location on the Signaling Group page correctly. Delhi-Bangalore trunk group is inter-office, and hence, it is private.
2. On the Delhi end of the signaling group, configure the far-end as **Bangalore** and configure the near-end as **Delhi**. On the Bangalore end of the signaling group, configure the far-end as **Delhi** and configure the near-end as **Bangalore.**
3. Administer all PSTN-connecting trunk groups (Pune:P and Bangalor**e**:Q) as **public**, with far-end as the city or the gateway – Bangalore or Pune .
4. Administer the local PSTN trunk (U) connected to the Singapore gateway as **private**, and set the far-end location for this trunk as the **Singapore** location.

   Note: The Singapore gateway is connected to the local PSTN trunk, but from India **Communication Manager** and toll compliance perspective, the PSTN trunk is an enterprise trunk since the point of PSTN connection is not in India.

5. Similarly, administer trunks to CM-2 and SBC as **private** and the far-end location as **Remote**.

6. Administer the trunk to Messaging as **universal** since toll compliance checks on that trunk are not required.

b. Simple Avaya Aura® configuration



Configuration Overview

The Avaya Aura® configuration consists of one (or more) Communication Manager connected to Session Manager in India and one (or more) Communication Manager connected to Session Manager outside India. In India, the enterprise users are located in different locations, that is, Pune, Bangalore, and Delhi. Each location has a media gateway and a PSTN trunk terminating to that media gateway. CM-1 is connected to a Central Messaging server, an Avaya Aura® Conferencing server, and Session Border Controller (SBC) via Session Manager.

Note: The location names are for the purpose of explaining the configuration. A customer setup can have completely different names.

Guidelines

1. Communication Manager-1 or any Communication Manager in India will have the special application enabled to support toll compliance.
2. Communication Manager -2 or any Communication Manager outside India will not have the special application enabled.

Configuring Communication Manager for SA9122

See configuration steps for Legacy multi-Communication Manager configuration.

Configuring SIP Stations

1. In System Manager, create an origination and termination application sequence with Communication Manager as the SIP main entity. Ensure that there is only one application, that is, Communication Manager (CM) in the application sequence.

   Note: There can be many entities for the same Communication Manager instance. The selected Communication Manager instance will correspond to the universal trunk on the Communication Manager side.

2. Add a SIP user on Session Manager and assign to it the origination and termination application sequence of the corresponding Communication Manager.
3. On the Station screen, set the SIP Trunk to **aar** or **ars**.

   Note: There can be many entities for the same Communication Manager instance. The selected Communication Manager instance will correspond to the universal trunk on the Communication Manager side.

   For detailed information about adding SIP users, see the Adding users section in the *Administering Avaya* Aura® *Session Manager* guide.

Configuring CM-SM link

1. For routing SIP station traffic, on the Trunk group screen, set the field to **SA9122 Restrict Public-Private Network Connections (Toll Bypass) For Toll Compliance, Treat As:** auto for the Communication Manager side of the trunk. On the corresponding signaling group screen, it is recommended to set a value in the **Far-end Network Region** field. The far end NR in the SIG group indicates the location of the far end of this trunk connection.

   Note: In case of multiple links between a CM-SM pair, configure them all as TCP or all as TLS. There is a Communication Manager limit of 16 links with TLS.

Configuring the Avaya Aura® solution

To identify whether the far-end party across CM-SM link is public, private, universal or auto, multiple links from Communication Manager to Session Manager need to be tagged accordingly.

1. In System Manager, assign locations to Communication Manager and Session Manager. **Note**:
   a. Communication Manager uses the IP address mapping screen only for IP stations (H.323 and SIP). Therefore, on the IP ADDRESS MAPPING screen, each Communication Manager needs only those entries that belong to its stations. Session Manager must have mapping of the entire IP address range to locations for all the Communication Manager instances that are connected to this Session Manager.
   b. For calls from trunks, Communication Manager uses the location name from the P-Location header that is sent by Session Manager. Therefore, ensure that you have matched location names on Communication Manager and Session Manager.
2. To route station calls and call to other PBXs that support federated compliance

a. Create a trunk and entity link between Communication Manager and Session Manager to support routing for SIP stations and messaging. On the Trunk group screen, administer the trunk as **auto**. On the corresponding signaling group screen, it is recommended to set a value in the **Far-end Network Region** field

3. To route calls to CUG entities like conference bridges

a. Create a trunk and entity link between Communication Manager and Session Manager to support routing to all enterprise elements that are strictly private, for example, international SBC and other PBXs, since these private elements are toll compliant themselves.

b. Administer the CM-SM link as **private**. The far-end Network Region of this signaling group is **Remote** or any logical location name that does not have any CM PSTN resource assigned to it.

4. To route calls to SIP gateways / SBC that connect to public network

a. Create a trunk and entity link each for every public entity connected to the SM. For example, if there are 2 SBCs that connect to the PSTN cloud, one in Bangalore and one in Chennai, then 2 links are required between Communication Manager and Session Manager to support call routing to these two SBCs. One link will have far-end as Chennai and the other as Bangalore.

5. For all signaling groups to Session Manager, on the Signaling Group screen, set the **IMS** field to **n**. Only CM-ES is supported. Therefore, all signaling groups to Session Manager must have IMS set to **n.**

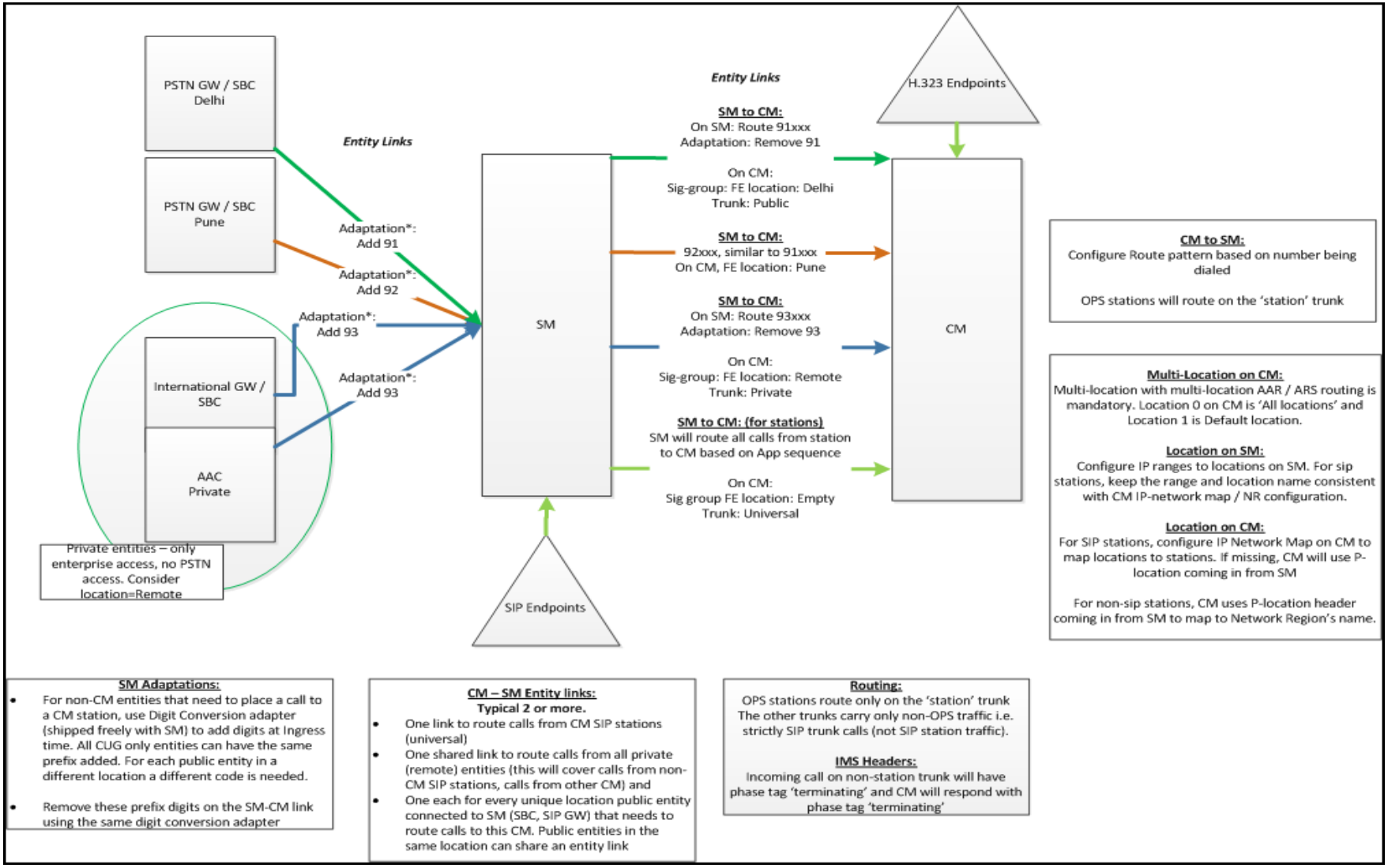
Related topics:

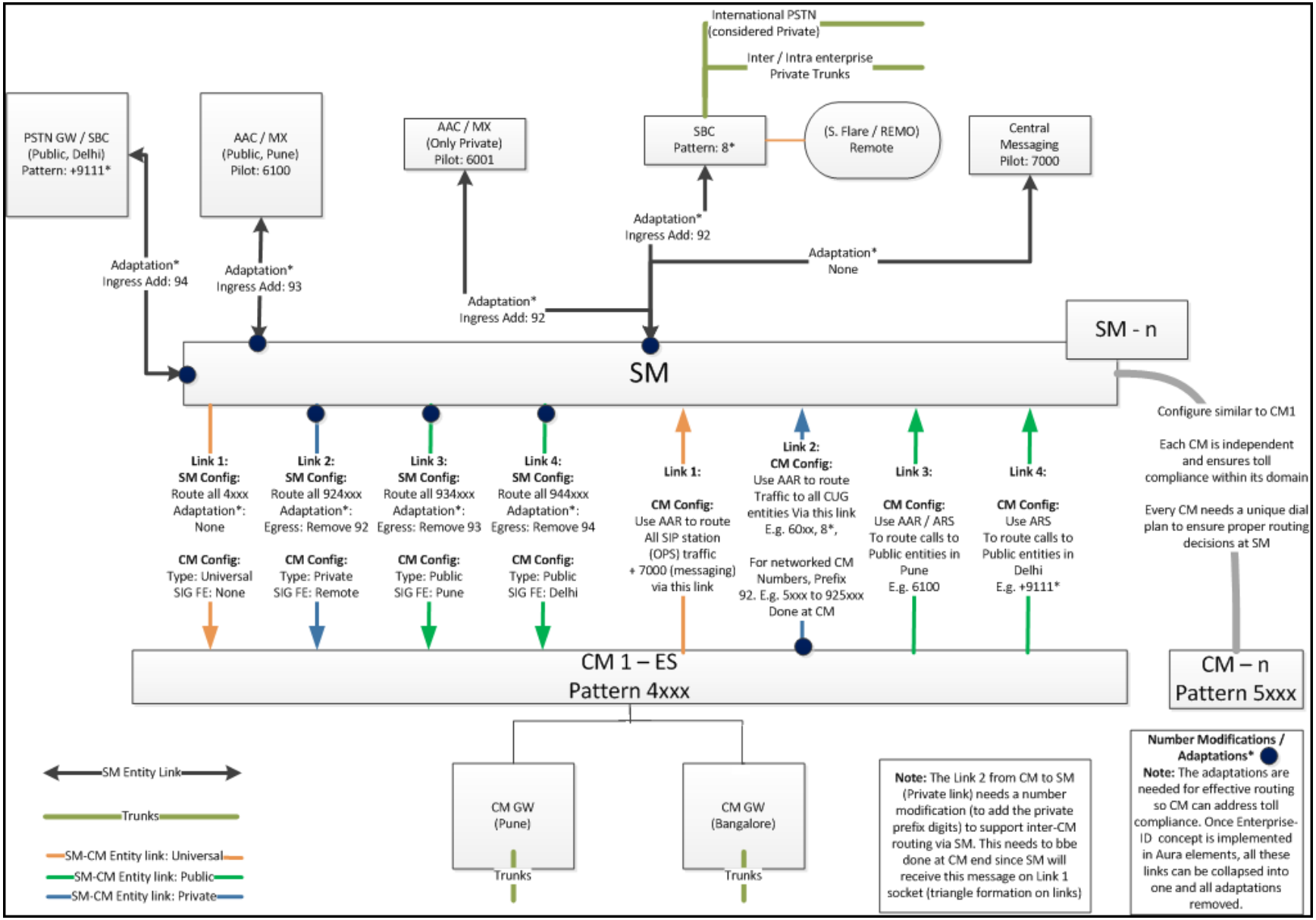
For diagrammatic representation of signaling and call flow, see:

- Signaling between Communication Manager, Session Manager and other entities
- Call flow between Communication Manager and Session Manager
- Call flow between Communication Manager and Session Manager (multiple entities and multiple links)

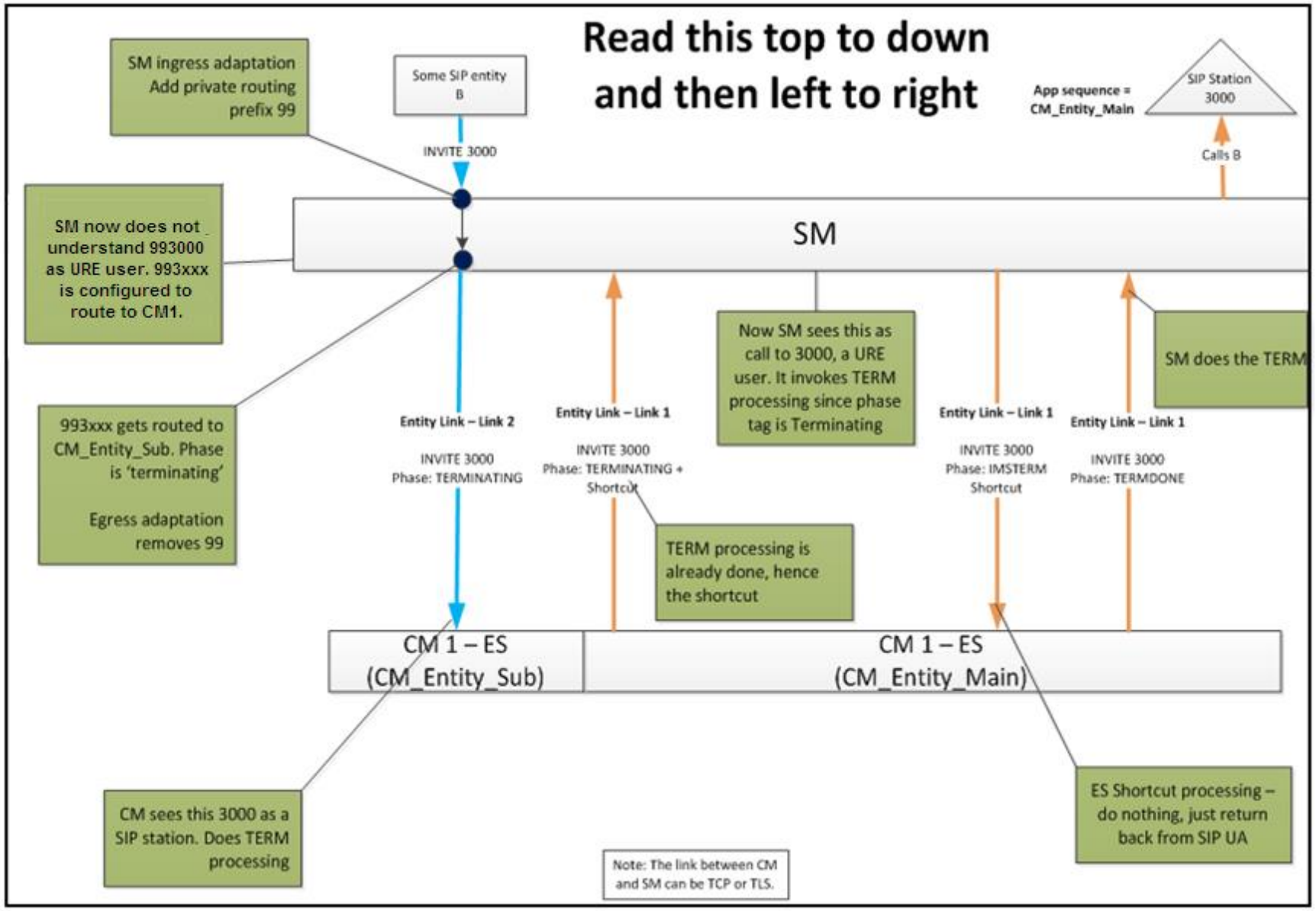
c. Signaling between Communication Manager, Session Manager and other entities

The adaptations or number modifications on Session Manager and Communication Manager are required to ensure that the calls get routed on the appropriate trunk based on the type of caller or the called party.


PSTN GW / SBC Delhi
PSTN GW / SBC Pune
International GW / SBC
AAC Private
Private entities – only enterprise access, no PSTN access. Consider location=Remote
Entity Links
Adaptation*: Add 91
Adaptation*: Add 92
Adaptation*: Add 93
Adaptation*: Add 93
SM
SIP Endpoints
Entity Links
SM to CM:
On SM: Route 91xxx
Adaptation: Remove 91
On CM:
Sig-group: FE location: Delhi
Trunk: Public
SM to CM:
92xxx, similar to 91xxx
On CM, FE location: Pune
SM to CM:
On SM: Route 93xxx
Adaptation: Remove 93
On CM:
Sig-group: FE location: Remote
Trunk: Private
SM to CM: (for stations)
SM will route all calls from station to CM based on App sequence
On CM:
Sig group FE location: Empty
Trunk: Universal
H.323 Endpoints
CM
CM to SM:
Configure Route pattern based on number being dialed
OPS stations will route on the 'station' trunk
Multi-Location on CM:
Multi-location with multi-location AAR / ARS routing is mandatory. Location 0 on CM is 'All locations' and Location 1 is Default location.
Location on SM:
Configure IP ranges to locations on SM. For sip stations, keep the range and location name consistent with CM IP-network map / NR configuration.
Location on CM:
For SIP stations, configure IP Network Map on CM to map locations to stations. If missing, CM will use P-location coming in from SM
For non-sip stations, CM uses P-location header coming in from SM to map to Network Region's name.
SM Adaptations:
For non-CM entities that need to place a call to a CM station, use Digit Conversion adapter (shipped freely with SM) to add digits at Ingress time. All CUG only entities can have the same prefix added. For each public entity in a different location a different code is needed.
Remove these prefix digits on the SM-CM link using the same digit conversion adapter
CM – SM Entity links:
Typical 2 or more.
One link to route calls from CM SIP stations (universal)
One shared link to route calls from all private (remote) entities (this will cover calls from non-CM SIP stations, calls from other CM) and
One each for every unique location public entity connected to SM (SBC, SIP GW) that needs to route calls to this CM. Public entities in the same location can share an entity link
Routing:
OPS stations route only on the 'station' trunk
The other trunks carry only non-OPS traffic i.e. strictly SIP trunk calls (not SIP station traffic).
IMS Headers:
Incoming call on non-station trunk will have phase tag 'terminating' and CM will respond with phase tag 'terminating'


International PSTN
(considered Private)
Inter / Intra enterprise
Private Trunks
PSTN GW / SBC
(Public, Delhi)
Pattern: +9111*
AAC / MX
(Public, Pune)
Pilot: 6100
AAC / MX
(Only Private)
Pilot: 6001
SBC
Pattern: 8*
(S. Flare / REMO)
Remote
Central
Messaging
Pilot: 7000
Adaptation*
Ingress Add: 92
Adaptation*
None
Adaptation*
Ingress Add: 94
Adaptation*
Ingress Add: 93
Adaptation*
Ingress Add: 92
SM - n
SM
Configure similar to CM1
Each CM is independent and ensures toll compliance within its domain
Every CM needs a unique dial plan to ensure proper routing decisions at SM
Link 1:
SM Config:
Route all 4xxx
Adaptation*:
None
Link 2:
SM Config:
Route all 924xxx
Adaptation*:
Egress: Remove 92
Link 3:
SM Config:
Route all 934xxx
Adaptation*:
Egress: Remove 93
Link 4:
SM Config:
Route all 944xxx
Adaptation*:
Egress: Remove 94
Link 1:
CM Config:
Use AAR to route All SIP station (OPS) traffic + 7000 (messaging) via this link
Link 2:
CM Config:
Use AAR to route Traffic to all CUG entities Via this link
E.g. 60xx, 8*,
For networked CM Numbers, Prefix 92. E.g. 5xxx to 925xxx Done at CM
Link 3:
CM Config:
Use AAR / ARS
To route calls to Public entities in Pune
E.g. 6100
Link 4:
CM Config:
Use ARS
To route calls to Public entities in Delhi
E.g. +9111*
CM Config:
Type: Universal
SIG FE: None
CM Config:
Type: Private
SIG FE: Remote
CM Config:
Type: Public
SIG FE: Pune
CM Config:
Type: Public
SIG FE: Delhi
CM 1 – ES
Pattern 4xxx
CM – n
Pattern 5xxx
CM GW
(Pune)
CM GW
(Bangalore)
Trunks
Trunks
SM Entity Link
Trunks
SM-CM Entity link: Universal
SM-CM Entity link: Public
SM-CM Entity link: Private
Note: The Link 2 from CM to SM (Private link) needs a number modification (to add the private prefix digits) to support inter-CM routing via SM. This needs to bbe done at CM end since SM will receive this message on Link 1 socket (triangle formation on links)
Number Modifications / Adaptations*
Note: The adaptations are needed for effective routing so CM can address toll compliance. Once Enterprise-ID concept is implemented in Aura elements, all these links can be collapsed into one and all adaptations removed.

d. Call flow between Communication Manager and Session Manager



e. Call flow between Communication Manager and Session Manager (multiple entities and multiple links)

