Best Practice Recommendations for Network Regions

Table of Contents

Chapter 1: Introduction

Purpose

The Avaya Aura Communication Manager provides a facility for determining codec usage for various call flows and associating media resources with a specified set of devices. The facility for performing this function is the network region. This document provides guidelines and best practices for achieving a sound network region design, which is scalable, extensible for nearly all applications and follows the conventions established for Avaya network region design.

Intended Audience

This document is intended for Avaya Professional Services, Business Partners and Customers who design, configure and maintain network region configurations.

Chapter 2: Network Region Overview

A network region is a logical grouping of endpoints sharing common characteristics and resources. These endpoints may include:

- Processor Ethernet (PROCR)
- IP Phones
- Media Servers
- H.248 Gateways
- Port Network Media Resources
- C-LANS
- SIP and IP trunk connections for:
  - Modular Messaging/AAM
  - Other CMs/PBX's
  - Avaya Aura Conferencing/Meeting Exchange
  - Avaya Experience Portal
  - SBCs
  - G860s/SIP Gateways

Proper network region configuration is essential for optimal performance and support of all call flows that have an IP infrastructure component. Improper configuration of network regions can have significant adverse impacts, including call failures.

Proper Network Region design depends upon first achieving a good understanding of the underlying WAN and LAN topology used by the Avaya Aura components. This knowledge is essential as a good network region design emulates the underlying WAN and LAN topology. Network region best practices are based upon this premise. In general, a proper network region design addresses:

- Optimal media resource and codec selection
- Proper call admission control (CAC) calculations

- Efficient alternate gatekeeper list (AGL) generation.

Also related to network regions is the concept of locations. A location relates to geography, whereas a network region is associated with a network topology. Locations identify a distinct geography, primarily for call routing and unique dial plan purposes. A location may encompass multiple network regions, whereas the inverse seldom applies. As an example, a campus environment may include a unique network region per building with a single location for the entire campus. This enables the campus to share a ubiquitous dial plan while each building could then have its' own associated gateway with trunking and survivability capability.

A typical branch office would have a single network region and a single location. The naming and numbering of these would be the same as a best practice, in order to make the configuration intuitive to grasp.

2.1 Basic Design Considerations for Network Regions

By default IP endpoints are in network region 1. If left that way, all IP endpoints would share the characteristics defined by network region 1 and use the same resources. For nearly all solutions this is impractical for accommodating the differences in locations and/or network characteristics. Therefore multiple network regions must be configured. However, as network region 1 is the default and the main data center typically possesses a large quantity of media resources, the main data center normally occupies network region 1.

Some of the many reasons a design includes multiple Network Regions is for support of the following requirements:

- Varying bandwidth limitations across the network
- Need for media encryption
- Fax over IP/Modem over IP sensitivity and requirements
- Music on Hold and/or voice mail requirement for G.711 for high quality delivery
- Locations interconnected via WAN links
- Local trunks, local country settings, local E911
- Unique 802.1p, diffserv, port prioritization
- Different RTCP monitor requirements across the system
- Limiting RTP traffic across the WAN
- Distributed vs. centralized VoIP resource allocation
- Registration of a group of phones to a particular survivable site
  - Alternate gatekeeper lists (AGLs) with particular PE/CLANs
- Prevention of shuffling and/or hairpinning for service observing
- Preventing calling between groups of users if IP Connect
- Isolating CMS and other adjuncts from other network regions

Network regions are also used to group IP endpoints, sharing common characteristics and resources. Some reasons for grouping VoIP endpoints are as follow:

- Grouping of IP endpoints by codec set, i.e. one group of endpoints with the same codec set requirements are in one group while endpoints with different codec requirements are in different groups.
- Ensuring that specific VoIP (C-Lan or MedPro) and/or gatekeeper (G450 or G650) resources are dedicated to certain groups of IP endpoints or adjuncts.
- Grouping IP endpoints by VLAN and/or QoS settings (note: only if these settings are administered from CM).
- Grouping IP endpoints that point to a specific RTCP monitor addresses for VMON, i.e. other groups report to a different VoIP Monitoring Manager (VMM) Server.
- Defining the shuffling/hairpinning characteristics for groups of users (IP endpoints)

2.2 Direct Connected Network Regions

The connections between the network regions can be one of three types:

- Direct Connections
  - Used to specify call admission control (CAC) values
  - Used to specify the codec set to use when appropriate
- Indirect Connections
  - NRs connected via an intervening network region
  - The network region connection must be specified as directly connected to the intervening region adjacent to it.
  - Used to specify the codec set to use between the two indirectly connected network regions
- Not connected
  - Used for proper media selection when transcoding
  - Compliments use of the ip-direct field

While connections must be specified between any network region and its' adjacent region, interconnecting all NRs directly is not recommended as:

- The topology does not emulate the data network
- Unnecessary WAN traffic would occur from data center components as media resources will be pulled on a pro-rated basis from all sites instead of first using available resources within the same data center.
- Access control must be done statically for each point to point connection, which would likely either over or underestimate the total available bandwidth.

The figure below depicts a network configuration using all direct NR connections.

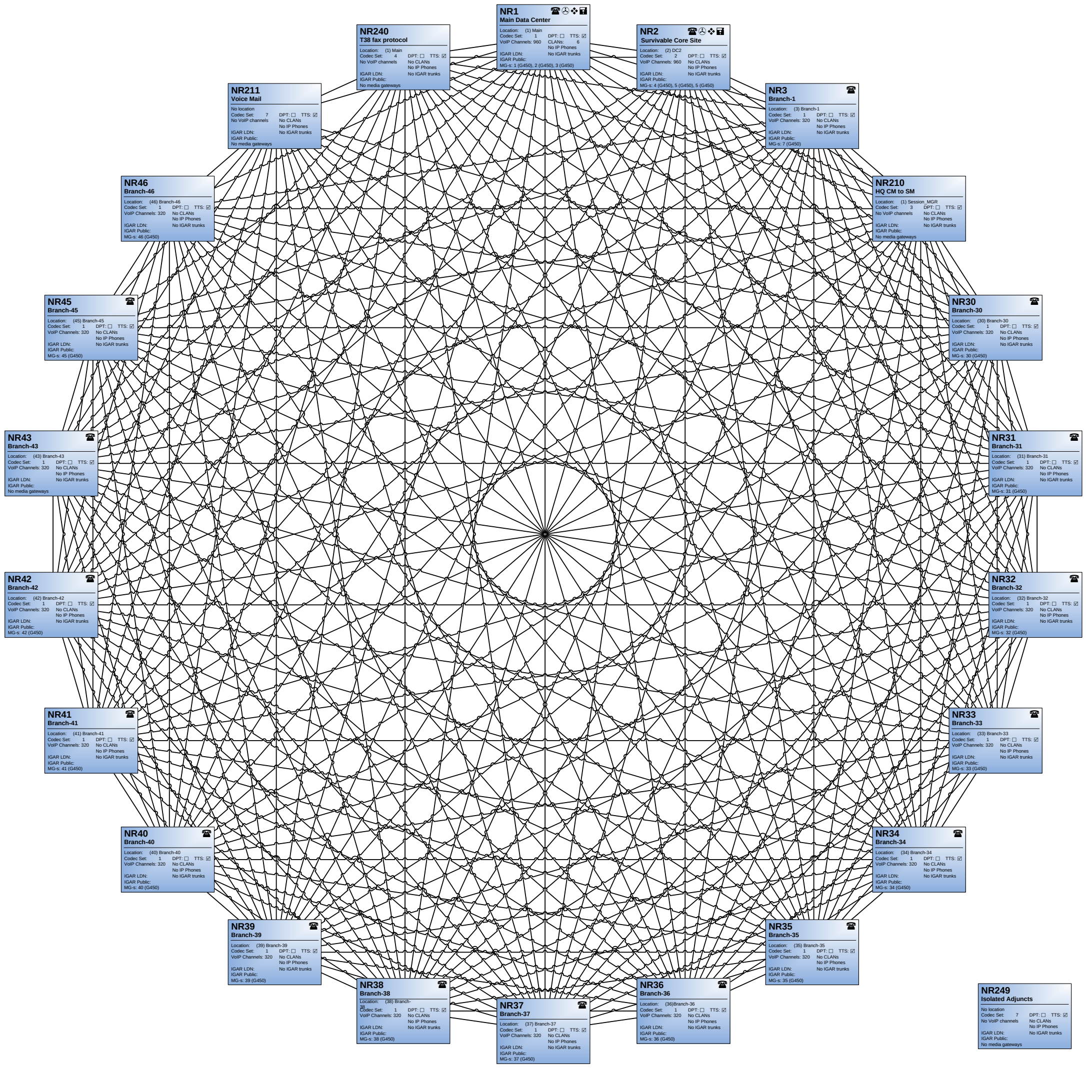


Figure 1 Direct NR Connections

While possibly aesthetically pleasing, the above configuration is also a nightmare to maintain and impossible to effectively design access control for. This is because values would need to be specified for each point to point connection and not the aggregate of the total offered traffic. That would likely result in imposing access control before bandwidth is exhausted or exhausting bandwidth before access control takes effect.

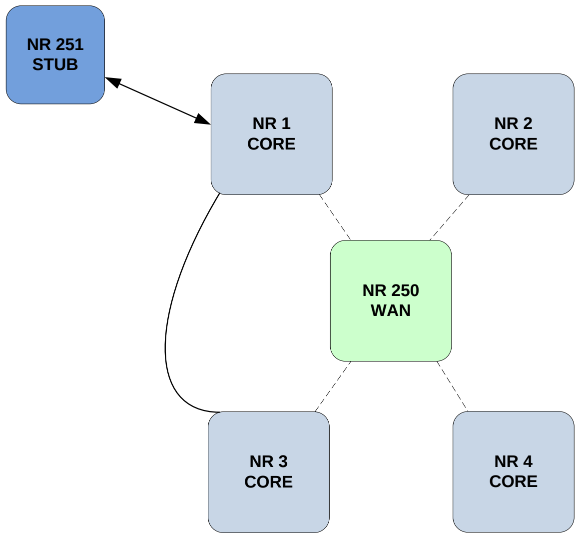
Stub Network Regions

With the introduction of CM release 6.3 network regions were expanded from 1-250 to 1-2000. The existing network regions 1 to 250 are referred to as Core network regions, the new NRs 251-2000 are referred to as stub network regions. A core region 1-250 can be configured as a stub. However that is not advisable considering the limited number of core regions and the large number of potential stub NRs.

Stubs are meant for IP phones and cannot contain Procr, a media gateway or media server. Stubs can only contain: IP Office branches, SIP and/or H.323 endpoints, third-party gateways, signaling group far end NRs or any combination of these.

A stub NR directly connects only to a single core NR and does not have defined pathways to any other edge network regions. This has the advantage of eliminating the need to configure multiple communication pathways to different network regions.

In the following diagram, when stub NR 251 needs to connect to core NR 3, NR 251 will follow NR 1's defined connection to NR3. No NR 251 to NR 3 path is specified.



2.3 Virtual Network Regions

An effective way to represent the WAN topology with network regions is through the establishment of a virtual network region. This virtual network region provides connectivity between the various site NRs in a similar manner to the way a WAN connects the various LANs.

The following diagram depicts the previous Direct NR Connections diagram after redesigning it with an intervening region present.

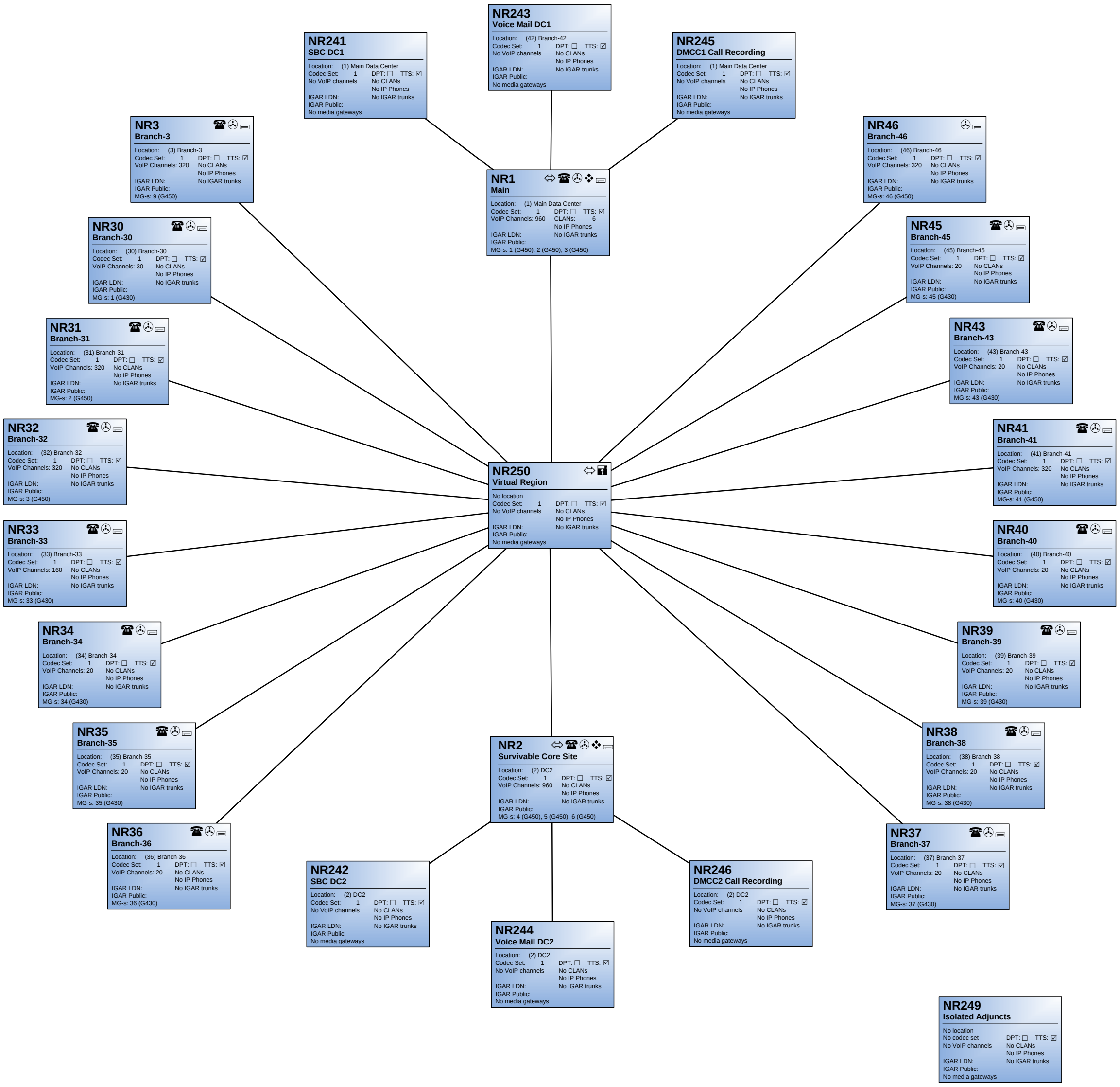


Figure 2 Virtual Network Region Configuration

Role of the Virtual Network Region

In the diagram above a virtual network region is established to represent the WAN. Remote branches in NRs 3-46 are each directly connected to the WAN NR 250 and indirectly connected to each other and the data centers via NR 250. Remote SIP endpoints connecting via an SBC use the site where the SBC is physically located as an intervening region to interface to the virtual NR. Similarly, VPN phones that interface internally via a VPN router reflect the topology of where the VPN router exists in the data network. If the VPN router exists at a data center, an NR directly connected to that data center would be used and that data center becomes the first intervening NR for the VPN router NR. If the VPN router interfaces via the WAN, The VPN router would use an NR that directly interfaces to the WAN virtual NR. In the latter configuration the VPN phones would obtain their media resources from all sites directly connected to the WAN virtual NR.

Connections to the WAN virtual network region are direct and can be used to specify bandwidth between a remote site NR and the NR associated with the WAN. With a single direct connection in place to a site NR, Call Admission Control can readily check total bandwidth used between that site and the virtual NR.

If an NR 3 phone calls a NR 42 phone, CM first constructs the NR path and then ensures that each leg of the path has sufficient bandwidth to support the call. In this example the virtual network region is intervening NR 250 between NR3 and NR42. By definition a virtual network region has no media; it is there to reflect the underlying WAN topology.

Intervening regions however, may have media and are configured to again reflect the underlying topology. Examples of where that holds true is with data center NRs 1 and 2, which serve as intervening regions and supply media for directly connected NRs. NR 1 and 2 are not virtual regions, although they supply the direct connection to the virtual region for the NRs that use NR 1 and 2 as intervening regions.

Data center applications such as SIP trunks and voice mail traverse through the data center NRs to connect to the remote branches. Applications use the media resources at the data center where they are collocated, thus minimizing WAN bandwidth consumption by the data center until connectivity needs to be established to the branch.

For solutions covering diverse geography it may be advisable to add an additional virtual region to localize traffic to a specific area. For example, Country A sites may all directly connect to NR 250. Then it may be practical to add a virtual NR 249 for direct connections to all Country B sites. NR 250 and NR 249 would be directly connected to each other. This would ensure that media would exhaust resources within one country before expanding the search for media resources to the other country.

2.4 CM Media Management Algorithms

It is useful to understand the CM algorithms used to manage media in arriving at an effective network region (NR) design. The algorithms used by CM are described below.

2.4.1 Media Resource Selection algorithm enhancement

The way CM selects media was enhanced from earlier CM releases. As a result design principles have also been updated. The following describes two of the enhancements made.

1. Prior to this enhancement, within any specific NR, there was a hard-coded preference for PN media resources over gateway media resources. So, where an NR contained both PN and gateway resources, the PN media resources were used until exhaustion before the H248 gateways were used. In some cases this resulted in a significant number of denied pegs as CM transitioned back and forth between selection of H248 gateways and PN resources. With this enhancement, all media resources for a network region are placed in a common pool and used according to their respective capacities. This also applies in release 7 to Avaya Media Server (AMS) resources which share this same pool.
2. The second enhancement addresses media allocation when direct or indirect media resources must be used. This enhancement was introduced via defsw112923 and applied back to CM 5.2.1. The NR allocation order preference formerly was:
    a. Use resources from the NR of the requesting endpoint.
    b. Use resources from NRs which are directly connected to the requesting endpoint.
    c. Use resources from NRs which are indirectly connected to the requesting endpoint.

The complication with Step c, was many regions were grouped into the same pool even though some indirectly connected network regions were closer and some further away. Two NRs may be connected thru up to 4 intervening regions.

For example NR 1 can be connected to NR 6 by up to 4 intervening regions: 1-2-3-4-5-6. NRs 1-6 are connected, but they are connected by 5 individual hops 1-2, 2-3, 3-4, 4-5, 5-6. NRs 1-3 are connected, but they are connected by 2 individual hops 1-2, 2-3. Both NR 3 and NR 6 are indirectly connected to NR 1 and hence when needing resources for an NR 1 endpoint, NR 1 is preferred 1st (0 hops), NR 2 second (1 hop) and then NRs 3,4,5,6 were treated equally. This resulted in non-optimal allocation of resources prior to the enhancement.

Following are examples that describe results after the two enhancements:

Example 1: endpoint and resources in the same NR.

- Given endpoints in NR1 with PN and GW resources existing in NR 1.
- PNs have a total capacity of 960 DSPs; GWs have a total capacity of 320 DSPs.
- Statistically select MedPro DSPs 75% of the time; choose GW DSPs 25% of the time.
- Statistically select means choose a random number between 1 and 1280 in this case (total capacity of MedPro DSPs + total capacity of GW DSPs).
- If random # is less than MedPro capacity, CM chooses a MedPro DSP, else chooses a GW DSP.

Example 2 - endpoint and resources in a single direct connected NR

- Given endpoints in NR 1 with no available DSP resources, PN resources and GWs exist in NR 2; NR 1 is directly connected to NR 2.
- Same operation as previous example.

Example 3 - endpoint in one NR, resources available in many directly connected NRs.

- Given endpoints in NR1 with no available DSP resources, PN resources and/or GWs exist in NR 2, NR 3.. NR X.
- NR 1 directly connected to NR 2, NR 3, NR X
- Step 1: statistically choose NR to pick from.
- Similar algorithm (add capacity across all NRs), pick a random number, which maps to NR Z.
- Step 2: within NR Z, select MedPro DSP or GW DSP based on the same rules as example 1 and 2

Example 4 - endpoint in one NR, resources available in many direct/indirect connected NRs.

- Given endpoints in NR 1 with no available DSP resources
- PN resources/GWs exist in NR 2,NR 3, NR X, NR 1 directly connects to NR 2, NR 3, NR X, i.e. 0 intervening regions
- PN resources /GWs exist in NR 20, N R21, and NR 22. NR 1 connects thru NR 250 to NR 20, NR 21, NR 22, i.e. 1 intervening region

- PN resources /GWs exist in NR30, NR31, and NR32. NR1 connects thru NR 250 thru NR 201 to NR 30, NR 31, and NR 32, i.e. 2 intervening region
- PN resources /GWs exist in NR40, NR41, and NR42. NR1 connects thru NR 250 thru NR 248 thru NR 249 to NR 40, NR 41, NR 42, i.e. 3 intervening region
    - Step 1 - find set of closest NRs. (i.e. smallest # of intervening regions/hops).
    - Step 2 - From the set of closest NRs statistically choose NR to pick from.
    - Step 3 - From the chosen NR, statistically choose a MedPro DSP or GW DSP

Example 4 is a compendium of the generic rules, incorporating all of the examples. These rules only apply to the initial allocation of DSP resources. Whenever a call already has ports established, existing rules that optimize the connectivity in relation to those ports continue to apply.

The main application for the direct and indirect allocation of resources is phone only NRs that are connected to all other NRs via an intervening NR that represents the WAN. In this case the phone is indirectly connected to multiple NRs with media including branch sites as well as data center sites. Prior to the enhancement, CM would allocate media to a phone, based on round robin selection of media in indirectly connected NRs rather than using media at the main data center.

With the new algorithm, the administrator can connect branch gateways to a network region that are in turn connected to the WAN NR. Assuming the following:

- Data Center 1 resources are directly connected to WAN NR 250.
- Phone only NR 100 is directly connected to WAN NR 250 as well.
- Branch GW NR 101 through NR 110 are all directly connected to NR 249 which in turn is directly connected to NR 250.
- From the NR 100 perspective, NR 1 media resources are one hop away, NR 101 through NR 110 resources are two hops away.

Therefore for the phone only NR 100, CM will prefer NR 1 resources, which are the shortest hop count away.

Following are a variety of algorithms used by CM Media Management

2.4.2 Algorithm used to select media for H.323 stations

- CM determines the NR of an IP Phone based on
    - ip-network-map
    - if no match, uses NR of registration point (in all cases for this document PROCR is the registration point)
- CM looks for media in the same NR as the IP Phone
- CM then looks for media in NRs directly connected to phone NR
- CM then looks for media in NRs indirectly connected to Phone NR

2.4.3 Algorithm used to associate SIP stations with Network Regions

A SIP Station or SIP Phone does not register to CM. It registers to Session Manager. Therefore CM cannot associate the SIP Phone with a network region until the SIP Phone is involved in a call. Depending upon administration options, CM may or may not retain the network region for the SIP phone after a restart. This is explained in more detail below.

CM determines the NR of a SIP Phone based on the following, by checking the first bullet item, then the next bullet item if the prior item is not configured, etc:

- ip-network-map
- P-Location Header
- The “Far-end Network Region” field on the ”signaling-group” form supporting the current active SIP phone call
- The physical resource (e.g. PROCR) supporting the current active SIP phone call. This is the final and default choice

Each SIP telephone call repeats the above selection process. The list below provides more detail of the process.

- The SIP Contract header in the initial Invite message or in the 180 Ringing or 200 OK SIP response message is used to search ip-network-map administration for an IP address match. If a match is found then the administered network region is assigned to that SIP phone. The network region assigned is also saved to the SIP phone’s translation set with the next translation-set save procedure. This value is then retained over a restart of CM.
- If no ip-network-mapping match is made, the next choice is a mapping of the Location name-value in the P-Location Header to the “Name” field for a network region. The Location name-value in the P-Location Header is configured using System Manager and used by Session Manger to fill the P-Location Header. CM attempts to match the P-Location name-value in the P-Location Header to the name field in one of the network regions. If a match is made then the network region is assigned to that SIP phone. The network region is also saved to the translation set for the SIP phone with the next translation-set save operation, and retained over a restart of CM.
- If the first two fail to find a match, then the “Far-end Network Region” field value is the next choice. The field value, that is the network region, is not saved to the translation set for the SIP phone. The value is only used during SIP phone call operations. If the field is blank, then selection falls to the next choice. The “Far-end Network Region” field is assigned using the “signaling-group” form.
- The final and default choice is the physical network interface network region. This is the network region assigned to the interface. This value too is only used for call actions and not associated and saved to the SIP phone’s translation set. The physical network interface is the facility supporting the SIP phone call.

The additional use of the network region relationship obtained by a possible match with an ip-network-mapping or a P-Location match is used in the case where, after a restart of CM and no SIP phone call has yet been made, and the call cannot complete under normal call handling, an alternate attempt is made by CM to complete the call. Two examples of alternate call handling is Inter-Gateway Alternate Routing (IGAR)—for media resource usage—and Dial Plan Transparency (DPT).

- Again, the relationship is made with each call, but is only refreshed to the translation set after each translation-set save procedure.

Once the relationship to a network region is made the selection of media is the same as for H.323 phones

- See Algorithm used to select media for H.323 stations above for SIP phone media selection

2.4.4 Algorithm used to select media on inbound IP/SIP trunks

While assignment of IP network regions for phones using ip-network-map and gateways via SAT administration is straightforward, assignment of NRs to IP and SIP trunks requires additional discussion.

Network region assignment of IP and SIP trunks is done on the signaling group form. Proper network region design is important if specific media assignment on inbound calls is required. A common requirement in Customer topologies is that SIP trunk calls coming in via Data Center 1 should use DC1 media resources and SIP trunk calls coming in via DC2 should use DC2 media resources. Resources could be required for SIP call flows that include: Music on Hold, conference, transcoding, and call recording.

Following is the algorithm used to select media on inbound IP and or SIP trunks:

- CM looks first at the far-end network region of the signaling group to see if there is any media in that NR. If not,
- CM looks at the network region associated with the near end node name, which in this case is PROCR to see if media exists in that NR. When not found,
- CM looks at the network regions directly connected to the far-end network region of the signaling group for media in associated NRs. If not,
- CM looks at network regions indirectly connected to the far-end network region of the signaling group for media in associated NRs

This algorithm is particularly important when using PROCR as the near end resource for SIP trunks. If PROCR is in NR 1, for example, all system wide SIP trunk call flows would use DC1's resources even if the call initially comes into DC2. Therefore, PROCR should not be in a NR that has media. PROCR is a system wide signaling resource and should not be used to base decisions upon regarding media.

2.5 Algorithm used to construct Inter-Gateway Connections (IGC)

In some cases it is desirable to force two NRs to communicate with each other via a third NR that has media. In this case the two NRs are not connected to each other but are connected to a common third NR. For example NR 1, NR 2 and NR 3 contain H.248 gateways. Because of the underlying WAN topology, the IP subnet associated with NR 1 cannot route to the IP subnet associated with NR 2; the CM TDM BUS must be used to communicate between the two subnets/NRs. In this case, NR 1 and NR 2 are directly connected each other, but are both directly connected to NR 3; NR 3 media and the associated TDM BUS is the common resource for NR 1 and NR 2

When constructing NR designs that include NRs not connected to each other for a variety of reasons, IGC connections may be necessary. CM has very specific rules regarding use of IGCs to support call flows. An IGC is a media connection between media in two PNs/H.248 GWs

A call between two ports in two regions can be connected by:

- One inter-region IGC
- One IGAR connection
- One IGAR connection plus one intra-region IGC
- One IGAR plus two intra-region IGC (one on each side of the IGAR connection)

In the example above if both NR 1 and NR 2 are GW locations they could not communicate with each other since two IGCs would be necessary: one from NR 1 to NR 3 and one from NR 2 to NR 3.

If either NR 1 or NR 3 is phone only or has an IP/SIP trunk, then the call flow would be supported since there would be only one IGC. For example if NR 1 was a phone only location that needed to communicate with a phone in NR 2 (with GW), the NR1 phone would use media in NR 1 to communicate via IGC to the IP Phone in NR2

3.0 Best Practice Network Region Resource Assignments

This guide addresses network region strategies to use when deploying Processor Ethernet (PROCR) as the main signaling interface. With PROCR as the signaling interface for IP and SIP stations, trunks and H.248 Gateways, instead of CLANs, a number of new strategies must be deployed in order to ensure resources are optimized.

The following diagram represents the network region standard configuration used by Avaya for a dual data center model. Further details on this topology are captured in the Appendix in the Avaya Network Region IP Guidelines table.

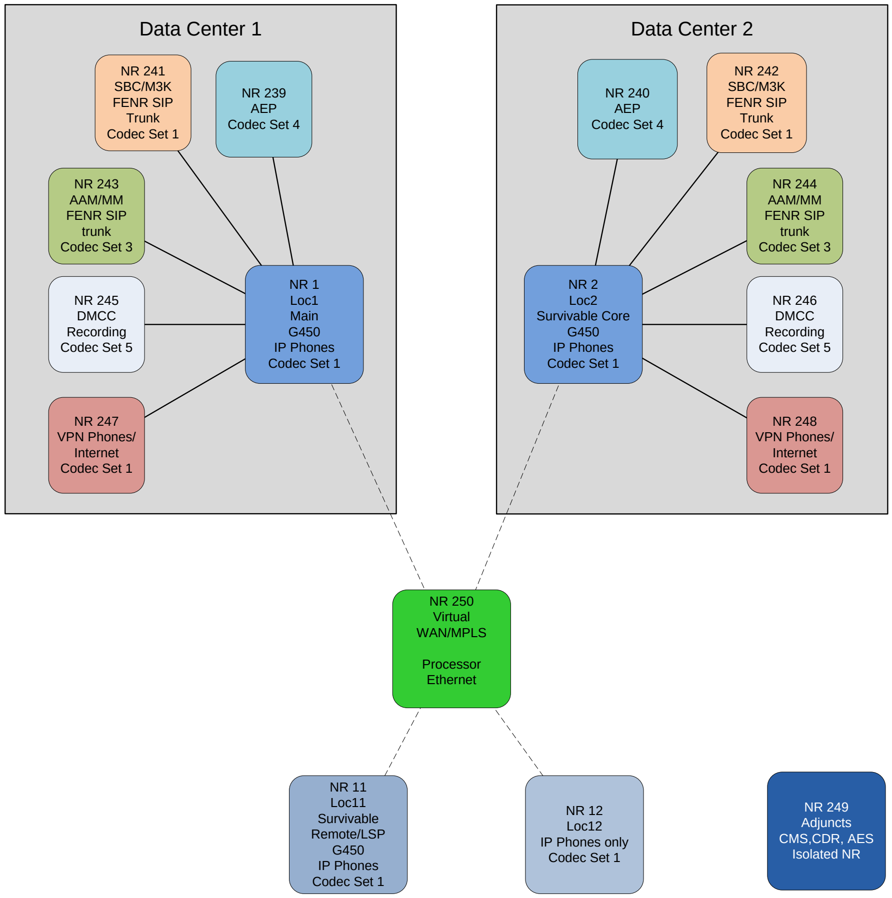


Figure 3 Network Region Standard Topology

The diagram above depicts a dual data center model with support for CM Main and Survivable Core (SCS) sites, with Session Managers at each of the data centers. Centralized SIP trunks are connected at each data center via Session Border Controllers. In addition there is a WAN in place, connecting the data centers to the remote branches. Some of these branches have phones, gateways and Survivable Remote Servers (SRS), other branches are phones only. There are adjuncts in the Main Data Center including Avaya Aura Messaging, Call Recording, and Avaya Experience Portal. There is also an Internet connection at both Data Centers using VPN tunnels to support remote IP Phones. If additional data center applications such as conferencing via AAC, MX or another application were present, additional NRs would be incorporated into the data center design, following the same depicted topology.

Note this topology mirrors the underlying LAN/WAN topology, with individual site components sharing the same LAN and site connectivity via the WAN.

While some solutions may not have dual data centers or have more or less than the data center applications depicted, the unused NR numbering at the data centers should remain reserved for potential future use. This ensures consistent NR configurations, which simplifies maintenance the thus potentially reduces total cost of ownership. Designs previous to this convention may have established different numbering schemes. However, the same topology should ideally be in place to ensure optimized operations in a fully vetted configuration.

The following sections provide additional information for assigning boards, cabinets, media gateways, IP Phones and trunks.

3.1 Processor Ethernet Network Region

In order to leverage the algorithm used to select media on inbound IP/SIP trunks, PROCR should be placed in a network region with no media. By so doing, the PROCR NR does not enter into the CM's decision for media.

In the Network Region Standard Topology diagram, PROCR is placed in NR 250. Placing PROCR in the same NR as the virtual WAN NR meets the requirement for having PROCR in an NR with no media. It also addresses a requirement to have PROCR in an NR that has direct or indirect connectivity to all NRs. This is needed to support H.323 phones that are using PROCR for socket establishment.

Following this recommendation enables a deterministic and optimal approach that can be applied in DSP resource selection. For inbound IP/SIP trunks, this is based on leveraging the far-end (FE) network region specified in the signaling group.

On inbound calls to the SIP trunk signaling group, CM first looks at the FE NR as a media candidate and in this case there is no media in NR 241. CM then looks at the near end PROCR NR 250 and again there is no media. So finally CM looks at the NRs directly connected to NR 241 and there is a direct connection to NR 1, which does have DSP resources. In this case calls coming into DC1 will use NR 1 resources for Music on Hold, Announcements, Call Recording, and transcoding where necessary. Similar logic applies to calls coming into DC2 using FE NR 242.

Per the standard diagram, the FE NR for signaling groups terminating at the data centers do not have media. However, SIP trunks that terminate at remote branches may reuse the FE NR of the branch, which would have media. Assume there are local SIP trunks connecting at the NR 11 branch with a local SBC at the branch. BSM could be equipped at the site to provide survivability in rainy day. The signaling group for these trunks would be assigned with a FE NR of 11.

For inbound SIP calls, the recommended method to ensure CM selects the desired signaling group is to leverage the FE domain assigned on the signaling group. See Algorithm used to select signaling group on inbound SIP trunks in the Appendix for details about this algorithm. CM attempts to match the P-Asserted-Identity domain in the From URI of the SIP messages for the inbound call, to a far end domain configured in the signal group. As the result of a match, CM selects a signaling group that identifies the DSP resources from the signaling group's FE. By prefixing the root domain with selected sub-domains, inbound traffic to CM can be steered to appropriate sets of signaling groups, enabling media resources to be appropriately engineered to accommodate the predicted traffic.

3.2 Survivable Processors

In order to use Processor Ethernet, the PE interface must be associated with a Network Region. This is performed via the survivable-processor form.

SURVIVABLE PROCESSOR			
Type: lsp	Cluster ID/MID: 38		Processor Ethernet Network Region: 38
V4 Node Name:	gw38lsp	Address:	135.9.146.162
V6 Node Name:		Address:	

It is recommended that the Procr address of the primary Survivable Core Server (SCS) occupy the same NR as the main CM Procr, which per the Network Region Standard Topology diagram would be NR 250. This ensures similar media resource behavior for the SCS should transition from the Main site occur.

Procr of other survivable sites will typically occupy the same NR as the gateways at that site. This ensures appropriate association of a site's gateways with the site's survivable CM. In most cases, endpoints should also use the NR used by the branch site's procr and gateway NR.

3.3 H.248 gateways

G430 and G450 Media Gateways are assigned to a location and network region on the media gateway form. (G250, G350 and G700 gateways are assigned in the same manner, but are no longer supported as of CM Release 7, though likely still functional.)

- "add/change media-gateway" form in SAT/ASA
- H.248 gateways should have the main CM Procr IP set as their Controller IP Address
- The internal mgc list configuration of the H.248 media gateway contains in order as comma separated values: the main CM Procr IP, primary SCS Procr IP and if present a remote CM Procr IP. For example:
  set mgc list 10.1.1.4,10.1.2.4,10.1.3.4
  Where 10.1.1.4 is the main CM Procr IP

	MEDIA GATEWAY 1	Generated?	y
Type:	g450		
Name:	G450-1		
Serial No:	150DR112833		
Link Encryption Type:	any-ptls/tls	Enable CF?	n
Network Region:	1	Location:	1
		Site Data:	Denver
Recovery Rule:	1		
Registered?	y		
FW Version/HW Vintage:	37 .39 .0 /1		
MGP IPV4 Address:	10.1.4.20		
MGP IPV6 Address:			
Controller IP Address:	10.1.1.4		
Mac Address:	a4:25:0d:02:0 6:8e		
Mutual Authentication?	n		

3.4 Non-H.248 gateways

Also known as port networks, G650s, are assigned to network regions only for purposes of access control calculations for IGAR. The boards within a port network can independently be assigned an NR of their own.

For G650 Port Networks:

- "change cabinet" form in SAT/ASA

	CABINET		Generated? y
CABINET DESCRIPTION			
Cabinet:	1		
Cabinet Layout:	G650-rack-mount-stack		
Cabinet Type:	expansion-portnetwork		
Location:	1	IP Network Region:	1
Rack:	Room:	Floor:	Building:

CARRIER DESCRIPTION		
Carrier	Carrier Type	Number
E	not-used	PN 01
D	not-used	PN 01
C	not-used	PN 01
B	G650-port	PN 01
A	G650-port	PN 01

3.5 IP boards

NRs for the port network boards are primarily used with MedPros. The NRs for these are assigned in CM's ip-interface form. VAL boards can also be assigned to a network region. But there is no advantage to this. So the NR for VAL is left blank and VALs default to use of NR 1.

- "add/change ip-interface" form in SAT/ASA

	IP INTERFACES		Generated? y
	Critical Reliable Bearer? n		
Type:	MEDPRO		
Slot:	01A14		
Code/Suffix:	TN2602		
Enable Interface?	y		
VLAN	n		
Network Region:	1		
VOIP Channels:	320		
	IPV4 PARAMETERS		
Node Name:	Medpro-01A14	IP Address:	10.1.55.24
Gateway Node Name:	10.1.55.1	IP Address:	10.1.55.1
Subnet Mask:	/24		

3.6 IP Trunks

Trunks are assigned to a network region on the signaling-group form. For SIP and H.323 IP trunks, use the “change signaling-group” form to identify the NR.

- Assign a “near-end” node name of PROCR. Since procr is placed in an NR without media resources, the near end will not be used in determination of media resource allocation.
- Populate the desired Far-end Network Region with the NR where media resources are expected to be obtained. Note per the Network Region Standard Topology diagram that resources do not exist in NR 243 and so are instead obtained from directly connected NR 1.

SIGNALING GROUP   Generated? y

Group Number: 301   Group Type: sip
IMS Enabled? n   Transport Method: tls
Q-SIP? n
IP Video? n   Enforce SIPS URI for SRTP? y
Peer Detection Enabled? n   Peer Server: SM
Prepend ‘+’ to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove ‘+’ from Incoming Called/Calling/ Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr   Far-end Node Name: sesm1-dc1
Near-end Listen Port: 5061   Far-end Listen Port: 5061
Far-end Network Region: 243

Far-end Domain: aam.customer.com
Bypass if IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate   RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload   Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3   IP Audio Hairpinning? n
Enable Layer 3 Test? y   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n   Alternate Route Timer(sec): 6

Trunks with SIP are a concept primarily associated with CM. The far end session manager has no constructs for trunks, and no knowledge of the network region. An appropriate domain-based routing design ensures that CM will associate inbound calls with the expected signaling and trunk groups. Outbound calls from CM select the trunk group and associated signaling group as specified by the route pattern.

3.7 Avaya Media Server

As of release 7.0, Avaya Media Server (AMS) can be used to provide media resources for a CM. AMS cannot be used with CMs running releases older than r7.0.

AMS has a direct SIP interface to CM and does not connect to SM. AMS can interface to multiple CMs. The AMS signaling group must have a FE NR assigned a value 1-250 and AMS cannot be assigned to a stub region. The signaling group’s NE node name of procr is read only.

For TLS the NE listen port defaults to 9061. This value can be changed. However, well-known TLS port 5061 must not be used for the NE port. By default, 5061 is used for the FE port.

The following represents an AMS signaling group assignment. As AMS is a direct connection to CM, the SM signaling group selection algorithm does not apply. Allocation of group numbers for AMS therefore by convention starts at 1.

```
display signaling-group 1                                              Page   1 of   2
                                  SIGNALING GROUP

 Group Number:    1                        Group Type:  sip
                                     Transport Method:  tls


  Peer Detection Enabled?   n              Peer Server:  AMS



    Near-end Node Name:   procr                           Far-end Node Name:   ams1
     Near-end Listen Port:   9061                         Far-end Listen Port:   5061
                                                    Far-end Network Region:     1

        Far-end Domain:   10.1.1.20
```

AMS may be virtual, AVP or bare metal based. Virtual and AVP have the same Message Processing Units (MPUs) sizes. The small version is 550 MPUs, the medium version is 1400 MPUs and the large version is 2800 MPUs. An MPU is the processing required to support 1 G.711 DSP. Other Codecs require additional MPUs and therefore limit the number of DSPs a particular version of AMS can support. The highest capacity AMS is the large bare metal server, which can support up to 4,800 MPUs and a maximum of 4,000 DSPs.

When assigning AMS to an NR, the capacity of the server needs to be taken into account for dimensioning UDP ports. By default the AMS uses port 6,000 as its' lowest starting port number and 32,599 is the maximum end port assignable. It is possible to modify port 6,000 to match the CM default port of 2048 used for other NRs. When determining the AMS UDP port range, 10% additional ports should be allocated to allow for ports freeing up after call termination. Therefore the largest bare metal server with 4,000 DSPs, requiring 2 ports for each call and keeping 6,000 as the starting port would result in a UDP port range of 6,000-15,000. AMS port ranges are not required to be contiguous

3.8 IP phones

Port networks are assigned to a location on the cabinet form. Media gateways are assigned to a location on the media gateway form. A traditional station (i.e. DCP) attached to a port network inherits the location of the port network. A traditional station attached to a media gateway inherits the location of the media gateway.

The most significant use of the location concept is for E911 calls. Port networks or gateways in different locations might have a different public safety answer point or PSAP. The system must be configured to ensure that emergency calls made from telephones are routed to the correct PSAP. Each port network or gateway that is in a different PSAP jurisdiction than the main server must be administered in a separate location. This separate administration ensures that the system can route emergency calls from that location. If a station in location 5 dials 911, it must be routed out a trunk in location 5 so that local public safety services, and not public safety services in a different city, respond to the emergency. A trunk in location 5 is attached to a port network or media gateway in location 5. There are other applications of the location concept, but in general it is used to route calls to the proper PSTN trunks.

Most IP enabled systems need the ip-network.map populated. The primary reason for the ip-network.map form is to associate an IP address range with an IP-Network Region. As an IP station is not attached to a port network or a media gateway, it is assigned via the ip-network-region form to a location based on its network region.

IP ADDRESS MAPPING — Generated? y

CM5.2+ FROM IP Address	CM5.2+ TO IP Address	Subnet Mask	Region	VLAN	Emergency Location Extension
135.9.14.0	135.9.14.255		101	n	
135.9.30.0	135.9.30.90		101	n	
135.9.33.187	135.9.33.187		33	n	
135.9.42.1	135.9.42.1		33	n	
135.9.44.0	135.9.44.255	24	101	n	
135.9.48.0	135.9.48.255	24	101	n	
135.64.4.0	135.64.4.255	24	39	n	
135.64.34.0	135.64.35.255	23	36	n	
135.64.44.0	135.64.44.255	23	7	n	
135.64.80.1	135.64.81.127		33	n	
135.64.150.92	135.64.150.127		5	n	
135.64.155.47	135.64.155.47	32	101	n	
135.64.155.89	135.64.155.89	32	1	n	
135.64.155.129	135.64.155.129	32	1	n	

In the absence of an ip-network-region form entry, an IP phone will implicitly inherit the network region of the gatekeeper to which the phone has registered.

Best practice is to ensure the location on the cabinet or media-gateway form matches what is on the ip-network-region form.

The example below would be used to associate IP phones in the 10.56.132.0/24 subnet to ip-network region 2

IP-Network-Map

From IP Address	To IP Address	Subnet Mask	Region	Vlan	Emergency Location Extension
10.56.132.0	10.56.132.255	24	**2**	**n**	

For additional information and assistance with subnetting, calculators can be found on the internet to determine masks and the subnet an IP value fits into.

Some of the common masks utilized are as follows:

28 = 255.255.255.240 (has 16 ip address's per subnet- 14 usable)

27 = 255.255.255.224 (has 32 ip address's per subnet- 30 usable)
26 = 255.255.255.192 (has 64 ip address's per subnet- 62 usable)
25 = 255.255.255.128 (has 128 ip address's per subnet- 126 usable)
24 = 255.255.255.0 (has 256 ip address's per subnet- 254 usable)

The 2 addresses deemed unusable as hosts in each subnet are the first and the last IPs in each subnet, the network and broadcast addresses respectively.

While a subnet mask in decimal may not be obvious, it is when represented in hex or binary as bit masks for an AND operation. An IP address is made up of 4 octets, separated by the dot, or a total of 8 hex digits. The leftmost non-255 value and rightmost non-0 octet for a subnet mask can assume a value of either:

(decimal = hex = binary).
255 = FF = 11111111
254 = FE = 11111110
252 = FC = 11111100
248 = F8 = 11111000
240 = F0 = 11110000
224 = E0 = 1110000
192 = C0 = 11100000
128 = 80= 10000000
0 = 00 = 00000000

The more 0s and the smaller the subnet mask value, the more IP addresses are represented by the mask.

3.9 Avaya Aura Messaging Transcoding considerations:

Prior to the r6.3 release and introduction of G.729 transcoding in AAM, only the G.711 codec was supported. In many cases this prohibited shuffling of calls on and off the TDM bus. So, dedicated signaling groups in CM were required for AAM to specify a far end NR for AAM. Use of dedicated signaling groups is still followed with NRs 243 and 244 standardized for this purpose.

On the signal group, "Direct IP-IP Early Media?" should be set to "n" on the NR form unless the G.711 codec is used universally. It is also recommended to set the Direct IP-IP Audio to "n" on the AAM Signal group to avoid clipping around 6 sec into a recorded message as a result of shuffling.

For calls inbound to CM from AAM, domain based routing is the Avaya Best Practice methodology for ensuring the appropriate signaling group is selected. For outbound calls to AAM, desired signaling group selection is accomplished through routing to the appropriate CM signaling group.

While technically feasible to use port based routing as an alternative methodology, in general this practice should be avoided. Port based routing requires multiple SIP entities in Session Manager as well as multiple routing policies. In addition there is a 16 port limit for TLS links in CM. As each unique port/IP combination equates to a unique TLS link, while multiple signaling channels using the same port/IP with different domains does not, use of port based routing can quickly exhaust CM configuration capability.

3.10 Traditional telephony resources

As analog and TDM resources do not use an IP codec, these are not assigned to network regions. These include:

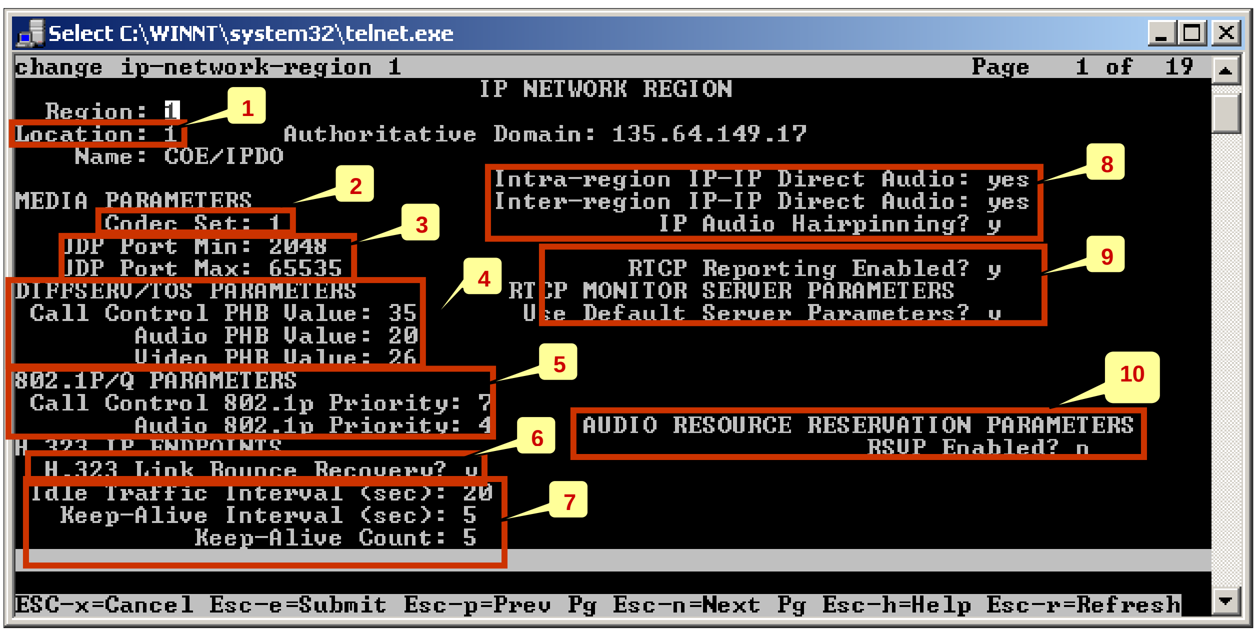
a. Analog and DCP stations
b. Analog and digital trunks
c. Any non-IP resource in general

3.11 Use of CM as a Firewall

CM TDM bus can be used to accommodate calls between NRs that are not connected to each other. This is accomplished by ensuring the two NRs are connected to a common NR with media. Most CM Firewall applications rely on PNs with media resources from two different NRs in the same PN. These configurations are beyond the scope of this document.

4.0 IP-Network-Region Form Basics

The network region points to a location ID. The location ID points to parameters. The parameters define local settings as described in these screens. The location ID must be unique if: local settings are different (time zone offsets, loss plan parameters, etc.), local call routing is required to utilize local trunks (ARS by location), for 911 reporting to local PSAP, or because local trunks are being used.



1. Location: Verify if endpoints for this NR need local settings, local trunks, or E911. Default 1. Settings administered separately.
2. Codec set: This is for intra-region. Default is 1. Codec settings administered in the ip-codec form.
3. UDP port min/max: Layer 4 port prioritization for RTP voice ports. Range of UDP ports shared by NR members for a device with one IP address. The minimum ports required

for a MedPro TN2302 is 256, CrossFire TN2602 and a 320 DSP port G450 = 1280. Each voice call uses 2 ports, 1 for RTP and another for RTCP. The typical UDP port range needed for gateway sites is 2048-3329. As each gateway is another IP address, the 2048-3329 range still applies for sites with multiple gateways. For AMS depending on the server type, a greater range up to 2048-11048 or 6,000-15,000 may be required. See the previous Avaya Media Server section for more information.

4. Diffserv/TOS: Layer 3 COS. Defaults 34, 46 and 26, for control, audio and video. Applies to all circuit packs, gateways, and IP phones assigned to the NR. Values should be adjusted to comply with Customer data network requirements.
5. 802.1 p/Q: Layer 2 COS. Defaults are 7 for control, 6 for audio and 5 for video. Applies to all respective circuit packs that tag from Communication Manager only: all gateways, and any IP phones assigned a VLAN ID. Values should be adjusted to comply with Customer data network requirements.
6. H.323 link bounce recovery: If set to y enables sending of TCP Keep Alives to CM per the values described next. . Default is yes.
7. Idle traffic & KA interval/count: Fine tunes TCP Keep Alive from IP phone to gatekeeper. Leave defaults (20, 5, 5).
8. IP-IP and hair-pinning: Define shuffling and hair-pinning functionality. Both enabled by default.
9. RTCP reporting/monitor server (VMON/VMM): Enabled by default. Specify default server, or NR specific server. Default server administered separately.
10. RSVP: DON'T USE IT. Typically not supported on customer networks. Defaults to "no."

4.1 IP Phones – Specifics involving Registration & Network Regions

Since this guide focuses on Processor Ethernet, the discussion of AGLs will be focused primarily on PROCR. For a detailed description of AGL generation and use with Time to Service (TTS) and non-TTS phones see the "IP Network Region Design with the Enhanced Alternate Gatekeeper List" document cited in the references at the end of this document.

Enhanced Alternate Gatekeeper List use with PROCR

The enhanced alternate gatekeeper list (E-AGL) was designed for C-LAN implementations to manage registration and socket establishment for IP Phones. In the examples in this document there are no C-LANS. It is recommended to use the E-AGL algorithm even for PROCR only implementations to explicitly administer use of PROCR. All Phone NRs should be directly or indirectly connected to the PROCR NR in a properly designed NR configuration. E-AGL administration would be based on placing the quantity 1 for NR 250 for all NRs that contain IP Phones. Actually, phones will register successfully even if the PROCR NR is not connected to IP Phones. But this requires that every phone's subnet is administered to an appropriate NR in ip-network-map; otherwise registrations will fail.

TTS Registration Method

The TTS feature implements a pseudo-permanent signaling connection. It applies the benefits of both permanent and on-demand signaling.

- Phone registers with gatekeeper and is considered in service upon registration.

- Following registration, Communication Manager establishes the signaling connection as quickly as possible in a metered fashion, based on available processor resources.
- A demand stimulus, such as an incoming call or the initiation of an outgoing call, results in the signaling connection being established immediately for the affected phone(s), pre-empting the metered process described above.
- Once established, the signaling connection remains up, with keepalive exchanges taking place to maintain the connection during idle times.
- If signaling is lost for a specified duration, as detected most likely by failed keepalive exchanges, the phone is not required to re-register. Instead, the signaling connection is simply re-established when the outage recovers.

The RAS keep-alive implementation with TTS allows the signaling connection to be disrupted and still maintain the registration state of the IP phone. This is key to faster mass recovery after an outage. If the phone is considered to be registered, even during an extended outage, there is no need to re-register after outage recovery. There is only a need to re-establish the signaling connection.

<table>
<tr><th colspan="2">Normal registration pre-TTS</th></tr>
<tr><th>IP Telephone</th><th>Communication Manager</th></tr>
<tr><td colspan="2">RAS Gatekeeper Request (GRQ)(UDP)
→</td></tr>
<tr><td colspan="2">RAS Gatekeeper Confirm (GCF)(UDP)
←</td></tr>
<tr><td colspan="2">RAS Registration Request (RRQ)(UDP)
→</td></tr>
<tr><td colspan="2">RAS Registration Confirm (RCF)(UDP)
←</td></tr>
<tr><td colspan="2">Phone is registered, but <u>not</u> in service.</td></tr>
<tr><td colspan="2">Phone immediately opens H.225 call signaling socket.

TCP SYN
→
TCP SYN ACK
←
TCP ACK
→</td></tr>
<tr><td colspan="2">H.225 Setup (TCP)
→</td></tr>
<tr><td colspan="2">H.225 Call Proceeding (TCP)
←</td></tr>
<tr><td colspan="2">H.225 Connect (TCP)
←</td></tr>
<tr><td colspan="2">Phone is registered and in service, which implies there is a signaling connection.</td></tr>
</table>

<table>
<tr><th colspan="2">Normal registration TTS</th></tr>
<tr><th>IP Telephone</th><th>Communication Manager</th></tr>
<tr><td colspan="2">RAS Gatekeeper Request (GRQ)(UDP)
→</td></tr>
<tr><td colspan="2">RAS Gatekeeper Confirm (GCF)(UDP)
←</td></tr>
<tr><td colspan="2">RAS Registration Request (RRQ)(UDP)
→</td></tr>
<tr><td colspan="2">RAS Registration Confirm (RCF)(UDP)
←</td></tr>
<tr><td colspan="2">Phone is registered and in service, without a signaling connection.</td></tr>
<tr><td colspan="2">Communication Manager opens H.225 call signaling socket. Could be immediate or delayed, based on call processing load.
TCP SYN
←
TCP SYN ACK
→
TCP ACK
←</td></tr>
<tr><td colspan="2">H.225 Setup (TCP)
→</td></tr>
<tr><td colspan="2">H.225 Call Proceeding (TCP)
←</td></tr>
<tr><td colspan="2">H.225 Connect (TCP)
←</td></tr>
<tr><td colspan="2">Phone is registered and in service, with a signaling connection.</td></tr>
</table>

Appendix A

A1 Avaya Network Region IP Standards

All IP enabled systems need the ip-network-region forms populated. The primary reason for the ip-network-region form is for media administration (Codec selection, location selection, QoS settings, control connections to other Network-Regions, CAC, IGAR, etc)

Avaya's recommended guidelines for network region numbering, which are also reflected in the Network Region Standard Topology diagram, are presented in the following table.

IP Network Region Numbering Guidelines

IP-Network Regions	Usage	Comments
01-199	MG/PN Locations	For media gateways, IP stations, branch processor Ethernet, CLANs, medpros, VALs, PN cabinets (NR 1 is the default and typically used by the main data center)
239-240	AEP	Used for Experience Portal or alternative IVR system where resources are split across DC1 and DC2
241-242	PSTN SIP Trunking	Used for PSTN facing SIP interfaces, which may be an SBC or SIP gateway. As DSP resources are provided from the inter-connected data center, each SBC connects via the DC NR before interfacing to the network
243-244	Voice Mail	Used for the voice mail system, which may be MM, AAM or another system. AAM server configuration usually involves a server(s) at each data center. To reduce WAN traffic, these NRs are homed to the DC NR where the media application server is located.
245-246	Call Recording	Used for recording of voice calls. As call recording is frequently located at a centralized location, the call recording NRs are interconnected via the NR controlling the NR resources where the call recording device resides.
247-248	VPN Phones	Used for work at home employees. VPN configuration usually involves a VPN server at each data center. To reduce WAN traffic, the VPN is homed to the DC NR where the VPN server resides
249	Adjuncts and IP Trunk dedicated CLANs	IP Connected Adjuncts such as CMS, Intuity, CAS, SAT, dedicated IP Trunk CLANs etc... NOT connected to any other Network Regions (All dedicated adjunct and IP trunks clans would share this NR)
250	Virtual Region/PROCR	Virtual network routing region with no media resources. Also the recommended NR for placing the Main and SCS PROCR. Provides a means to control

IP-Network Regions	Usage	Comments
		number of calls or bandwidth limits between network regions with limited WAN bandwidth (Call Admission Control). Can include a pool of directly connected CLANs if needed for IP phone registration. Is used to represent the WAN cloud for the underlying data network.

All IP enabled systems need the ip-codec set form populated. The primary reason for the ip-codec form is for audio Codec selection and settings, media encryption selection and Fax and Modem mode and settings. Note: using AES encryption requires 25% more TN2302 Medpro resources.

The following table identifies the bandwidth requirements of commonly used codecs.

Codec Information				Bandwitch			
Codec & Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Nominal Ethernet Bandwidth (Kbps)
G.722-64K	80 Bytes	10 ms	4.13	160 Bytes	20 ms	50	87.2 Kbps
G.711	160 Bytes	20 ms	4.1	160 Bytes	20 ms	50	87.2 Kbps
G.729	10 Bytes	10 ms	3.92	20 Bytes	20 ms	50	31.2 Kbps
G.723-6.3K	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	21.9 Kbps
G.723-5.3K	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	20.8 Kbps
G.726A-32K	20 Bytes	5 ms	3.85	80 Bytes	20 ms	50	55.2 Kbps

The following table contains an example of possible Codec settings and usage. Up to 7 Codec sets are supported. Each set may have to 6 codec selections, with the first selection weighed first for use.

IP Codec Sets

	Codec Set 1	Codec Set 2	Codec Set 6	Codec Set 7
Name/Usage	intra-site	inter-site	Voice Mail	Recording
Codec Selection 1	G.711mu	G.729	G.711mu	G.729
Frames Per Packet	2	2	2	2
Silence Suppression	no	no	no	no
Codec Selection 2	G.729	G.711mu		G.711mu
Frames Per Packet	2	2		2
Silence Suppression	no	no		no
Media Encryption 1	10-srtp-aescm256-hmac80	10-srtp-aescm256-hmac80	none	10-srtp-aescm256-hmac80
Media Encryption 2	aes	aes		1-srtp-aescm128-hmac80
Media Encryption 3	none	none		none
Allow Direct-IP	no	no	no	no

	Codec Set 1	Codec Set 2	Codec Set 6	Codec Set 7
Multimedia				
Maximum Call Rate				
Maximum Call Rate for PRI				
FAX Mode	relay	relay	t.38 standard	relay
FAX Redundancy	0	0	0	0
Modem Mode	off	off	pass-through	off
Modem Redundancy	0	0	0	0
TDD/TTY Mode	US	US	US	US
TDD/ TTY Redundancy	3	3	3	3
Clear-channel	no	no	no	no
Clear Channel Redundancy	0	0	0	0

For the CM, a standardized naming convention should be used for node names. CM has a limit of 15 characters maximum for node names. So the convention must adhere to this limitation. Lower case is preferred.

Following is one possible convention. Many Customers already have their own convention to adhere to or more appropriate alternatives can be created.

For global accounts, it is useful to have the first 1 or 2 characters represent the country as in the following table.

Global Code Name (Length 2)	
Region/Country	**Code Name**
United States	us
Latin America	la
Canada	ca
Europe	eu
Asia Pacific	ap

If the solution exists in a single nation, the above can be omitted. The next field could be used to identify the site and could incorporate the country if necessary. Keeping this to 4 characters is a safe practice

Site Code Name (Length 3) (Example)	
Site/Building Name	**Code Name**
Brea, CA	bre
Denver, CO	den
Camas, WA	cam
Chelmsford, MA	che
Melville, NY	mel
Toronto, Canada	tor

One the site has been identified, the type of physical equipment or application should be reflected, pre the following example

Device Code Name (Length 3-6)	
Device	**Code Name**

Device Code Name (Length 3-6)	
Main CM Procr	procr
Main CM Duplex-A	cm-a
Main CM Duplex-B	cm-b
Survivable Core Server	scs
S8300 SRS (embeded server)	srs
AES	aes
CMS	cms
System Manager	smgr
Session Manager	sesm
G430	mg43
G450	mg45
G650 Port Network	pn
Port Network IPSI	ipsi
Port Network CLAN	clan
Avaya Aura Conferencing	aac
Avaya Aura Messaging Storage Server	mss
Avaya Aura Messaging Application Server	mas

Finally the device numeric identifier should be appended at the end using 1-3 characters depending upon the device type. If the 15 character limit has not reached, hyphens can be added as desired to make the name more legible by separating the fields. Following are possible results of applying this convention.

Server/MG Hostname Results Examples				
Resulting Hostname	**Global Code Name**	**Site Code Name**	**Device Name**	**Identifier**
usdenprocr-1	us	den	procr	a
usdevcm-b	us	dev	cm	-b
usdevsesm-1	us	dev	sesm	-1
usdevsmgr-1	us	dev	smgr	-1
usrtpmg450-20	us	rtp	450	-20
catorms450-01	ca	tor	450	-01
catorclan01a01	ca	tor	clan	01a01

A3 Algorithm Used to Select a Signaling group on Inbound SIP Trunks

With SIP trunks it is possible to administer multiple signaling groups with the same socket. In this case PROCR is the near end node name/IP address and a Session Manager, as assigned in the CM's node names table, would be the far end node name/IP address. With all of these signaling groups, using the same near end listen port number, usually either well known port number 5061 for TLS transport or 5060 for TCP transport, only one socket is required.

Note, while possible to use other port numbers, this is not the recommended design approach, other than for special exceptions.

The advantage of using these well-known ports is that, from session manager's perspective, the trunk groups become a single SIP entity. This is highly desirable as it reduces the required administration between CM and SM. The benefits are:

- Domain based-routing reduces routing complexity in SM versus port-based routing, which even with a single CM requires multiple SIP Entities and routing policies.
- TLS sockets are more efficiently used in CM. Port-based designs can easily reach the limitation of 16 sockets when TLS is required. Even when starting with a TCP design, the potential adding of encryption into a port-based design could introduce the necessity of redesigning the SIP core and all SIP trunk and signaling groups.

In order to achieve consistent designs that are scalable and extensible, domain based signaling group designs are therefore recommended as an Avaya Best Practice.

Inbound Selection Algorithm

There are two separate algorithms used for inbound CM signaling group selection when there are multiple signaling groups with the same far end domain name and near end listen port. These algorithms are based on the “Peer Server” field on the signaling group form.

If the Peer Server field is set to “Others” the following algorithm is used to select a signaling group for an inbound call:

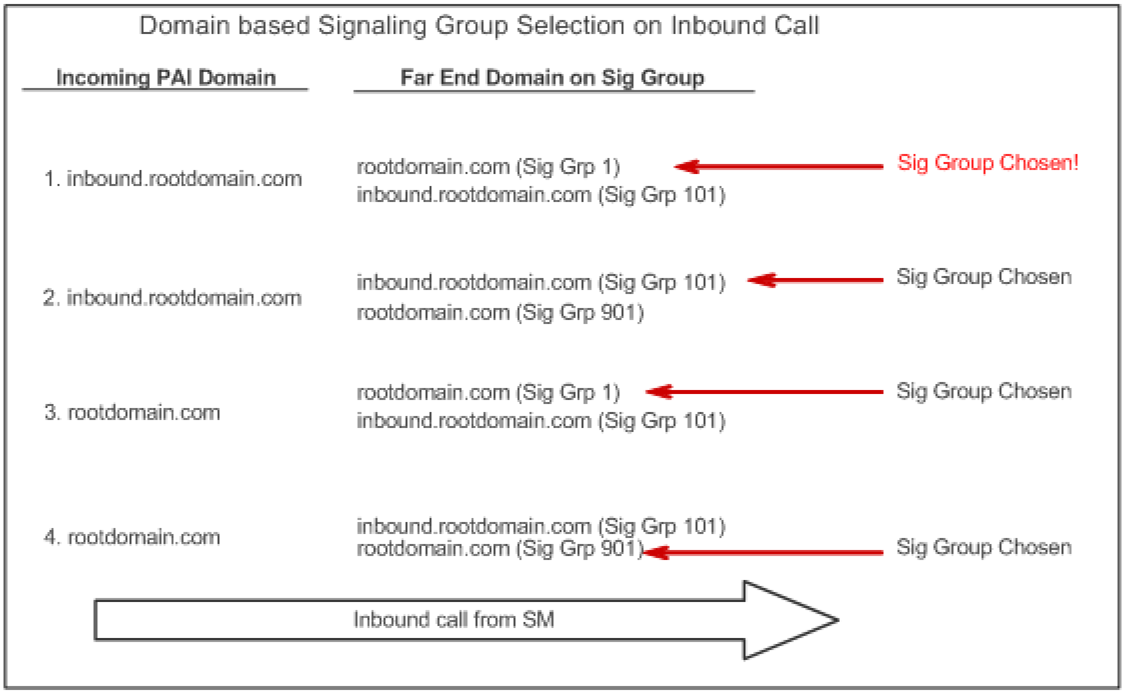
- Start with lowest numbered signaling group
- Select signaling group that matches the far end IP address and the near end listen port
- If multiple signaling groups match this criteria, select the lowest number signaling group where there is an exact match between the domain contained in the PAI header with the ‘Far-end Domain’ on the signaling group form.
- If no exact match, select the lowest number signaling group with a blank domain
- If still no match, reject the call

On the signaling group form, if the “Peer Detection Enabled” field is set to “y” the “Peer Server” field should display “SM”. If “SM” is displayed the following algorithm is used to select the signaling group on an inbound call:

- Start with lowest numbered signaling group
- Select the signaling group that matches the far end IP address and near end listen port
- If multiple signaling groups match this criteria, select the lowest number signaling group based on first match of
    - Domain contained in the PAI header
    - ‘Far-end Domain’ on the signaling group form (does not need to be the best or exact match)
- If no match, select the lowest number signaling group with a blank domain
- If still no match, reject the call

Following is an example of how domain based inbound signaling group selection works when the Peer Server field contains SM, with all possible combinations of signaling groups to potential domain matches. The example assumes the same session manager in the far end node name and the same near end listen port of 5061.

Selection starts with the lowest numbered signaling group and CM looks for the first match, not necessarily the best match, between the incoming PAI Domain and the Far End Domain on the signaling group form.



Note that in the first call flow there is a better match on signaling group 101. However, CM picks signaling group 1 as the top level domain of rootdomain.com in the PAI matches signaling group 1, even though there is not an exact match with the sub-domain. The second and third call flows are obvious matches. In the fourth call flow the incoming PAI of rootdomain.com does not match signaling group 101 and does match on 901. In other words, an exact match of the signaling group FE domain is attempted to either the PAI's top level or any of its' sub-domain levels.

In order to take advantage of this algorithm for proper signaling group selection:

- The lowest number signaling groups should contain the most specific sub-domain names
  - sbc1.inbound.rootdomain.com is more specific than
  - inbound.rootdomain.com, which is more specific than
  - rootdomain.com
- Signaling groups for Off-PBX Integration and Mobility (OPTIM) trunks should use the root domain and occupy the highest numbered signaling groups. OPTIM trunks are non-measured trunks used by SIP endpoints registered to the SM(s) and on-net calls to other CMs in the Enterprise.
- The authoritative domain for all network regions should be configured with the root domain

A4 Use of Authoritative Domains and Far End Domains in CM

Domains can be used in CM to authenticate inbound calls and to populate PAI on outbound calls:

- On outbound call flows, the authoritative domain specified in the NR associated with PROCR is used to populate the From and PAI headers. The domain specified as the far end domain on the signaling group is used to populate the domain of the R-URI header. If the domain is blank then the From and PAI headers will show “invalid.unknown.domain”.
- On inbound call flows, the authoritative domain specified in the NR associated with PROCR is used to authenticate the call against the domain in the R-URI header. Signaling group selection, if multiple signaling groups have the same socket, is based on the domain contained in the inbound PAI, matching to the far end domain in the signaling group. For inbound SIP Phone calls to CM, the authoritative domain of the NR of the SIP phone determines what is used.

To recap:

OUTBOUND CALL
CM------>authoritative domain of PROCR is used for the From and PAI headers. If no domain is included in the authoritative domain then invalid.unknown.domain is used to populate From and PAI headers.

CM------>far end domain of the signaling group used for the To and R-URI headers

INBOUND CALL
------>authoritative domain of PROCR used for authentication of the call ------>CM

If instead of a domain in the R-URI it contains the IP address of PROCR that is considered authoritative as well, even if there is no authoritative domain associated with PROCR in the associated ip-network-region

------>if the PROCR IP address is contained in the R-URI it can be used for authentication of the call ------>CM

------> the far end domain of the signaling group is used for determining signaling group selection based on a match with the inbound PAI domain ------>CM

Note: using an IP address instead of a domain is not recommended.

Where an Authoritative Domain is specified, it should be the top level (root) domain for the Enterprise, e.g., avaya.com

- On inbound calls, the R-URI is matched against the NR authoritative domain of the “Near-end Node Name” from the signaling group.
- With PROCR there is only one authoritative domain for SIP trunks
- The authoritative domain for SIP phones is associated with the NR of the phone

Incoming R-URI Domain	NR Auth. Domain associated with Near-end Node Name	Result
br101.avaya.com	br101.avaya.com	Match - PASS
avaya.com	br101.avaya.com	No match - FAIL
br101.avaya.com	avaya.com	Match - PASS

A5 Signaling and Trunk Group CM Numbering Convention

As previously mentioned with domain based routing, the signaling groups with the most specific Far-end Domain names should be assigned to the lowest numbered groups and OPTIM trunks should have the highest numbered groups. As CM selects the inbound signaling group with the lowest numbered group, it may be useful for the route pattern to select within a set of trunks, the highest numbered group where two-way trunks are used. This allows for outbound trunk usage to operate in inverse of inbound and has the benefit during troubleshooting of dividing the traffic directionally across the groups. As a consequence group numbering would start at the top of the range and grow downward. Taken a step further, SIP trunk groups can be segregated into incoming and outgoing instead of two-way at a cost of needing a somewhat larger quantity of trunks to compensate for Erlang efficiencies.

Trunk and signal group numbering depends upon Customer considerations for the mix and quantities of SIP, H.323 and TDM trunks. For different solutions, adjustments will likely be required to expand or contract number ranges for the particular circumstances for a Customer's environment. The following table provides a starting point and general convention for group numbering.

Trunk/Signaling Group Range	Purpose	Comment
1-199	AMS signaling groups and TDM trunks	
200-299	Optional for use of inbound when used instead of 2-way	
300-499	SIP adjunct entities: AAM, AEP, AAC, etc….	Sub-domain used which incorporates an adjunct identifier
600-699	PSTN trunks via an SBC or SIP gateway, two-way or optionally outbound only.	Sub-domain used which incorporates an SBC or gateway identifier. Expand if necessary to 700-799
800-899 or 900-999	OPTIM trunks using root domain in the signaling group FE. Includes SIP endpoint traffic and/or on-net trunks to other CMs.	If desired, endpoint and on-net can optionally be carried over separate groups with port-based routing used to enforce selection.

A6 References

1. CM 6.x Network Region Design, Compas ID: 159877, January 2016
2. Avaya Communication Manager Network Region Configuration Guide, Compas ID: 103244, October 2005
3. Implementing End-to-End SIP Vol 2: SIP Telephone Signaling and Dial Plan Options, Compas ID: 157210, September, 2014

4. "IP Network Region Design with Enhanced AGL Administration", Compas ID 147566, Mar 2011