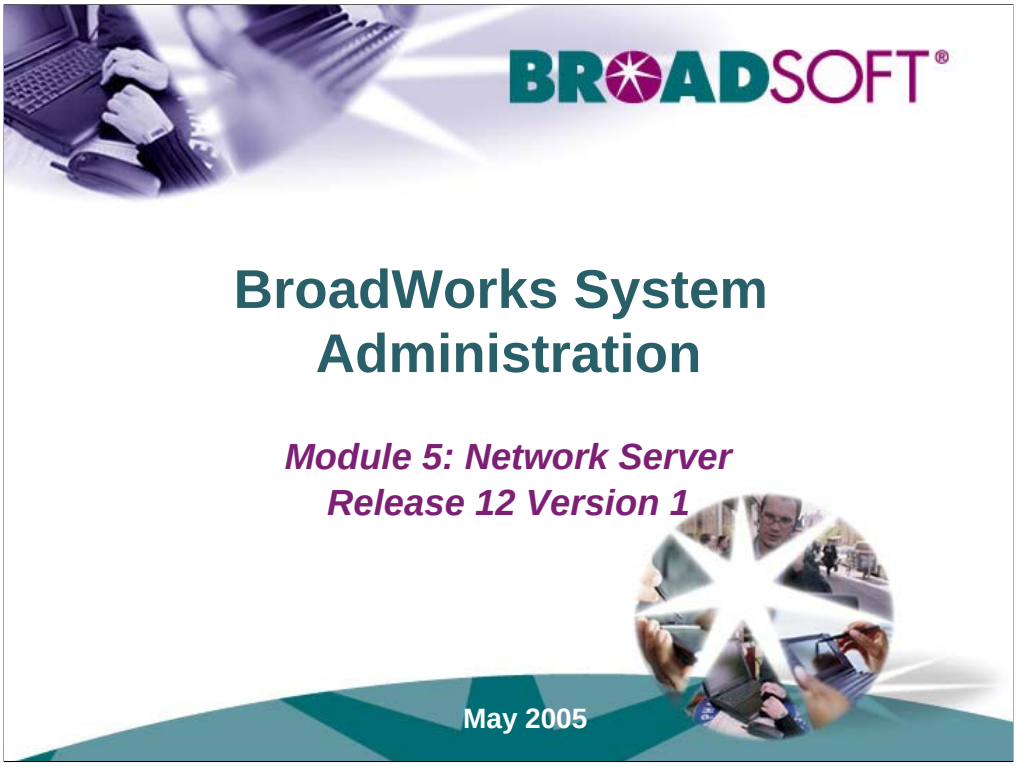

BROADSOFT®
BroadWorks System Administration
Module 5: Network Server
Release 12 Version 1
May 2005

Module 5: Agenda

BroadWorks Network Server
- Brief review of Network Server

Redundancy
- Overview and implementation

SIP/MGCP Overview
- SIP redirect message

Enterprise and Private Policies
- Concept of an enterprise
- Private policies and policy instances

Public Policies and Instances
- Translation policies
- Routing policies

Network Elements
- Hosting and resource network elements

Advanced Feature
- Configurable policy precedence

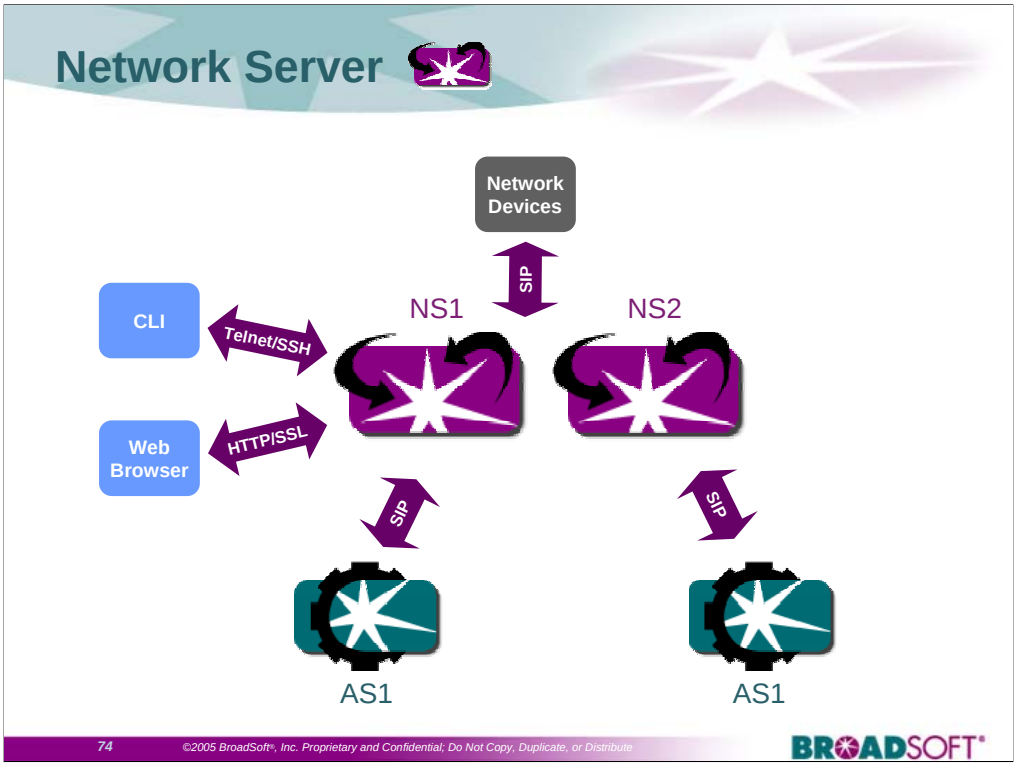
Module Objectives

At the end of this module, you will be able to:

- Explain the Network Server SIP Redirection function
- Explain the Network Server Media Server Selection function
- Understand Policies, Policy Instances and Profiles
- Understand the difference between Public and Private policies
- Understand Network Server call processing flow
- Explain the function of Public and Private policies

Network Server Reference Documents

- *BroadWorks Network Server Product Description*
- *BroadWorks NNACL Translation File User Guide*
- *BroadWorks Dialing Plans Guide*
- *BroadWorks DNs, CCs, and NDCs Guide*
- *BroadWorks E.164 Overview Guide*
- *BroadWorks Special Call Types Routing Guide*



Centralized Routing

E.164 and URL supported transaction-based system.

Enterprise voice VPN services.

Policy-based routing.

Acts as SIP redirect server: 302 Moved Temporarily.

Translations and routing.

Management

Multi-location enterprise portal.

Self-service and private dial plan management.

Location Register

“SyncAPI” maps user or group addresses to owning Application Server.

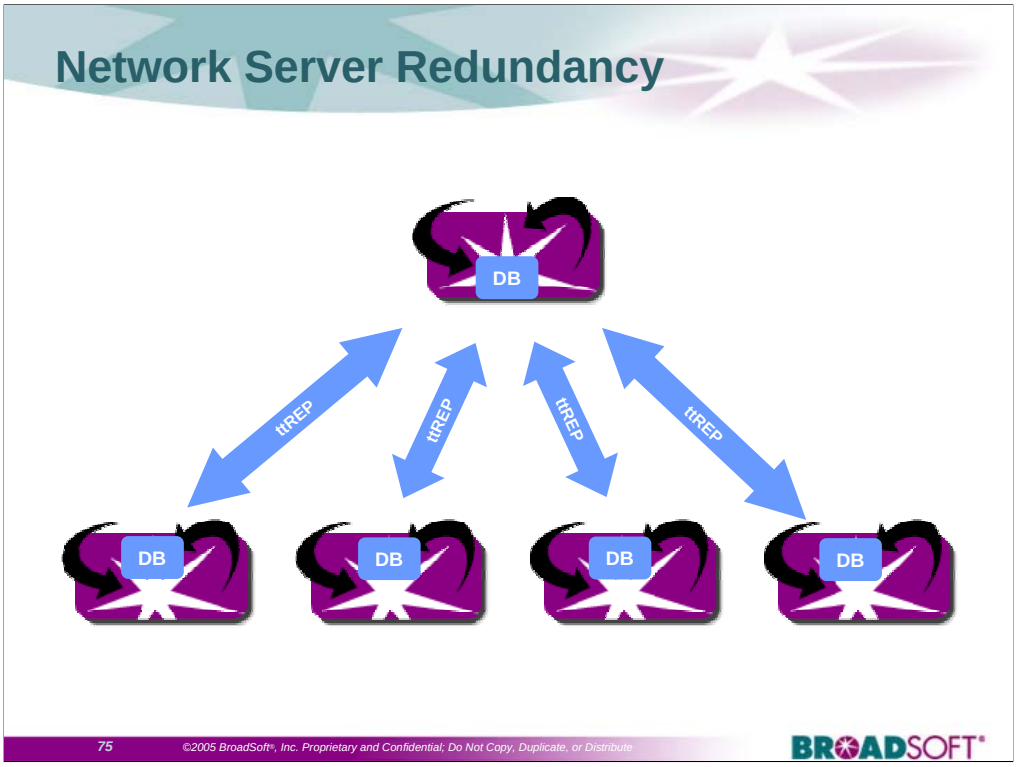
Media Server Selection

Locates closest Media Server to the end user or network gateway.

Uses proprietary MSS protocol to send list of Media Servers to the Application Server.

SIMPLE Support

Supports Windows Messenger communications.



Network Server Clustered Architecture

Network Servers are deployed in a cluster model, whereby servers providing duplicate functionality are deployed together. The cluster model has been designed to meet capacity, scalability, and redundancy requirements.

Redundancy

Network Servers are deployed in an N+1 configuration for redundancy.

Network Server provides IP interface redundancy.

Scalability

Network Servers are independent of one another.

Each Network Server has its own image of the data and can be used to add new data.

Data Replication

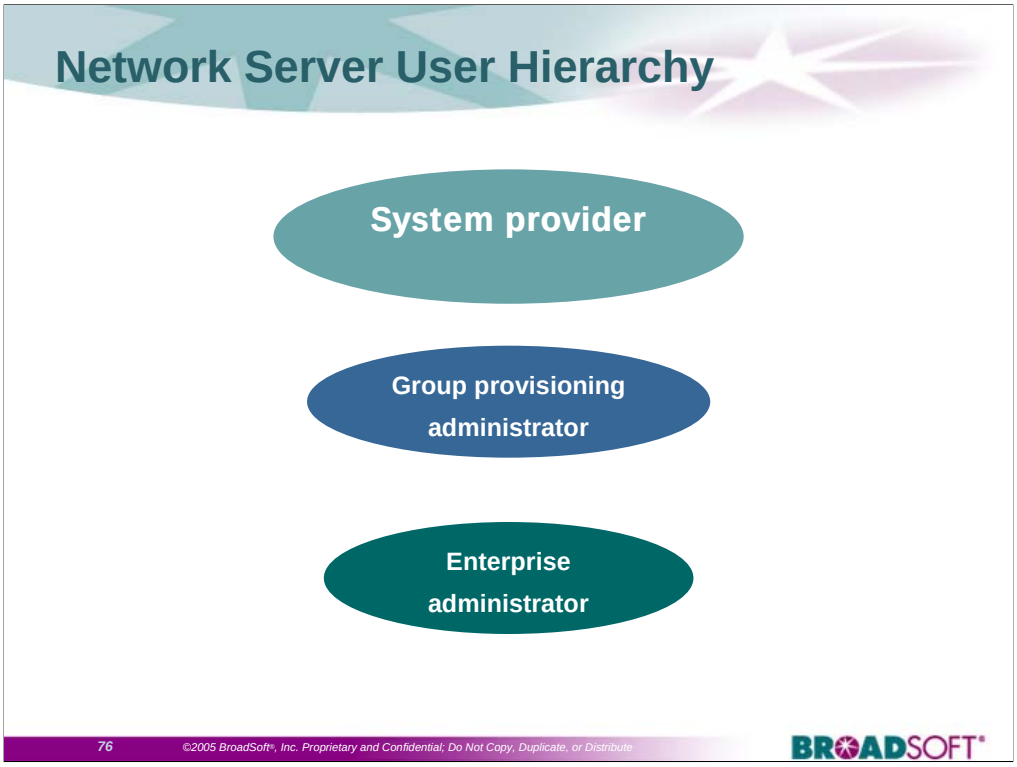
Network Server is delivered with the commercial database, TimesTen.

When a change occurs in a server, data is automatically replicated to the other Network Server databases. Replication ensures consistency between servers.

Load Balancing

Load balancing ensures distributed usage of the Network Servers in a configuration and also permits Network Servers to operate in failover mode.

Load balancing between Network Servers is performed through route list management; Application Servers use a pre-defined route list or a DNS-returned route list.



Levels of Access

System provider

Accesses and manages all Network Server information.

Performs system maintenance and management, maintains system and subscriber security, and monitors system events.

Sets system-wide service and interface parameters to configure public routing and translations functionality and configure network elements.

Creates and manages enterprise private policies.

Customizes and brands the BroadWorks interface.

Group provisioning administrator

Management access to subscriber management level.

No access to system information and policies.

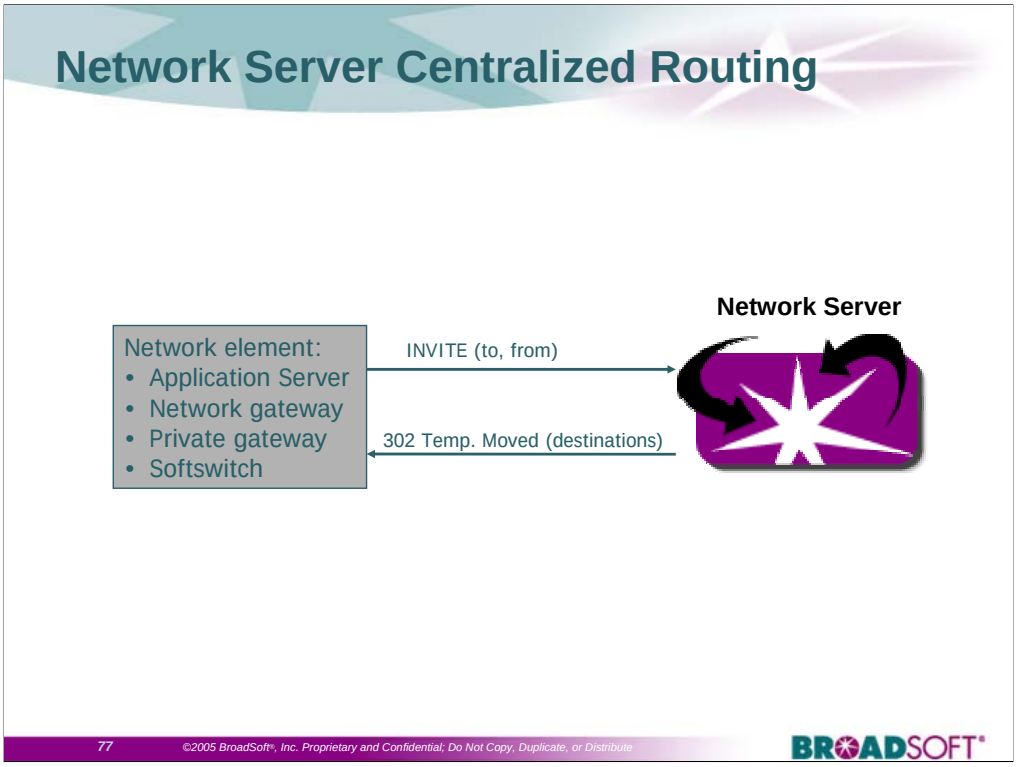
Enterprise administrator

Access to information related to a specific enterprise.

Views enterprise and groups attributes associated with enterprise.

Manages private policies.

Verifies private policies.



Network Server

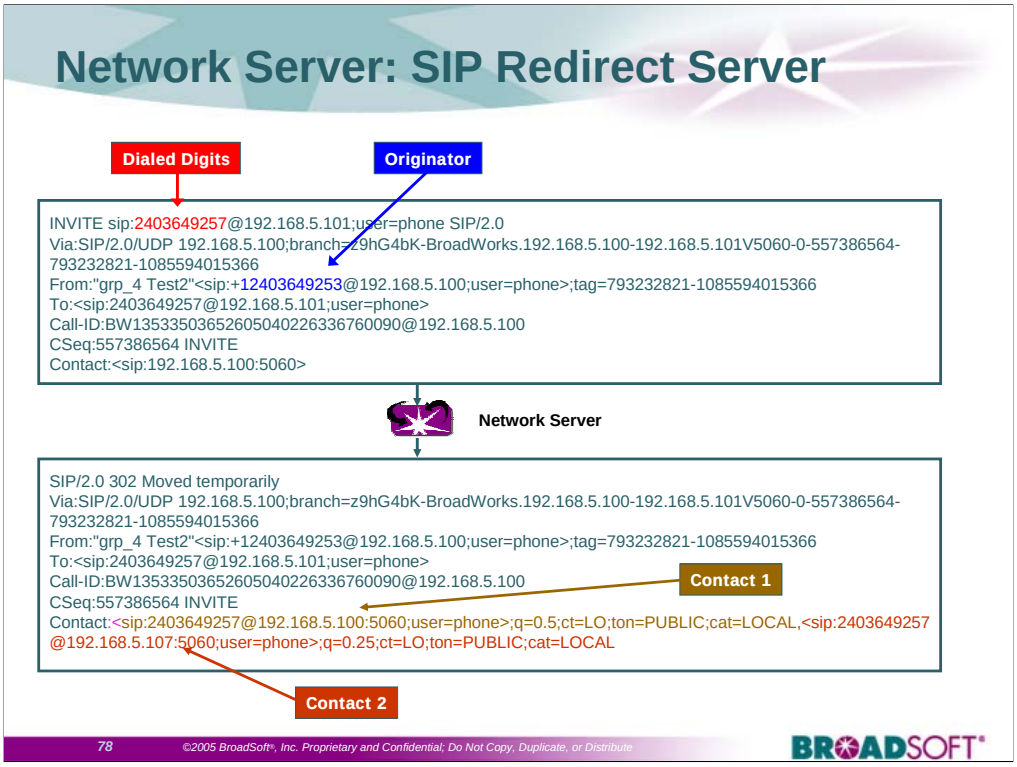
Provides a centralized repository of IP telephony routing information.

Maintains a topology of the network allowing flexible routing policies.

Policy-driven engine to determine destinations: location register, centralized routing.

Translations are DN-driven (E.164 encoding is imposed).

Transaction based (stateless).



SIP Redirect Function

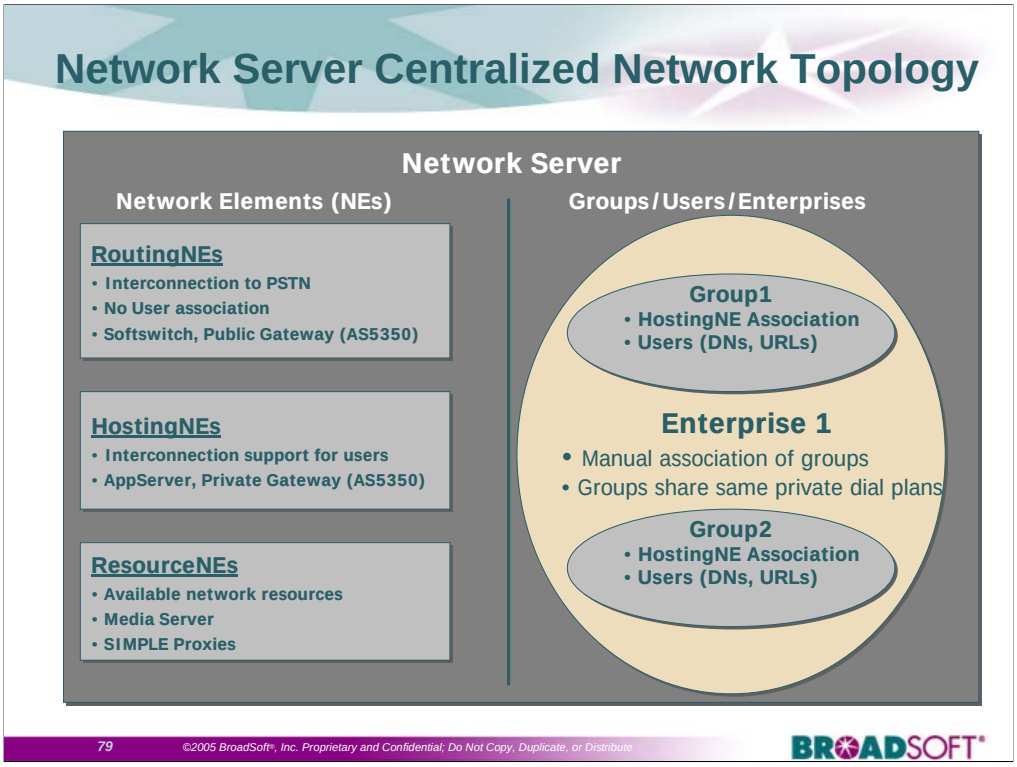
Network Server receives incoming INVITE from network element (NE).

Network Server processes INVITE and applies policies based on dialed digits, originator, forwarding party.

Network Server returns "*302 Moved Temporarily*" message to NE.

NE creates a new INVITE with URI equal to the Contact info provided.

If first Contact does not respond, NE will route advance to next contact.



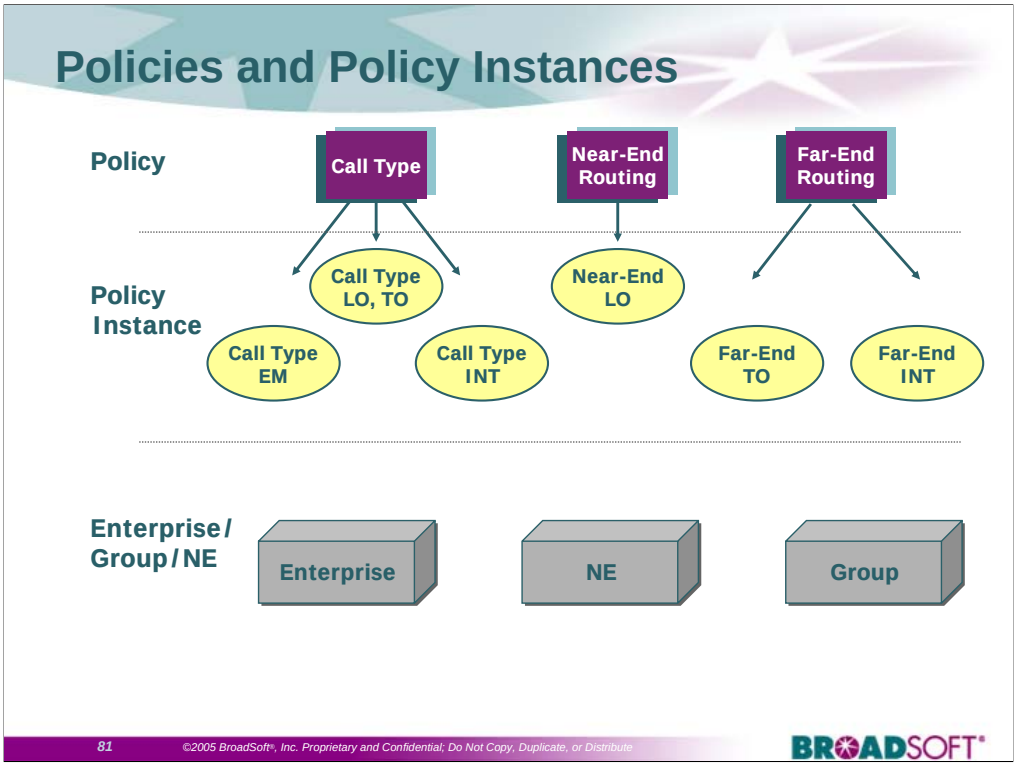
Network Topology

Network topology must be known by the Network Server to return a contact for calls from the network elements.

Users and their groups must be known to the Network Server to return a contact for their calls to proceed.

Translations and Routing Basics

- **Network Server uses policies to translate and route incoming calls**
- **Policy is a set of rules defining how to translate and route calls**
- **Two families of policies:**
  - **Public policies**: Globally defined and assigned to routing profiles by the system provider
  - **Private policies**: Assigned and configured by enterprises and are used to provide VPN-type services
- **Policies are configurable by Network Server administrator**



Policy

Set of rules used to translate or route a call.

Can be network-wide or specific to an enterprise.

Usually has configuration information that customizes the policy, thereby creating a policy instance.

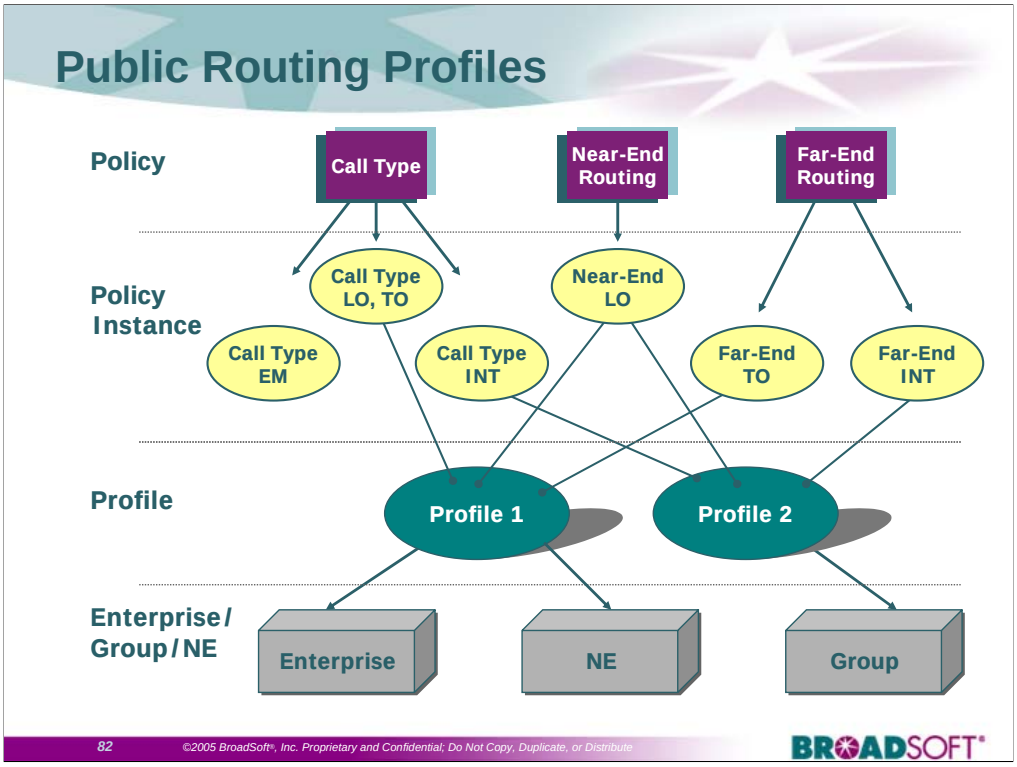
Policy Instance

Customization of a policy.

Used to provide a specific type of processing, for example, on-net routing.

Public policy instances can be grouped to create a routing profile which can be assigned to enterprises, groups, HostingNE, or RoutingNE.

Private policy instances are assigned to an enterprise.



Public Routing Profile

A routing profile is a set of public policies.

A routing profile can be assigned to a RoutingNE, HostingNE, enterprise, or group.

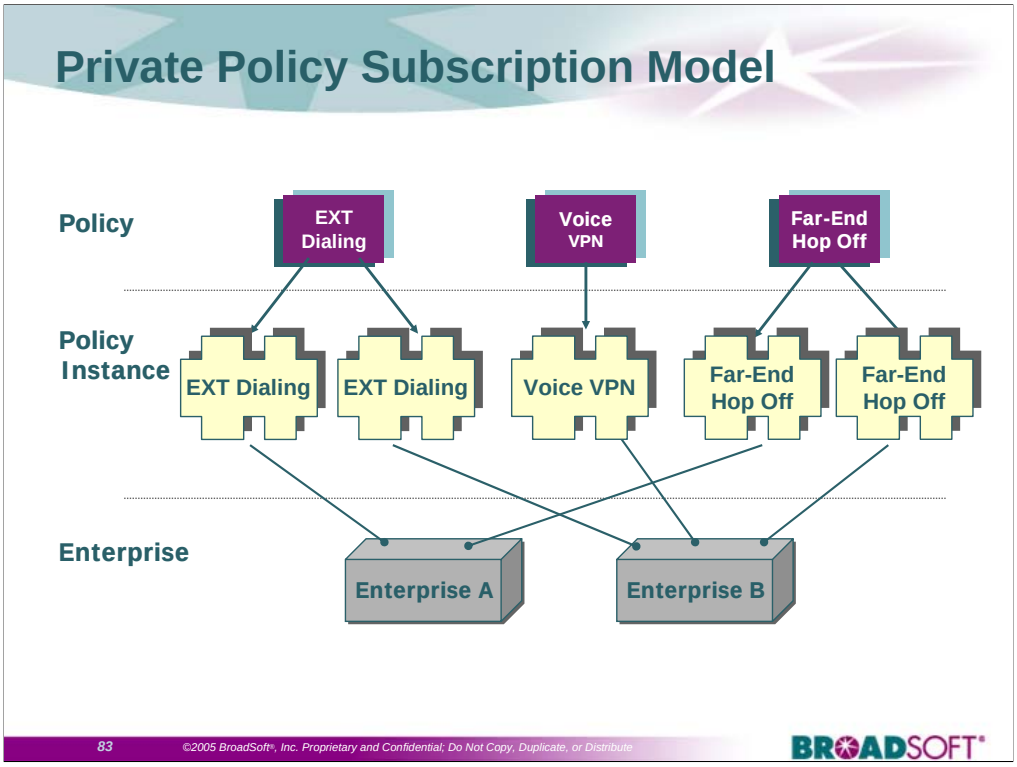
Relationship between public policies, policy instances, profiles, and enterprises (consisting of groups of subscribers)

A public policy can have multiple instances.

A public policy instance can be assigned to more than one profile.

A public routing profile can be assigned to more than one enterprise, group, HostingNE, or RoutingNE.

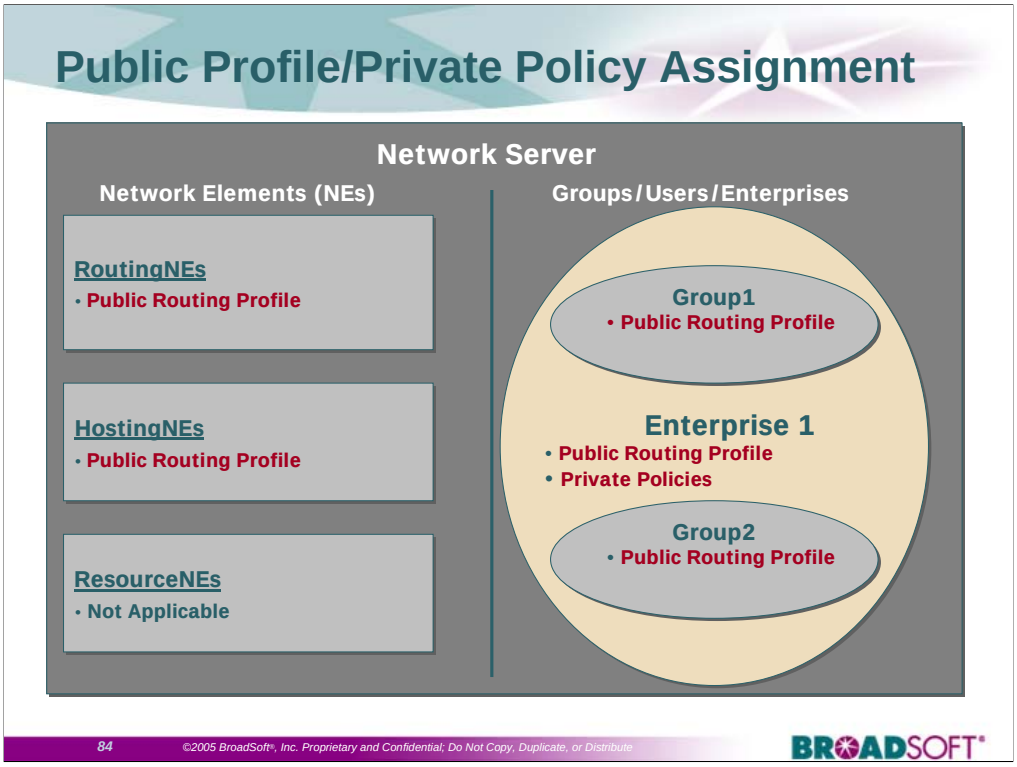
A public policy is triggered (applied to a call) or not based on the call type returned by translations.



Private Policy Subscription Model

There is no profile concept for private policies

Private policies instances are directly assigned to enterprises



RoutingNE Profile Selection

If the call is incoming from a RoutingNE, the RoutingNE public profile is selected.

HostingNE Profile Selection

Users belong to groups that are associated with a HostingNE.

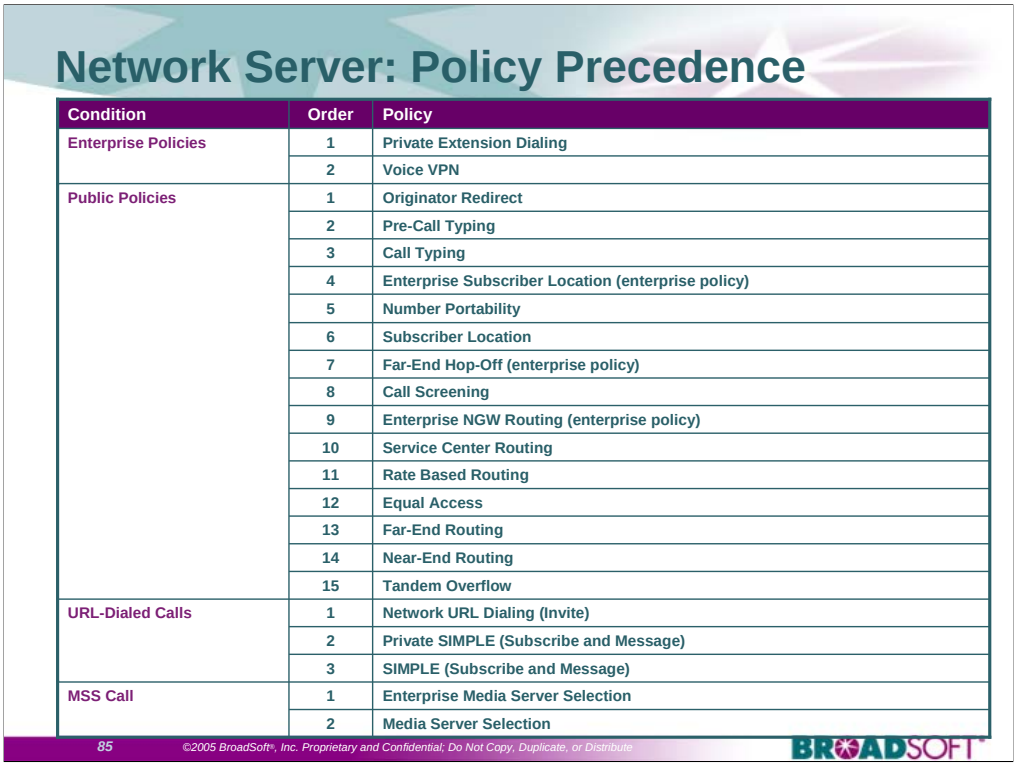
Group can belong to enterprises.

Groups, enterprises, and HostingNEs can have public profiles associated to them.

Network Server first selects the group profile, if available, then performs an intersection with the enterprise profile.

Group profile policies have precedence over enterprise profile policies.

HostingNE profile is only when the FROM: DN is not identified (not a known Network Server DN or URL).



Network Server Policies

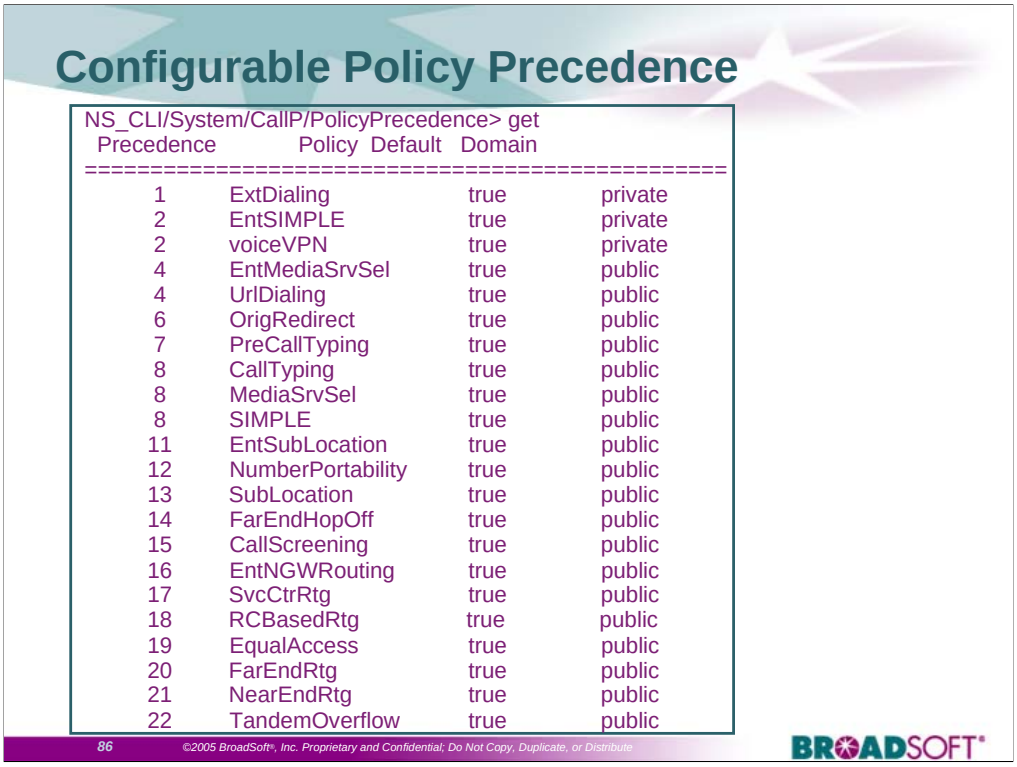
Private policies can be assigned to an enterprise.

Public, URL and Media Server selection policies can be associated together in a profile and then assigned to:

– Network element

– Enterprise

– Group



Configurable Policy Precedence

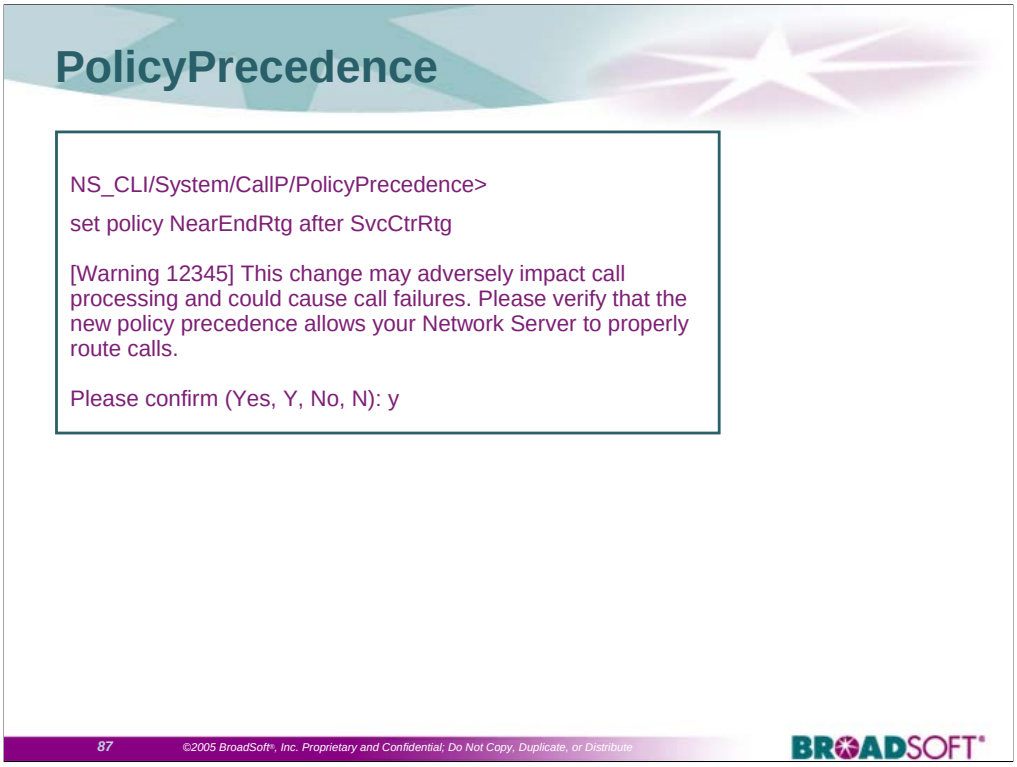
The Network Server now supports the following ordering functions:

– Move policy A **before** policy B.

– Move policy C **after** policy D.

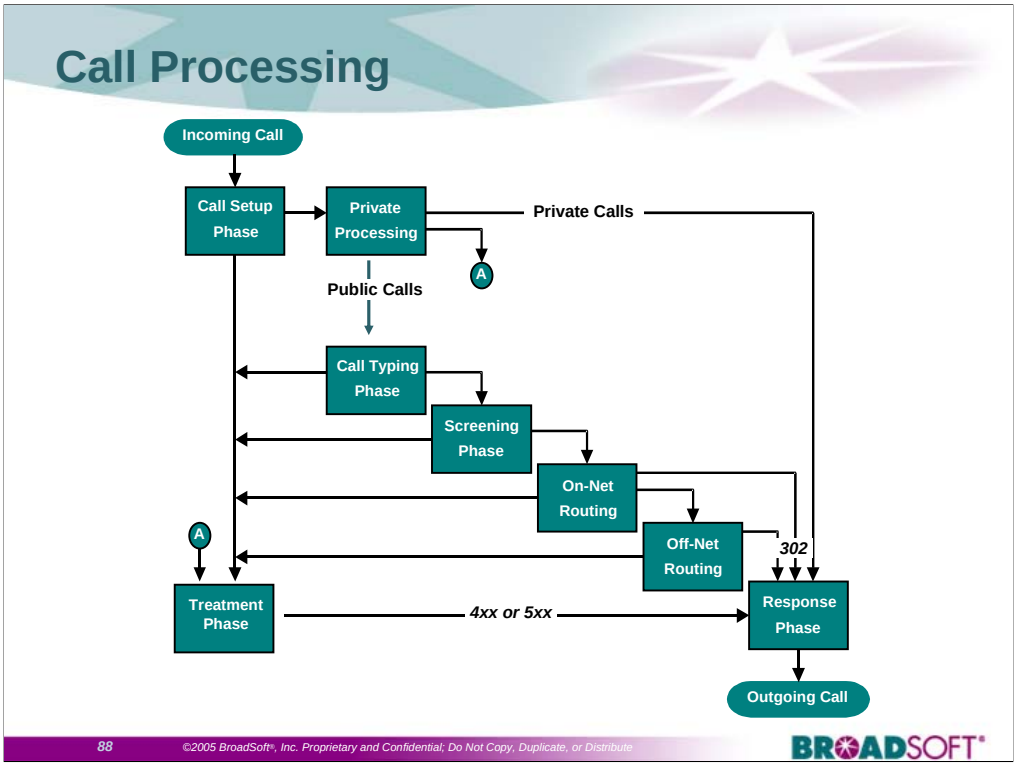
– **Reset** the precedence number of **policy** E to its original default value. The actual new position of policy E relative to the others is undetermined as the order of the other policies might have been changed by previous commands.

– **Reset** the precedence number of **all** policies to their original default value.



Set

<attribute>, Choice = {defaultAll, policy}
policy:
<name>, Choice = {CallScreening, CallTyping, EntMediaSrvSel, EntNGWRouting, EntSIMPLE, EntSubLocation, EqualAccess, ExtDialing, FarEndHopOff, FarEndRtg, MediaSrvSel, NearEndRtg, NumberPortability, OrigRedirect, PreCallTyping, SIMPLE, SubLocation, SvcCtrRtg, TandemOverflow, UrlDialing, voiceVPN}
<action>, Choice = {after, before, default}
after:
<name>, Choice = {CallScreening, CallTyping, EntMediaSrvSel, EntNGWRouting, EntSIMPLE, EntSubLocation, EqualAccess, ExtDialing, FarEndHopOff, FarEndRtg, MediaSrvSel, NearEndRtg, NumberPortability, OrigRedirect, PreCallTyping, SIMPLE, SubLocation, SvcCtrRtg, TandemOverflow, UrlDialing, voiceVPN}
before:
<name>, Choice = {CallScreening, CallTyping, EntMediaSrvSel, EntNGWRouting, EntSIMPLE, EntSubLocation, EqualAccess, ExtDialing, FarEndHopOff, FarEndRtg, MediaSrvSel, NearEndRtg, NumberPortability, OrigRedirect, PreCallTyping, SIMPLE, SubLocation, SvcCtrRtg, TandemOverflow, UrlDialing, voiceVPN}



The Network Server call processing model is based on a multi-stage approach; phases are mapped to one or more policies.

Call Setup

Maps incoming call to enterprise/routing element.

Identifies public profile enterprise/routing element.

Identifies private policies associated with enterprise.

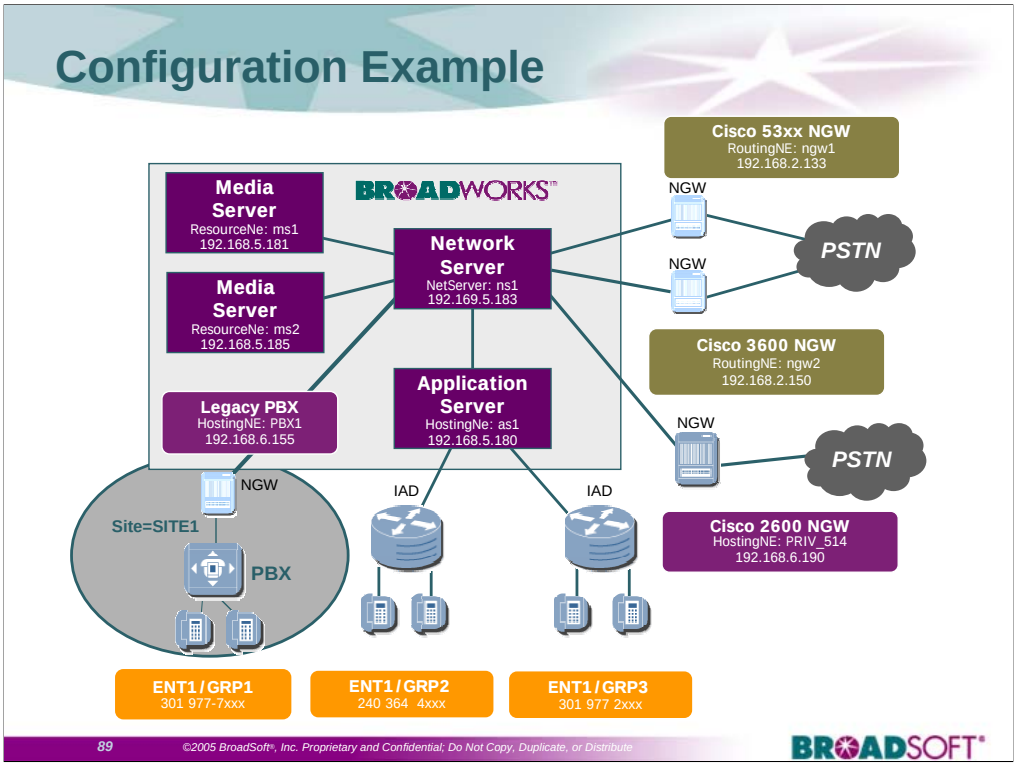
Private Processing

Applies private policies associated with enterprise.

No match, call may or may not continue to public processing depending on permissive/non-permissive setting.

Public Processing

Applies public policies associated with selected profile.



Network Server Dial Plan: Private Policies

AS groups (GRP2/GRP3) and PBX users (GRP1) are part of the ENT1 enterprise.

ENT1 has ExtDialing assigned to support redundancy.

Private dialing using ENT1 VoiceVPN private policy:

4xxx/2xxx VoiceVPN dialing to groups, 7xxx VoiceVPN dialing to PBX users

9+ PSTN dialing for PSTN local/toll/international calls

911/411 calls do not require 9+ dialing

Calls to 514 area code use the ENT1 FarEndHopOff private policy to route to private gateway PRIV_514 and drop off as local 10-digit calls.

Site1 users use the ENT1 EntNGWRouting policy to route DA calls to private gateway PRIV_514.

Network Server Dial Plan: Public Policies

CallTyping policy – for proper setting of call type.

SubLocation policy- allowing on-net calling between all hosted.

MediaSrvSel policy – allowing for MS selection by the Network Server.

Local calls from 240364xxxx users use ngw1, Local calls from 301977xxxx users use ngw2 (NearEndRtg).

Toll calls for all users use ngw1, International calls for all users use ngw2 (FarEndRtg).

911 calls from 240364xxxx use ngw1, 911 calls from301977xxxx use ngw1 and prepend a 99 gateway routing prefix (SvcCtrRtg).

411 calls from all users use ngw1 or ngw2 after 411 has been replaced by 18005551234 routing number to preferred OA carrier (SvcCtrRtg).

Configuration Steps

Step 1: Basic Network Server Configuration
- Network Server identity

Step 2:Public Policy Configuration
- Public policies instances
- NNACL and LCA file for public routing
- Public profiles for enterprise and routing element assignment
- Equal access carriers

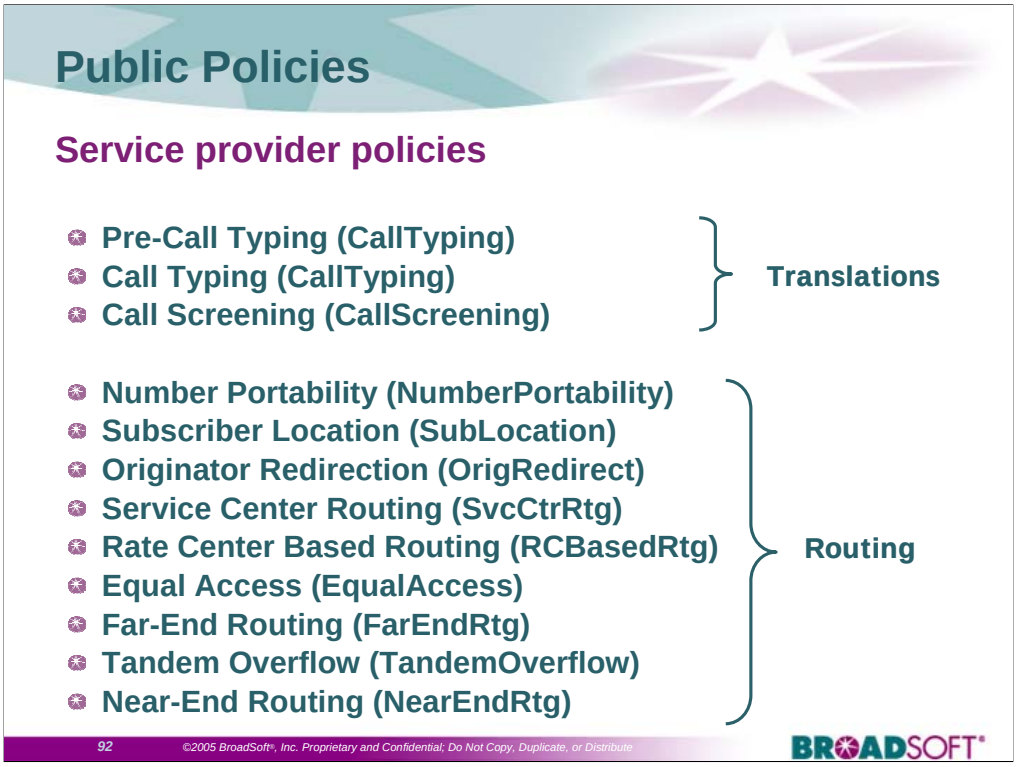
Step 3: Network Server Device Configuration
- Hosting NE entities
- Public routing NE entities
- Media Servers

Step 4: Public Routing Configuration
- Number Portability
- Fixed static Near/Far-End Route list
- Service Center Routing Route list
- Rate Center Based Routing

Step 5: Enterprise Private Policy Configuration
- Create enterprises and assign private policies
- Create VoiceVPN Dial Plan
- Set up FarEndHopOff
- Set up EntNGWRouting

Basic Network Server Configuration

```
NS_CLI/System/Alias> add 192.169.5.183
NS_CLI/System/Alias> add ns.lab.broadsoft.com
NS_CLI/System/Alias> add ns1.lab.broadsoft.com

NS_CLI/System/Alias> get
About to access 6 entries. Continue?
Please confirm (Yes, Y, No, N): y
Retrieving data... Please wait...

127.0.0.1
192.169.5.183
ns.lab.broadsoft.com
ns1.lab.broadsoft.com
```



Translation policies determine the call type and category of the call.

Call types can either be system- or user-defined.

System-defined call types are mandatory and are always added back, if deleted.

User-defined call types are added by a system provider and can be referred to from policies with flexible call type support.

Call Categories

There are five call categories that are subsets of call types:

– Local

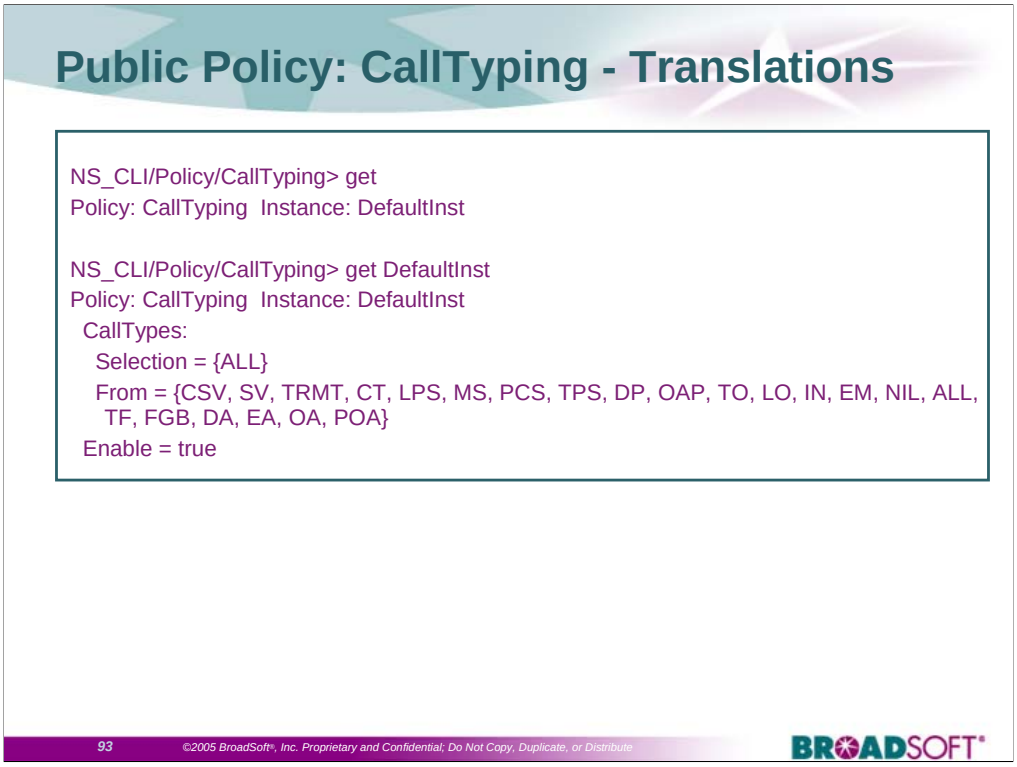
– Intra-LATA/National (Call within a LATA)

– International

– Inter-LATA (calls between two LATAs)

– Other

Routing policies determine the contact(s) to return in the 302 SIP message.



The Call Typing policy uses the Dial Plan of the country code set at installation. This policy then looks at the dial plan to determine the call type, if it matches the selection parameter it will continue with the call routing procedure. If not it returns a treatment.

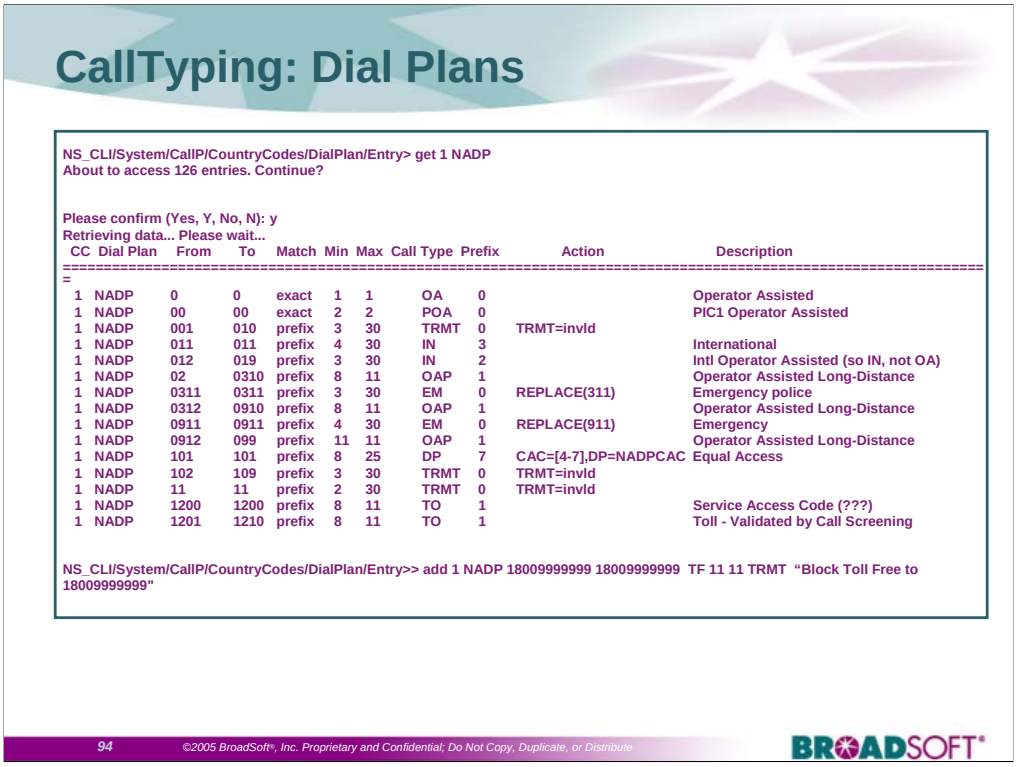
Call Typing Policy Instance Setup

The get command with no parameter returns a list of policy instances.

Using the get command with the instance name displays the policy parameters set for that instance.

The set command with the instance name is used with the following fields:

Selection	Selects the call types to trigger on.	
Enable	false	The instance is not active (off).
	true	The instance is active (on).



Dial Plans

The Network Server is delivered with default public dial plans and provides support for the public North American Dial Plan (all NA call types).

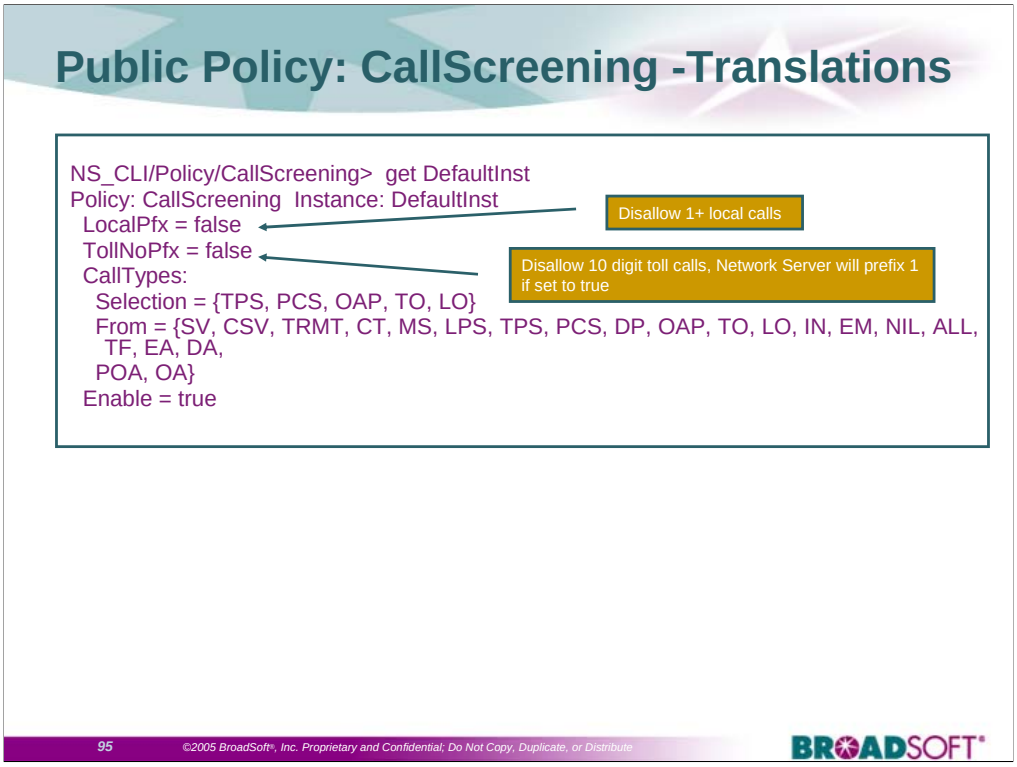
System providers can build their own public dial plan or customize an existing one using the CLI.

Dial plans are applied based on the country code of NE that originated the INVITE.

When the INVITE terminating DN is a global E.164 number (starts with a +), this policy causes the call processing to jump from the current instance to another specified Call Typing instance which handles E.164 DNs with no prefix.

The add command and the following fields are used to add an entry to the dial plan:

Field	Description
CountryCode	Specifies the country code for which a dial plan entry applies.
DialPlanID	A dial plan name used to assemble a collection of from-to digit ranges.
*From/*To	Digit sequence defining the beginning/end of a range of digits.
Match	Defines the scope of from-to range. “Prefix” means that this entry applies if the called party number starts with digits matching from-to range. “Suffix” means that this entry applies if the called party number ends with digits matching from-to range. “Exact” means that this entry applies if the called party number is identical to from-to number.
CallType	Call type to be set if the incoming digit sequence is included in the range defined by from-to, and has a length between Min and Max.
Prefix	The prefix to be set, if the incoming digit sequence is included in the range defined by the from-to, and has a length between Min and Max. The prefix indicates the number of prefix digits to ignore.
Min/Max	Minimum/maximum length of a digit sequence for the rule to apply.
Action	Describes: Actions to be taken by the translation (run-time). Extra conditions on digit pattern matching.
Description	Short description of the expected behavior for the given digit range.



The Call Screening Policy has been designed to work with the North American Numbering Plan. It validates that the call type found by the Call Typing policy is coherent with NPA/NXXs implied in the call.

Knowing the NPANXX of the originator and at least the NXX of the terminator, the Call Screening policy searches the NNACL (NPA/NXX Active Code List) and LCA (Local Calling Area file) database to determine the category of the call (local, intra-LATA toll, and inter-LATA). It then checks if the call type found by the Call Typing Policy is valid based on the dialed digits.

Call Screening Policy Instance Setup

The get command with no parameter returns a list of policy instances.

Using the get command with the instance name displays the policy parameters set for that instance.

The set command with the instance name is used with the following fields:

Selection	Selects the call types to trigger on.	
Enable	false	The instance is not active (off).
	true	The instance is active (on).
LocalPfx	true	Allows 1+ local calls.
	false	Disallows 1+ local calls.
TollNoPfx	true	Allows 10-digit toll calls (NS prefixes 1 to calls).
	false	Disallows 10-digit toll calls.

CallScreening – NNACL and LCA files

```
NS_CLI/System/CallP/Translation> set NNACL dir /var/broadworks/translations/nnacl/
NS_CLI/System/CallP/Translation> set LCA dir /var/broadworks/translations/lca/
NS_CLI/System/CallP/Translation> set NNACL File 3Q01nnacl
NS_CLI/System/CallP/Translation> set LCA  File GBURG.lca
NS_CLI/System/CallP/Translation> set active

NS_CLI/System/CallP/Translation> get
Sending the request
      NNACL(1)                              LCA(1)
      --------                               ------
Name:                                 Name:
Status: No File Loaded                      Status: No File Loaded
Row(s): 0                             Row(s): 0
Date:                                 Date:

      NNACL(2) *Active*               LCA(2) *Active*
      --------                        ------
Name:   1Q03nnacl                           Name: GBURG.lca
Status: File Loaded                         Status: File Loaded
Row(s): 144262                              Row(s): 256
Date:   Sep 1, '04 at 10:48 AM        Date:   Sep 1, '04 at 10:42 AM
```


Call Screening Policy

Determines the category of the call:

– Local

– Intra-LATA toll

– Inter-LATA toll

Works in conjunction with the North American Numbering Plan (NANP).

Uses the NPA-NXX Active Code List (NNACL) file provided by Telcordia for North America.

Uses the Local Calling Area (LCA) file, a file customized by the system provider that specifies a list of originating rate centers and their related terminating rate centers/NPA-NXX codes for which the call will be categorized as local.

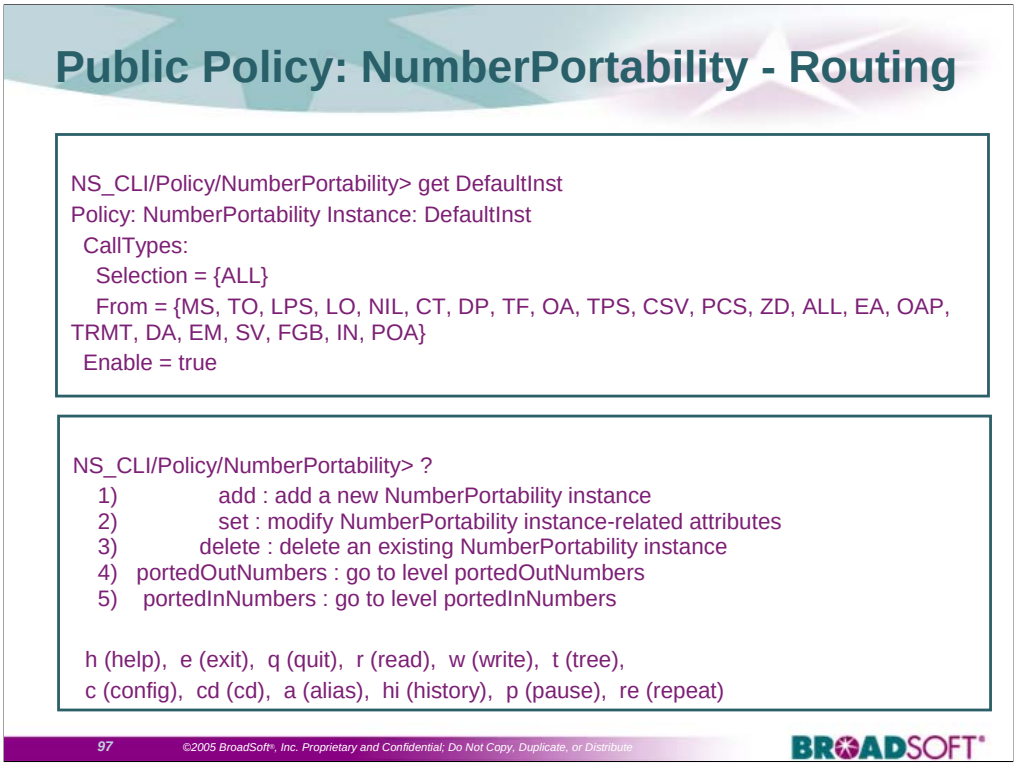
NNACL and LCA File for Public Routing

Create directories /nnacl and /lca under /var/broadworks/translations/.

FTP Telcordia-provided NNACL file to /nnacl directory.

FTP operator-provided LCA file to /lca directory.

Set translations directory path and file name.

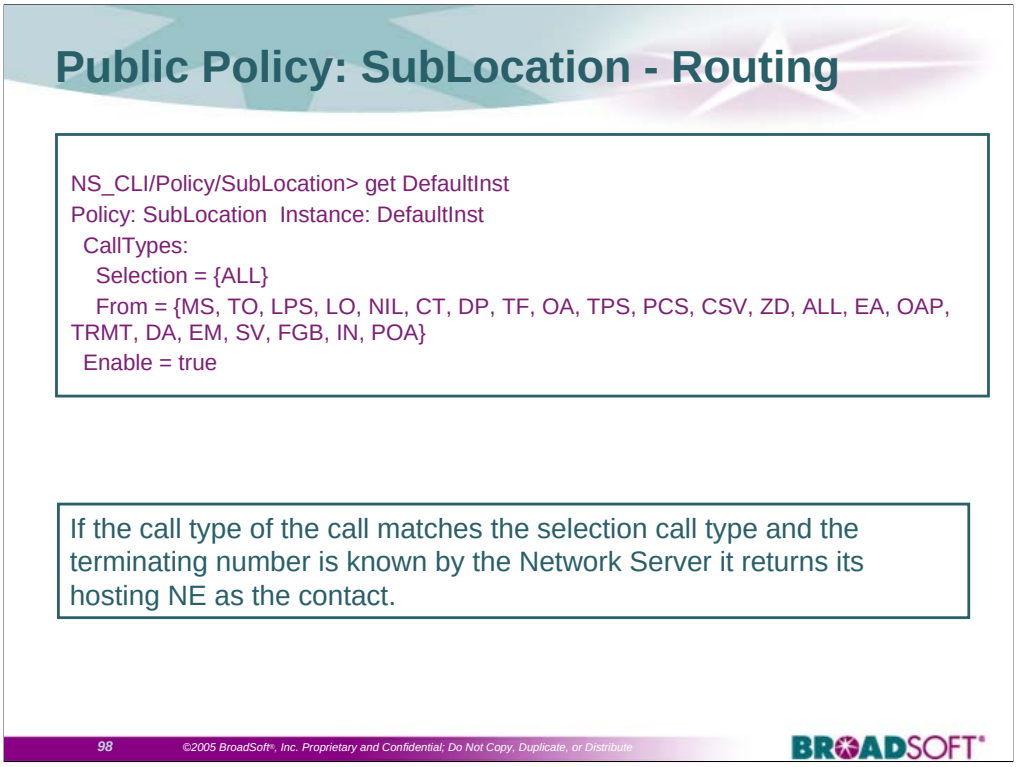


Number Portability Policy

Supports users ported on to BroadWorks and users ported out of BroadWorks.

The external number of the ported users remains the same and an internal routing number or route is used to port the users from one system to another.

```
NS_CLI/Policy/NumberPortability/portedOutNumbers> get DefaultInst
Policy: NumberPortability Instance: DefaultInst  Table: PortedOutNumbers
  portedOutNumber     internalNumber   routingNe  cost weight  dmi
================================================================
     15145550000       +1555559999        -    -     -   -1
     15145550011        1555559988       ngw1    1     99   -1
     15145550011        1555559988       ngw2    1     99   -1

NS_CLI/Policy/NumberPortability/portedInNumbers> get DefaultInst
Policy: NumberPortability Instance: DefaultInst  Table: PortedInNumbers
   PortedInNumber       PublicNumber
==================================
     15145552222        1555553333
```



Subscriber Location Policy

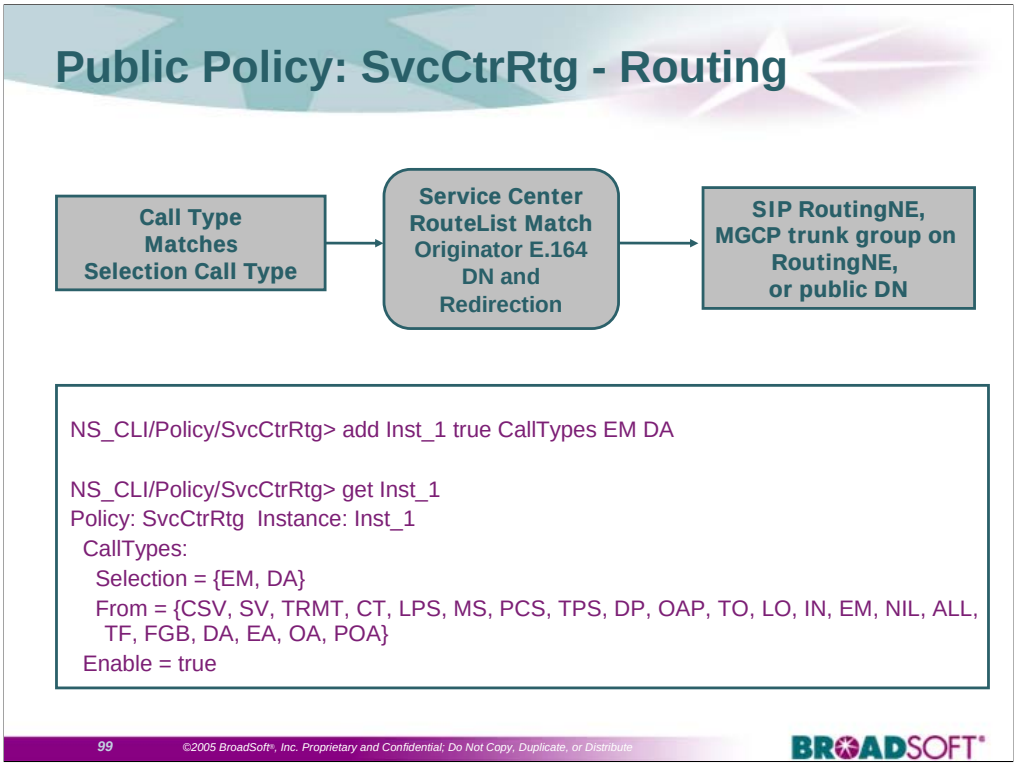
Applies to on-net routing.

Identifies the “dialed digits” as a subscriber on the Network Server and allows incoming calls to terminate to end user in a given IP network.

Used to allow on-net calling between users in different groups (and/or different Application Servers) by returning the terminators HostingNE in the contact list.

Used for calls from the PSTN (RoutingNE) to terminate a call to a known user on the IP network.

Without SubLocation, public calls between Network Server users always route to PSTN through off-net routing.



Service Center Routing Policy

The Service Center Routing Policy (SvcCtrRtg) is an origination-based routing policy. It allows a Network Server administrator to route incoming calls to specific destinations based on the call originator and on the Network Server identified call type.

This policy uses service routing entries to map incoming call types, call attributes, and originator defined by a range of valid digits to a destination. It provides support for three types of routing results:

– Fully-specified DN destination

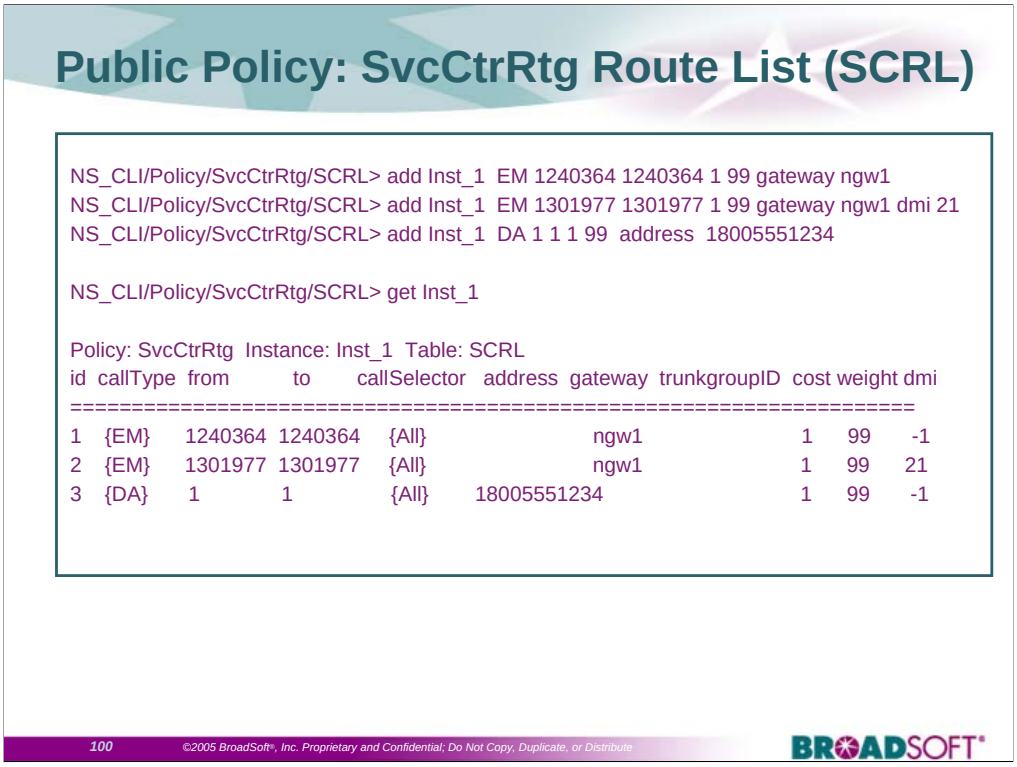
– A destination network gateway

– A destination MGCP gateway with and a specific trunk group name

Users can access unique SCRLs through application of different SvcCtrRtg policies and instances to public policies.

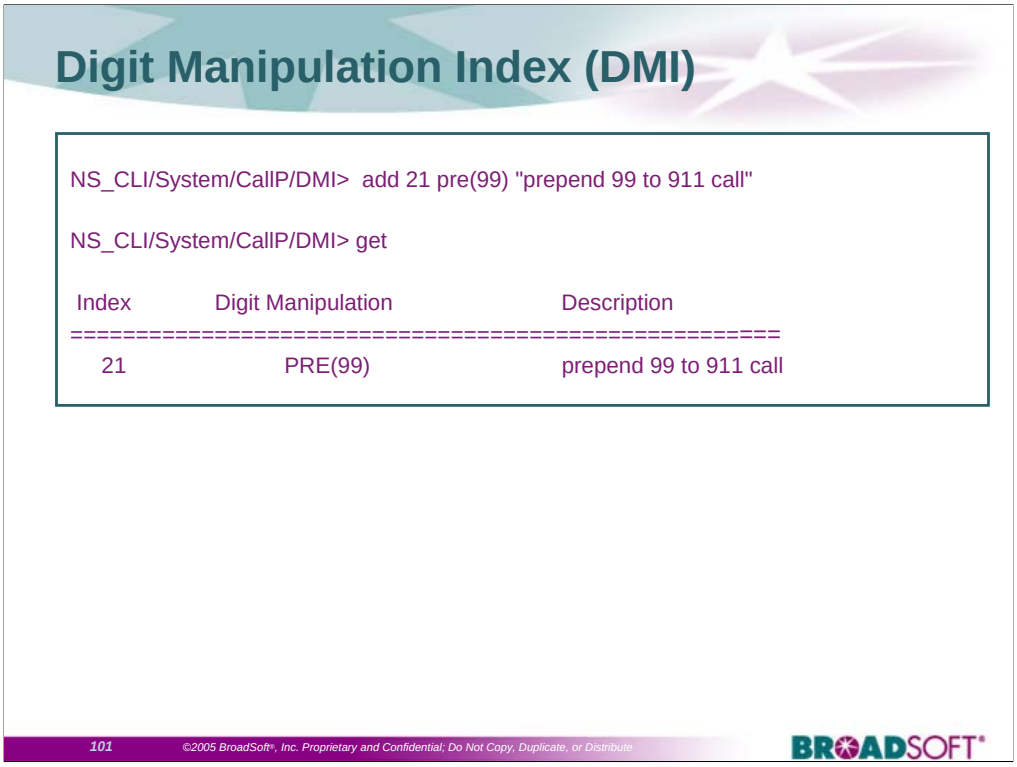
Supports multiple routes with different results cost and weighting (multiple contacts returned).

Supports full digit manipulation of dialed digits.



Service Center Routing List

CallType	Call type to which this entry applies.
From/To	Digit sequence defining the beginning/end of a range of digits.
CallSelector	A call attribute used to discriminate if the route applies or not:
	All: Route applies to any call.
	Redirect: Route only applies to calls received with a Diversion indicator.
	NoRedirect: Route only applies to calls received without a Diversion indicator.
Cost	Route selection cost.
Weight	Route selection weight.
DMI	Digit manipulation index to the list of service provider-defined digit manipulation algorithm.
Address	(DN) Route to a specific address.
Gateway	Route to a specific routing NE. Destination gateway.
TrunkGrpID	Route to a trunk group. The trunk group's unique ID consists of:
	Protocol: The protocol of the trunk group (MGCP).
	TrunkGroup: A string that represents the trunk group name that is used when returned in a contact.
	Channel: The channel that can be used on the specified trunk group.
	Gateway: The MGCP device that owns the trunk group.
	GatewayControllerGroupID: (Optional) The group ID for gateway controllers (hosting NEs). A list of controllers, for example Application Servers used to interface with the MGCP device.



Digit Manipulation Index

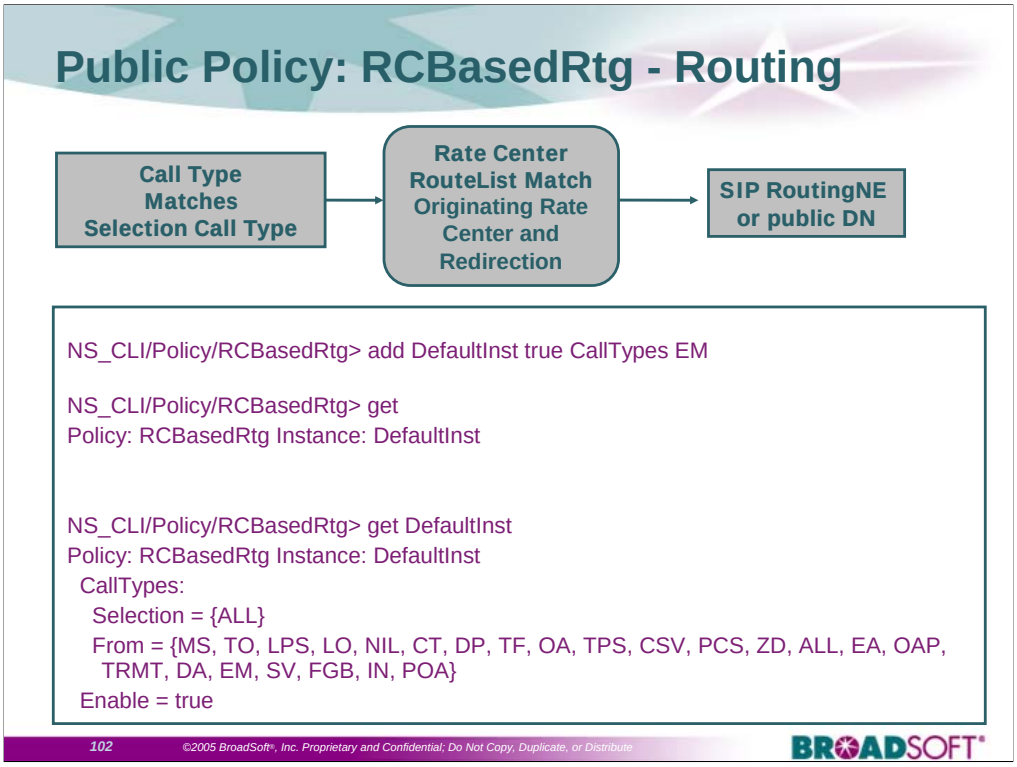
The DMI add command has the following fields:

Index The index number.

dmStr The digit manipulation string or algorithm

desc The description of the digit manipulation string.

The DMI can be used in other policy instances.



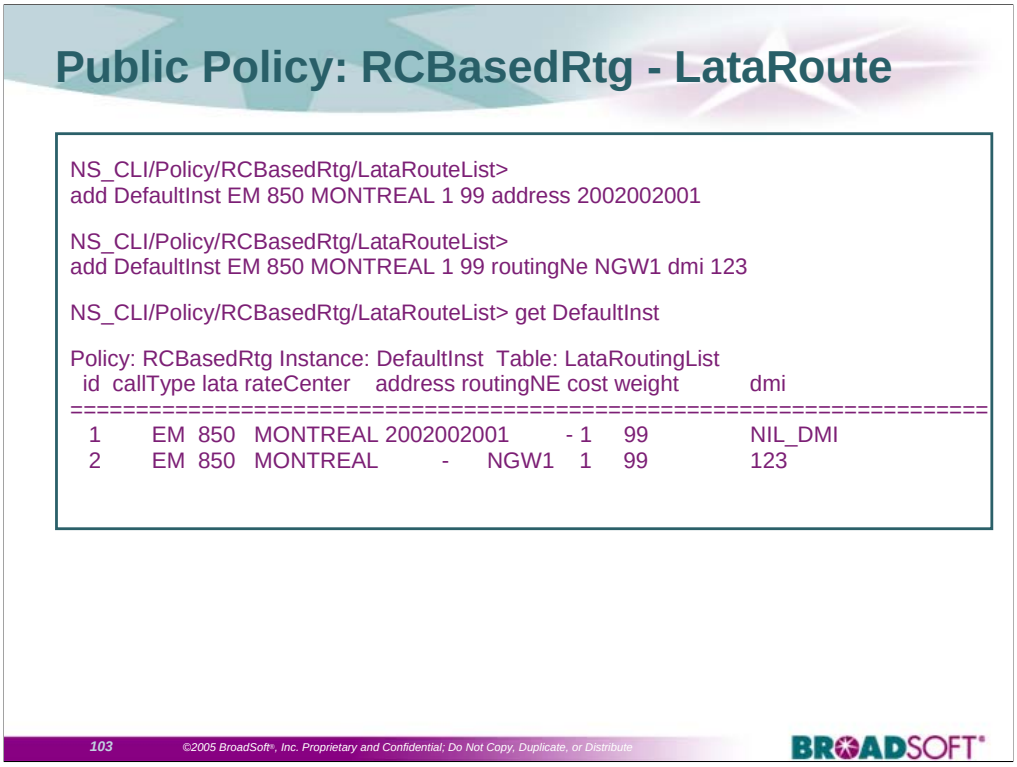
Rate Center Routing Policy

The Rate Center Routing Policy (RCBasedRtg) is an origination-based routing policy. This policy allows a system provider to select a destination based on the call originator's Rate Center and call type.

The rate center identification can be based on one of the following:

– Telcordia NNACL file (also referred as LATA-based rate centers)

– ZONEs assigned directly against NDCs



Rate Center LATA Route List

This command is used to add a new rate center routing rule. Entries can either be used to set a new destination address or a routingNe but not both at the same time. A DMI entry can optionally be specified for both address and RoutingNe results.

add

<instance>, String {1 to 12 characters}

<callType>, Choice = {MS, TO, LPS, LO, NIL, CT, DP, TF, OA, TPS, CSV, PCS, ZD, ALL, EA, OAP, TRMT, DA, EM, SV, FGB, IN, POA}

<lata>, Integer {100 to 9999}

<rateCenter>, String {3 to 25 characters}

[<attribute>, Multiple Choice = {cost, weight, address, routingNe, dmi}]

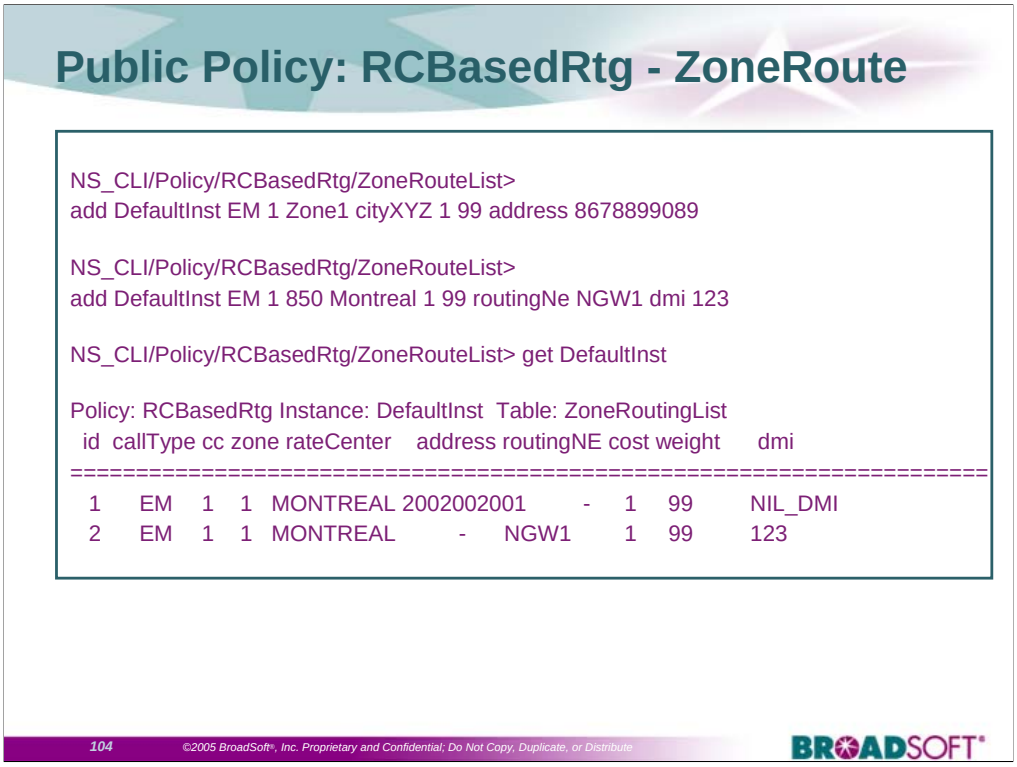
<cost>, Integer {1 to 9}

<weight>, Integer {0 to 99}

<address>, String {1 to 15 characters}

<routingNe>, String {1 to 40 characters}

<dmi>, Integer {-1 to 32767}



Rate Center Zone Route List

This command is used to add a new rate center routing rule. Entries can either be used to set a new destination address or a routingNe but not both at the same time. A DMI entry can optionally be specified for both address and RoutingNe results.

add

<instance>, String {1 to 12 characters}

<callType>, Choice = {MS, TO, LPS, LO, NIL, CT, DP, TF, OA, TPS, CSV, PCS, ZD, ALL, EA, OAP, TRMT, DA, EM, SV, FGB, IN, POA}

<cc>, String {1 to 3 characters}

<zone>, String {1 to 32 characters}

<rateCenter>, String {3 to 25 characters}

[<attribute>, Multiple Choice = {cost, weight, address, routingNe, dmi}]

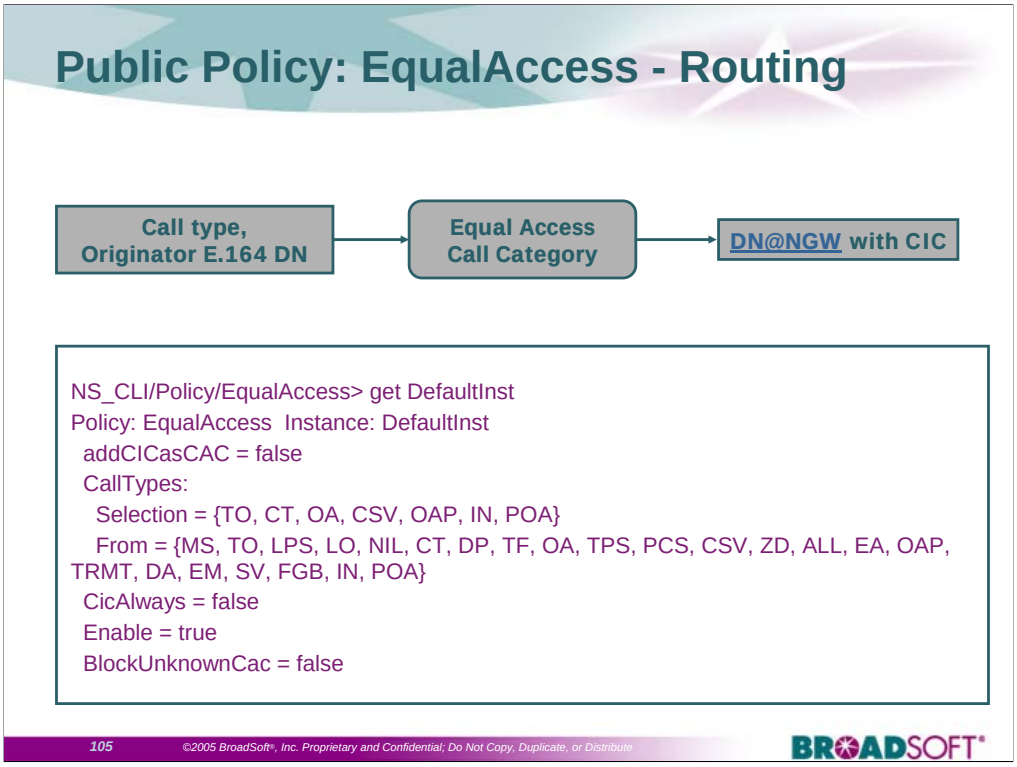
<cost>, Integer {1 to 9}

<weight>, Integer {0 to 99}

<address>, String {1 to 15 characters}

<routingNe>, String {1 to 40 characters}

<dmi>, Integer {-1 to 32767}



Equal Access Policy

The Equal Access policy allows for selection of pre-defined carriers for off-net routing.

Origination-based routing policy triggered on call type toll or international calls.

Uses preferred inter-exchange carriers (PICs).

PICs can be assigned to an enterprise or group.

Each enterprise/group has three PICs provisioned:

– Intra-LATA

– Inter-LATA

– International

System default PICs are configurable.

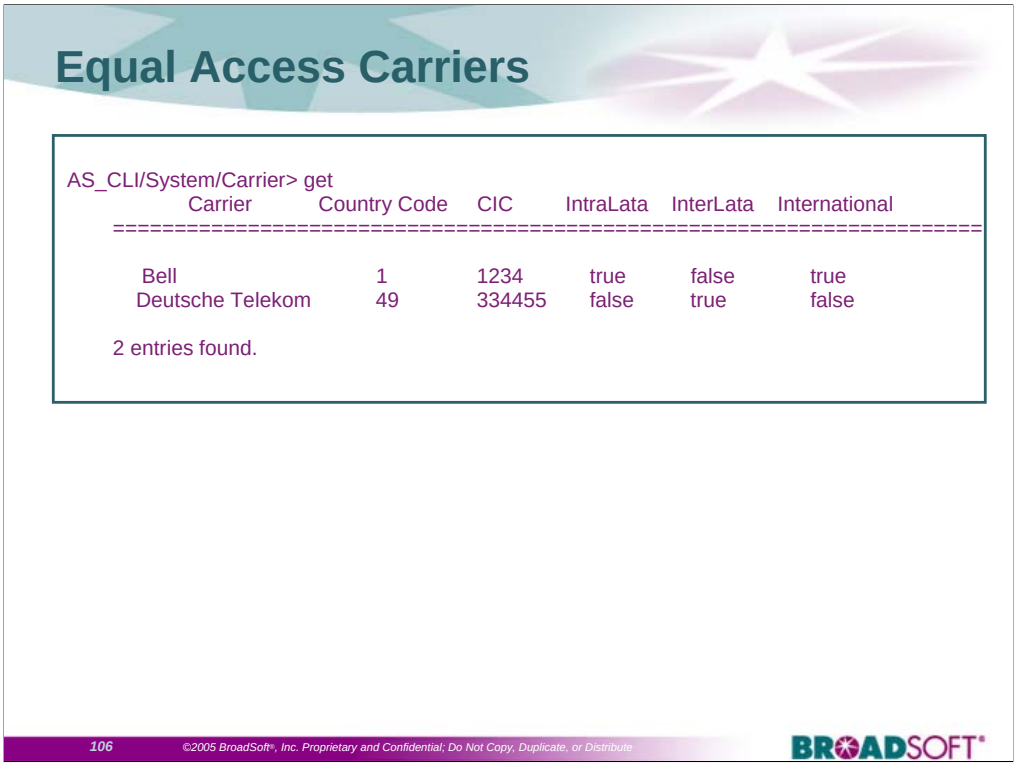
Equal Access Functionality

Can associate a carrier with a list of RoutingNEs.

When a list is not provided, the preferred inter-exchange carrier or carrier access code is prefixed to the outgoing call and routed to the POP device closest to the call originator (selected from the POP devices configured on the Network Server).

Carrier Identification Code (CIC) is passed back to the requesting Network Element (NE) as part of the 302 Temporarily Moved Contact list.

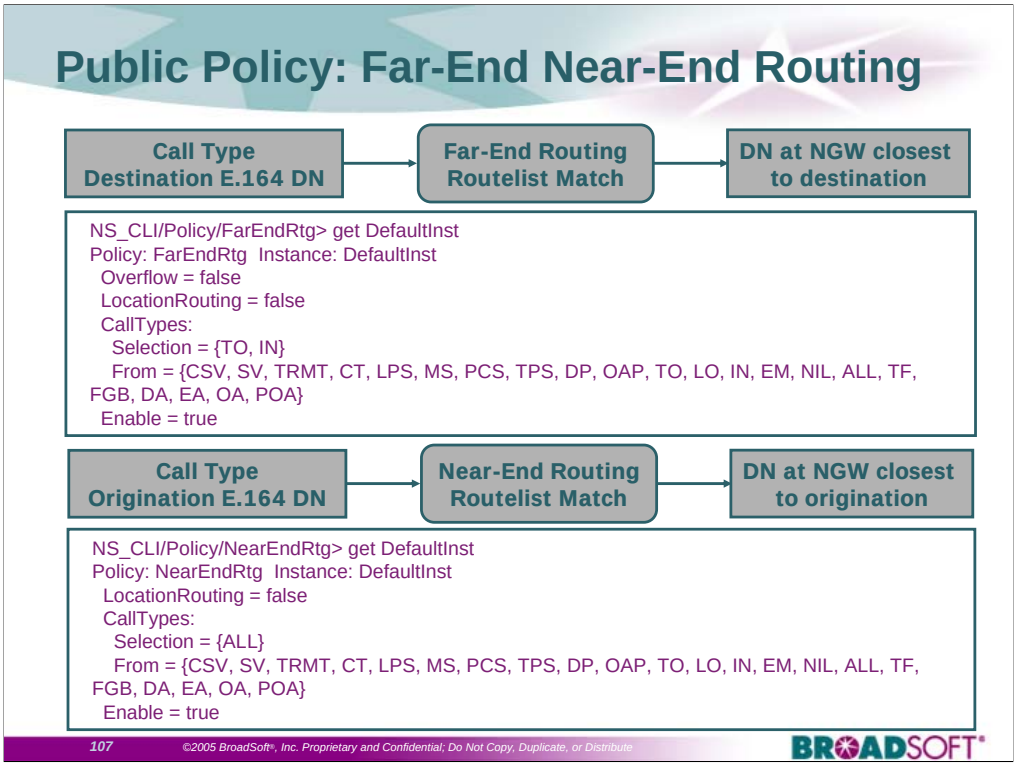
Receiving RoutingNE (SS7 or PRI-based) maps CIC to Transit Network Selector (TNS) parameter in outgoing IAM or SETUP message.



Add an Equal Access Carrier

The add command and the following fields are used to add an Equal Access carrier:

carrier	The name of the carrier.	
CAC	The carrier access code.	
intraLata	no	This carrier does not support intra-LATA toll call routing.
	yes	This carrier does support intra-LATA toll call routing.
interLata	no	This carrier does not support inter-LATA toll call routing.
	yes	This carrier does support inter-LATA toll call routing.
intl	no	This carrier does not support international toll call routing.
	yes	This carrier does support international toll call routing.



Far-End Routing Policy

This policy is used for off-network routing.

Selects a routing path using rules ensuring the least cost.

Identifies the POP device closest to the call destination, for example, between an IP network and the PSTN.

The system provider is the default carrier for the call.

Near-End Routing Policy

This policy is used for off-network routing.

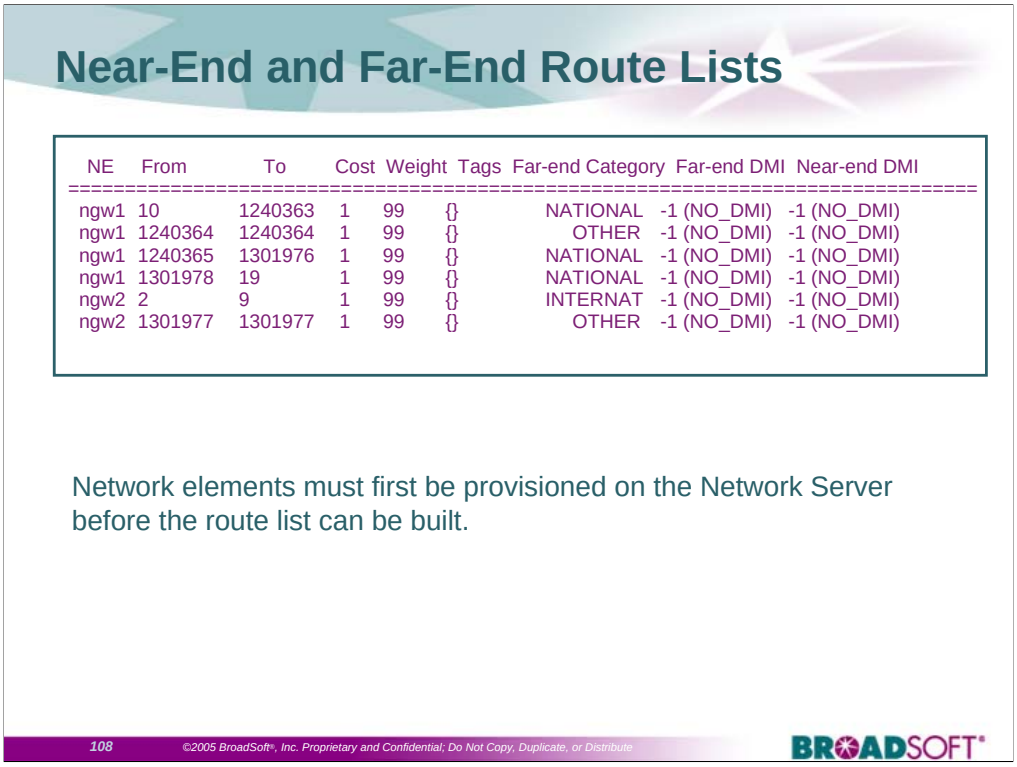
Terminates a call to the network element (point-of-presence [POP] device, such as a network gateway or a softswitch) closest to the call originator.

Uses the network route selector framework to route a call.

Typically the default Network Server policy.

The add command and following fields are used to add an instance:

instance	The name of the instance for this policy.	
Enable	false	The instance is not active (off).
	true	The instance is active (on).
CallTypes	The type of call this policy instance can process.	
LocationRouting	false	Indicates only routing entries are used and that location-based search is not used.
	true	Indicates that the policy tries to find contacts from routing entries and location-based search.



Fixed Route Assignment

Selection based on ranges of originating/terminating E.164 DNs.
Cost to determine route ordering.
Weight to distribute traffic load.
Near-End and Far-End Routing share common route list.

Dynamic Route Selection by Geographic Location of Routing Element

Routing element assigned location (NPA/NXX).
Uses vertical and horizontal (V&H) to find closest routing element.
Used as a backup when no or only one route is identified.
Also used for geographic Media Server Selection.

Telcordia Vertical and Horizontal (V&H)

North America overlaid with vertical and horizontal coordinates grid.
NNACL file provided V&H location for every NPA/NXX.
Example:
202822 EOCN WASHDCMTDS15E 9211236 WASHGTN ZONE 1 05622 01583 DCY

Originator/Terminating NPA/NXX and all routing elements plotted on V&H grid.
Routing elements closest to originator/terminator makes up contact list.

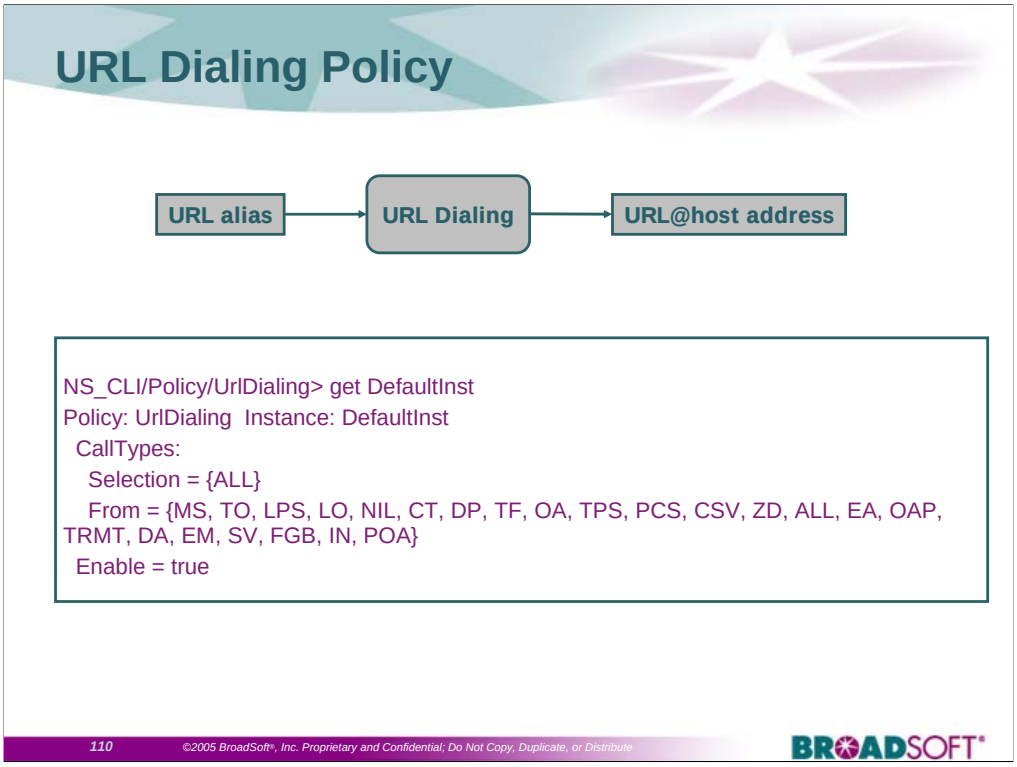
Other Network Server Policies

URL policies

- Network URL Dialing (UrlDialing)
- Public MSN SIMPLE (SIMPLE)
- Enterprise MSN SIMPLE (EntSIMPLE)

Media Server policy

- Media Server Selection (MediaSrvSel)



Network URL Dialing

URL calls are distinguished from DN-based calls.

Performs subscriber location for URL-dialed calls, allowing calls to terminate to any end user in a given IP network.

This is a SIP-based policy.

Call Routing

Upon URL dialing call origination, the Application Server sends the call with an unknown alias to the Network Server.

The Network Server then looks up in its table of URLs to identify the subscriber location.

If the subscriber is found, a 302 (moved temporarily) is returned to the originating Application Server with the new destination attached using the maddr parameter.

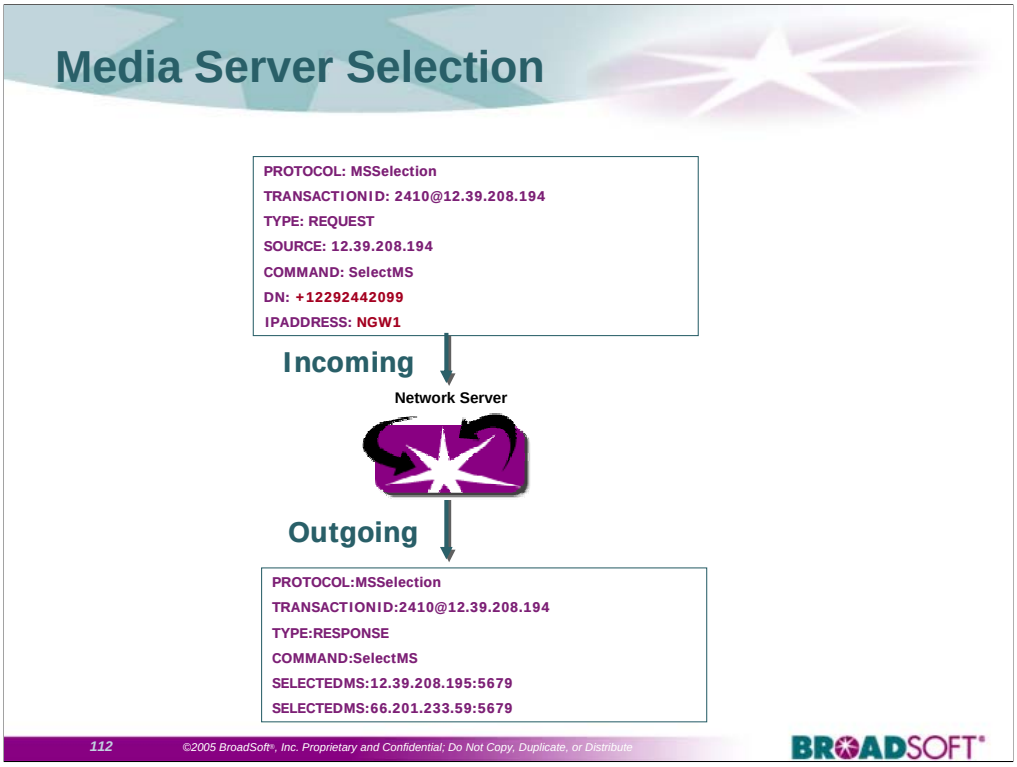
If the subscriber is not found, a 302 is still sent but with the original targeted domain as the new destination.

The add command and the following fields are used to add an instance:

instance	The name of the instance for this policy.	
Enable	false	The instance is not active (off).
	true	The instance is active (on).
CallTypes	The type of call this policy instance can process.	

SIMPLE Policy (Public)

- This policy routes Windows Messenger SIMPLE (Session Initiation Messaging and Presence Leveraging Enhancements) messages between end users
- Triggers on SIP Message and Subscribe messages
- Policy uses the provisioned end-user URLs to route SIP Subscribe and Message messages
- If the Request URI indicates that the message is for a URL provisioned in the Network Server, the policy redirects this message to the Hosting NE on which the URL is hosted
- If the URL is not known in the Network Server, the policy redirects the message to the SIMPLE proxy server capable of handling traffic for the domain specified in the URL



Media Server Selection

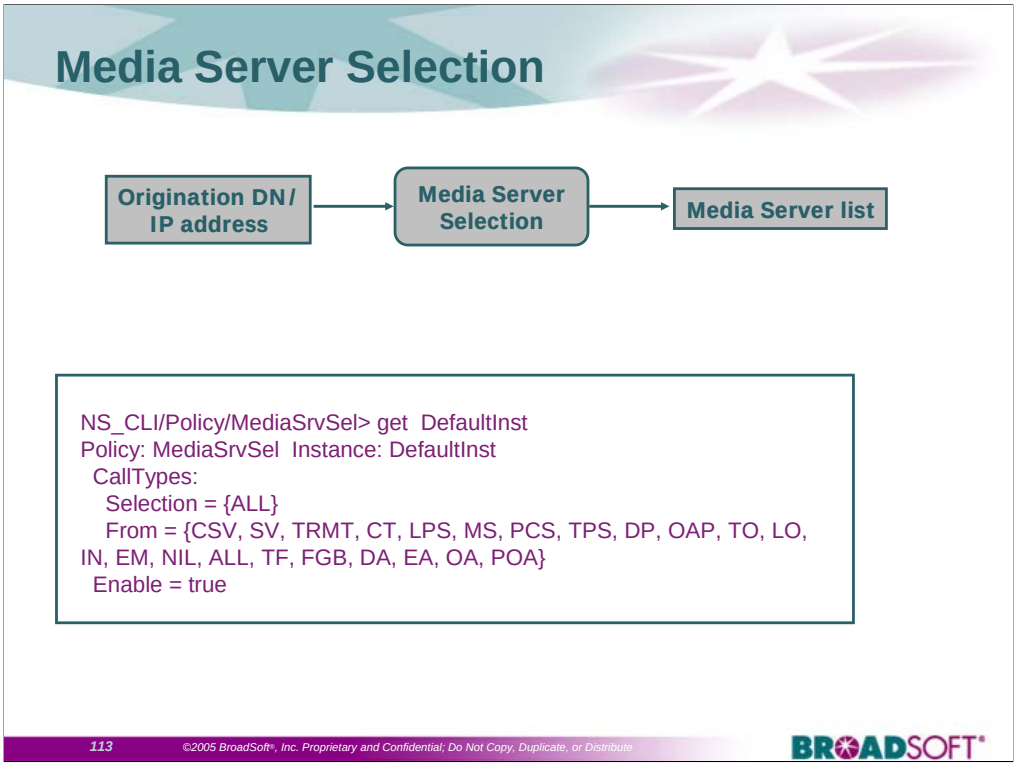
Uses proprietary the MSS protocol.

The Network Server receives an incoming MSS Request from an Application Server.

The Network Server processes an MSS Request by looking at the DN of the requestor or the IP address of the NE that requires a Media Server.

The Network Server returns an MSS Response message to the Application Server with list of Media Servers to try.

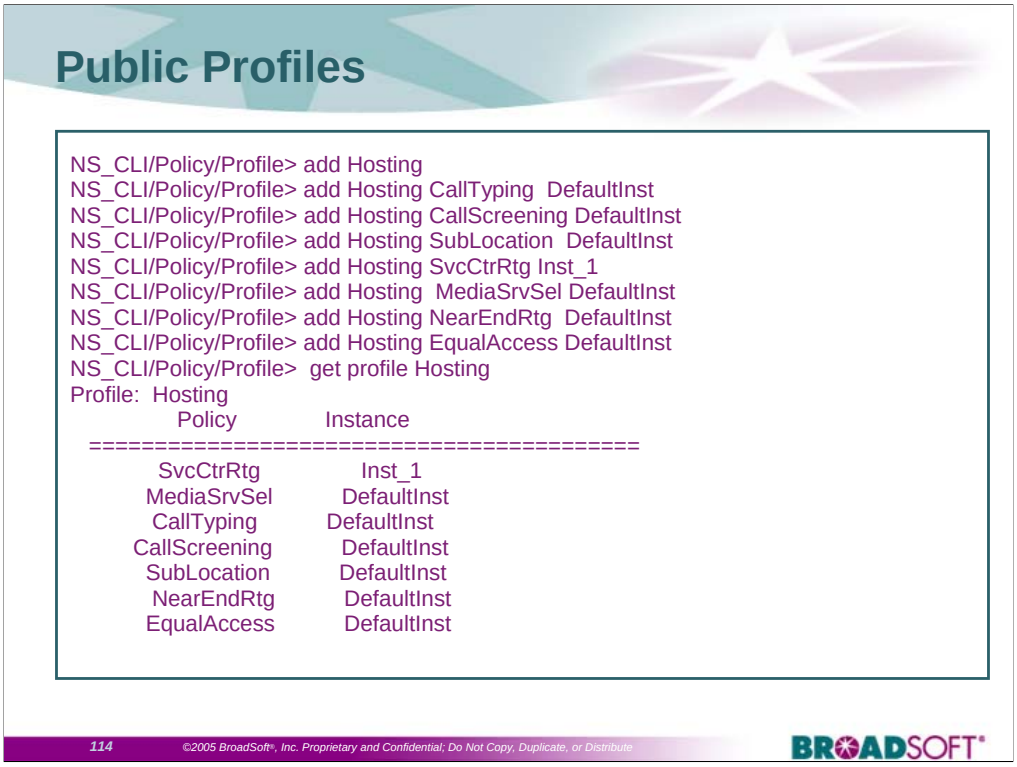
If the first Media Server does not respond, the Application Server tries the next Media Server in the returned list.



Media Server Selection Routing Policy

Locates the Media Server which is physically closest to a RoutingNE or to an end-user DN on an IP network.

This policy allows Media Servers to be decoupled from Application Servers so they do not have to be collocated; an operating company can locate Media Servers close to network gateways.



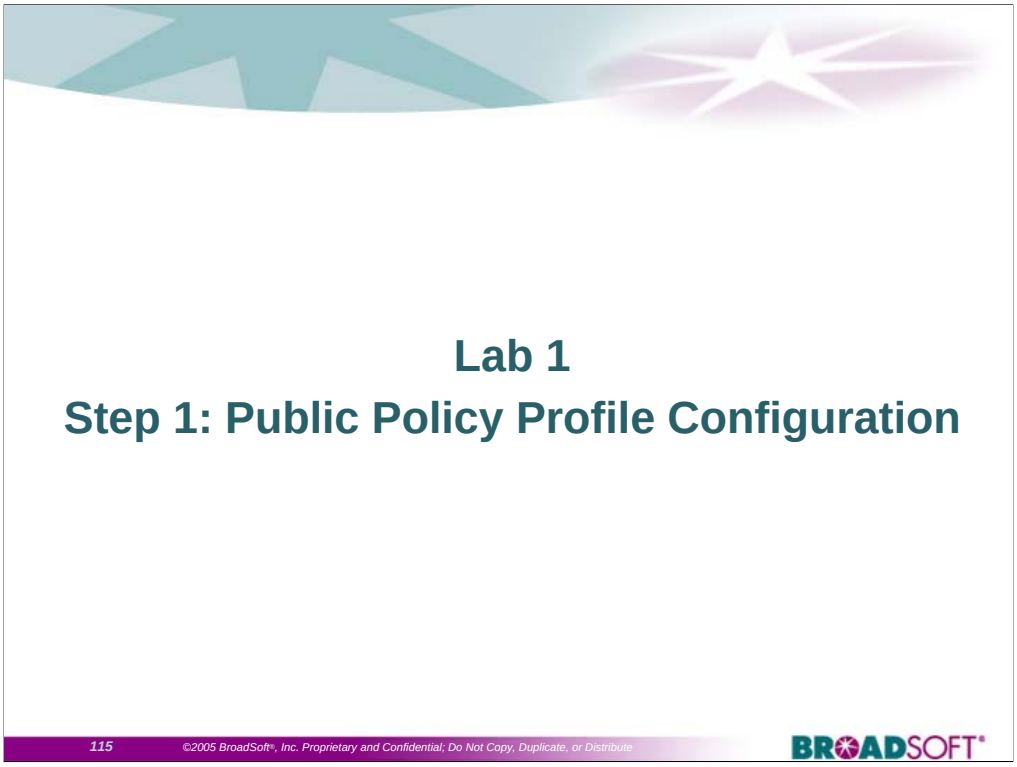
Public Profiles

Profiles can be assigned to network elements, enterprises, and groups.

Policy instances are grouped together in a profile to be assigned.

The add command and the following fields are used to add an instance:

profile	The name of the profile.
policy	The name of the new policy.
instance	The name of the profile policy instance.



Public Policy and Profile Creation

Public call routing is driven by public policies. Public policies are grouped into profiles and can be assigned to hosting network elements, routing network elements, enterprises, or groups.

Each team will create two public profiles (one associated with the enterprise and the associated with the RoutingNE).

For the enterprise profile:

– The CallTyping policy is used to set call types. CallScreening policy used to validate call types. MediaSrvSel policy used by the Network Server for Media Server selection.

– A combination of the FarEndRtg, NearEndRtg, and SvcCtrRtg policies, which are assigned to support the following routing.

- All calls from 240364xxxx users use a static route list of ngw1(NearEndRtg) with the exception of Teams 1,2,3 and 4 who set toll calls for all users to use ngw1 (FarEndRtg). Teams 5, 6, 7,8 and 9 set International calls for all users to use ngw1 (FarEndRtg).
- For all teams, 911 calls from 240364xxxx use a SCRL for each team's DUMMY<Team#> routingNE after prepending 99 to the dialed digits (SvcCtrRtg).
- For all teams, 411 calls from all users use ngw1 after 411 has been replaced by 18005551234 routing number to the preferred OA carrier (SvcCtrRtg).

For the RoutingNE profile:

– The CallTyping policy is used to set the call type.

– The SubLocation policy is used to allow incoming PSTN calls to terminate to hosted users.

– The MediaSrvSel policy is used by the Network Server for Media Server selection.

1. Log in to the Network Server as bwadmin.
2. Log in to the BroadWorks command line interface level as admin.
3. Teams 1, 2, 3, and 4, create the following team-specific policy instances under the corresponding NS_CLI/Policy level.
4. Teams 5, 6, 7, 8, and 9 create the following team-specific policy instances under the corresponding `NS_CLI/Policy` level.

Policy Name	Instance Name	Applicable Call Types
SvcCtrRtg	INST_<Team#>	EM, DA
FarEndRtg	INST_<Team#>	TO

5. Under `NS_CLI/Policy/FarEndRtg` level, ensure that location routing is disabled for your **FarEndRtg** policy instance.
6. Under `NS_CLI/Policy/Profile` level, each team creates a public profile called *HOST_<Team#>* and assigns the following policies and policy instances. Under `NS_CLI/Policy/Profile` level, each team creates a Routing NE public profile called *ROUTE_<Team#>* and assigns the following policies and policy instances.

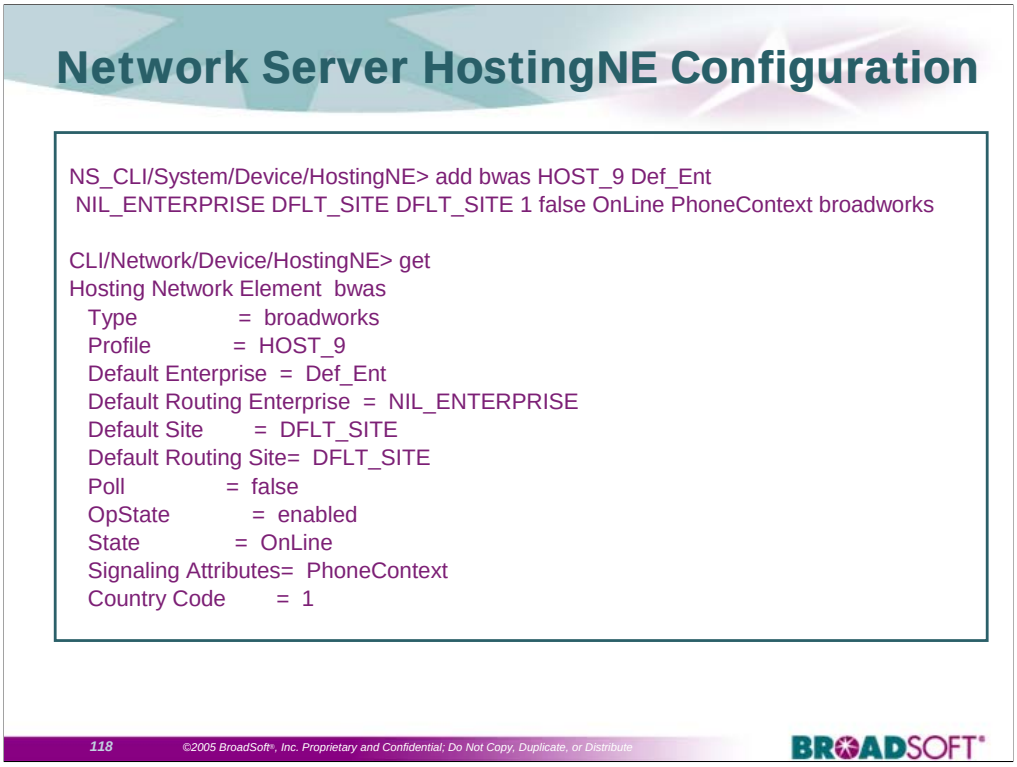
Policy Name	Instance Name	Applicable Call Types
SvcCtrRtg	INST_<Team#>	EM, DA
FarEndRtg	INST_<Team#>	IN

7. Under `NS_CLI/Policy/Profile` level, each team creates a Routing NE public profile called *ROUTE_<Team#>* and assigns the following policies and policy instances.

Policies	Policy Instance
CallTyping	DefaultInst
CallScreening	DefaultInst
MediaSrvSel	DefaultInst
NearEndRtg	DefaultInst
SvcCtrRtg	INST_<Team#>
FarEndRtg	INST_<Team#>

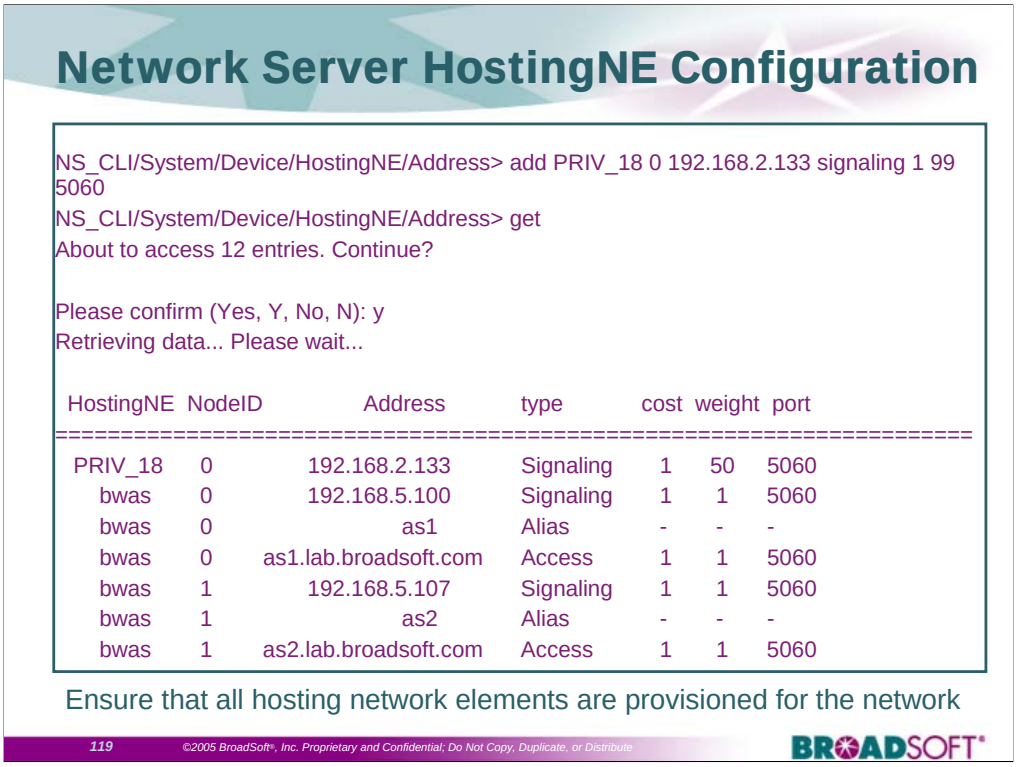
Build Network Elements

- Network Server must know the network element (NE) to route calls to and from the NE



The add command and the following fields are used to add a hosting network element:

hostNe	The network element name.
profile	The profile to be used for this hosting NE.
dfltEnterprise	Used to temporarily map a default enterprise name on the Network Server when user data is uploaded from the Application Server.
dfltRoutingEnterprise	Used to temporarily map a default routing enterprise name on the Network Server when user data is uploaded from the Application Server.
dfltSite	Used to temporarily map a default site on the Network Server when user data is uploaded from the Application Server.
dfltRoutingSite	Used to temporarily map a default routing site on the Network Server when user data is uploaded from the Application Server.
countryCode	The country code.
signaling	One of the following: NONE: No signaling defined. E164Compliant: The NE supports E.164. PhoneContext: The NE supports phone-context. Forking: The NE supports forking. CallTypeInfoRequired: The NE requires the call type info to be sent back as part of the 302 contacts returned by the NS. sourceId: The NE supports Originating Trunk Groups.
poll	True or false: Allows the Network Server to poll another device.
state	Offline or online: Sets the state of the device.
type	BroadWorks or other: Indicates the type of device.



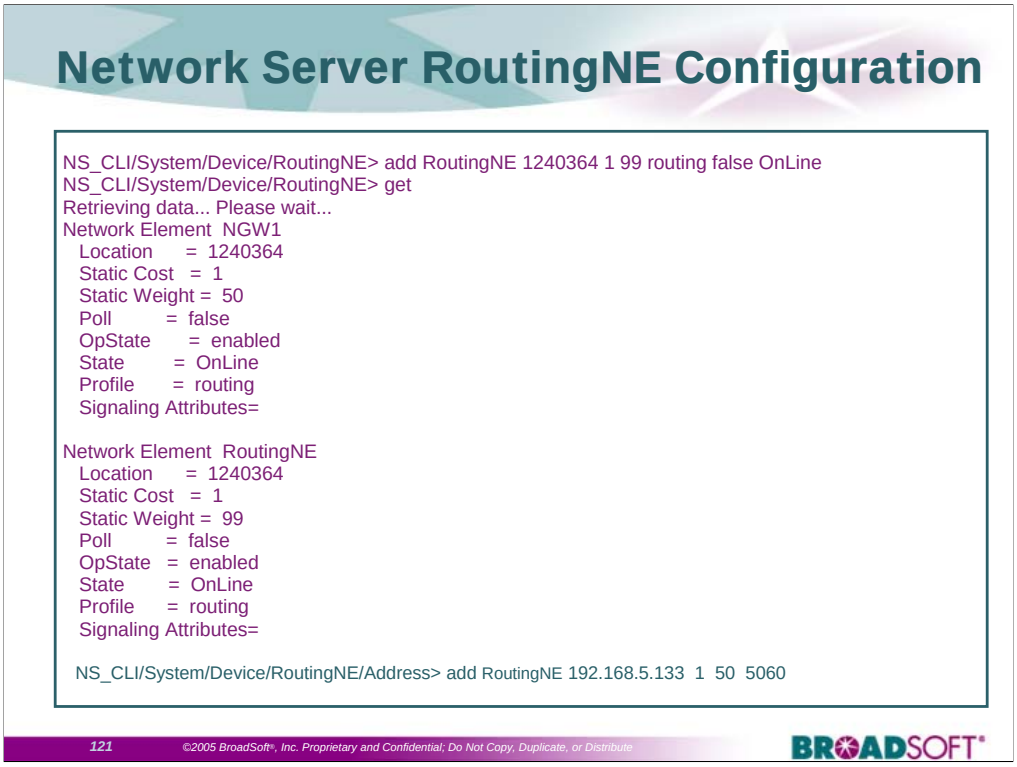
Once the network element is provisioned on the network it must have an address provisioned for it.

The add command and the following fields are used to add a network element:

hostNE	The name of the network element.
nodeID	Cluster member ID. Default is 0.
address	The corresponding IP address, or host name, or domain name for the network element.
type	One of the following: DualRouting: The address is a SIP signaling address. It can be added to the contact list from a returned 302 following a SIP request. Access: The address is a public address used for Location API. Signaling: This address is public and also a SIP signaling address at the same time. It will be returned for SIP and location API requests. Alias: Alias of hosting NE used for the Sync API.
cost	The associated cost code for the network element
weight	Given the same cost, network elements will be randomly listed according to weight with a higher weight appearing more often at the top.
port	The port number.

Network Server HostingNE Configuration

```
NS_CLI/System/Device/HostingNE/Node> add asqtsc 1 default false

NS_CLI/System/Device/HostingNE/Node> get
About to access 5 entries. Continue?

HostingNe  NodeID          default          description
============================================================
   PRIV_1     0            true        Node 0 (automatically added)
   PRIV_3     0            true        Node 0 (automatically added)
   PRIV_2     0            true        Node 0 (automatically added)
   asqtsc     0            true        Node 0 (automatically added)
   asqtsc     1            false
```



The add command and the following fields are used go add a routing network element:

ne	The network element name.
location	The physical location of the network element in the network.
cost	The associated cost code for the network element.
weight	Given the same cost, network elements will be randomly listed according to the weight with a higher weight appearing more often at the top.
profile	The profile to be used for this routing network element having precedence over the system profile.
poll	True: Allows the Network Server to poll another device.
	False: Polling is turned off.
state	Offline: When set to offline, no calls are routed to this NE
	Online: When set to online, calls will be routed to this NE.
signaling	One of the following:
	NONE: No signaling defined.
	E164Compliant: The target device supports E.164 encoded information.
	PhoneContext: The target device supports phone-context.
	Forking: Target device supports forking.
	InboundOnly: The device is only used for sending calls in the in bound directory.
	UseOrigBasedScreening: Use the call category from call screening (Caller to Called number) instead of the call category from the RoutingNE to the called number.

Network Server ResourceNE Configuration

```
NS_CLI/System/Device/ResourceNE> add ms1 ms all 1240364 1 99 false Online default 1 99
NS_CLI/System/Device/ResourceNE> add ms2 ms all 1301977 1 99 false Online

NS_CLI/System/Device/ResourceNE> get

 Resource Type  Location  Stat   Stat     Poll  OpState  State    Dflt  Dflt   Dflt Services
 NE                       Cost   Weight                             Cost Weight
 MS1      ms    1240364   2      50       false enabled  OnLine   true  1      99     all
 MS2      ms    1240364   2      50       false enabled  OnLine   false -      -      all


NS_CLI/System/Device/ResourceNE/Address> add ms1 192.168.5.180 1 99 5060
NS_CLI/System/Device/ResourceNE/Address> add ms2 192.168.5.185 1 99 5060
```


The add command and the following fields are used to add a new resource network element:

neName	The resource network element name.
neType	ms: The device is a Media Server.
	SIMPLE: The device is a SIMPLE-based messaging server.
location	The physical location of the resource network element in the network.
staticCost	The static cost for the resource network element used in the post-processing for a V&H lookup.
staticWeight	The static weight for the resource network element used in the post-processing for a V&H lookup.
poll	True or false: Allows the Network Server to poll another device.
state	OffLine: The resource network element is off line and not available.
	OnLine: The resource network element is on line and is available.
default	defaultCost: The default cost used in the post-processing of the default resource network element list.
	defaultWeight: The default weight used in the post-processing of the default resource network element list.

To add network element address attributes, enter: add neName, address, cost, weight, port.

neName	The name of the resource network element.
address	The corresponding IP address, or host name, or domain for the resource NE.
cost	The associated cost code for the resource network element.
weight	The weight assigned to the
port	The resource network element port number.

Network Server ResourceNE Configuration

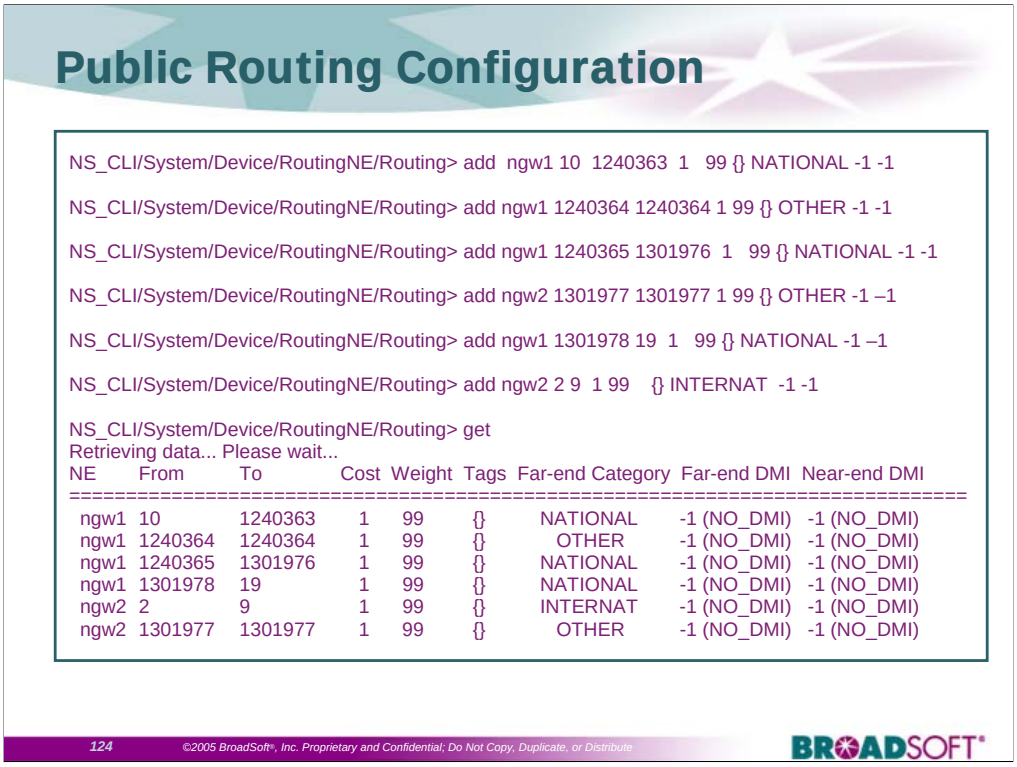
```
NS_CLI/Policy/MediaSrvSel/RouteList> add DefaultInst ms1 1240364 1240364 all 1 50
NS_CLI/Policy/MediaSrvSel/RouteList> add DefaultInst ms2 1240364 1240364 all 2 50
NS_CLI/Policy/MediaSrvSel/RouteList> add DefaultInst ms2 1301977 1301977 all 1 50
NS_CLI/Policy/MediaSrvSel/RouteList> add DefaultInst ms1 1301977 1301977 all 2 50

NS_CLI/Policy/MediaSrvSel/RouteList> get DefaultInst
Policy: MediaSrvSel  Instance: DefaultInst  Table: RouteList
  mss     from          to       service  cost  weight
==============================================
  MS1  1240364  1240364   {all}       1     50
  MS2  1240364  1240364   {all}       2     50


NS_CLI/System/Device/ResourceNE/MSSelect> add ms1 ngw1 all 1 50
NS_CLI/System/Device/ResourceNE/MSSelect> add ms2 ngw1 all 2 50
```


The add command and the following fields are used to add a new routing list:

instance	The name of the instance for this policy.
ms	The name of the Media Server to which this instance applies.
from/to	Digit sequence defining the beginning/end of a range of digits.
service	One of the following: ivr: This is interactive voice response. conf: This is a conference repeater. fax: This is a fax. liveAudio: This is a live audio source. all: The routing entry applies to all possible media services.
cost	The associated cost code for the route.
weight	The relative value (user defined) to randomize distribution of traffic along this route.

The add command and the following fields are used to add a new Media Server network element:

ms	The Media Server name.
routingNE	The name of the routing network element.
service	*See service description listed above.*
cost	The associated cost code for the Media Server.
weight	Given the same cost, Media Servers are randomly listed according to the weight with a higher weight appearing more often at the top.

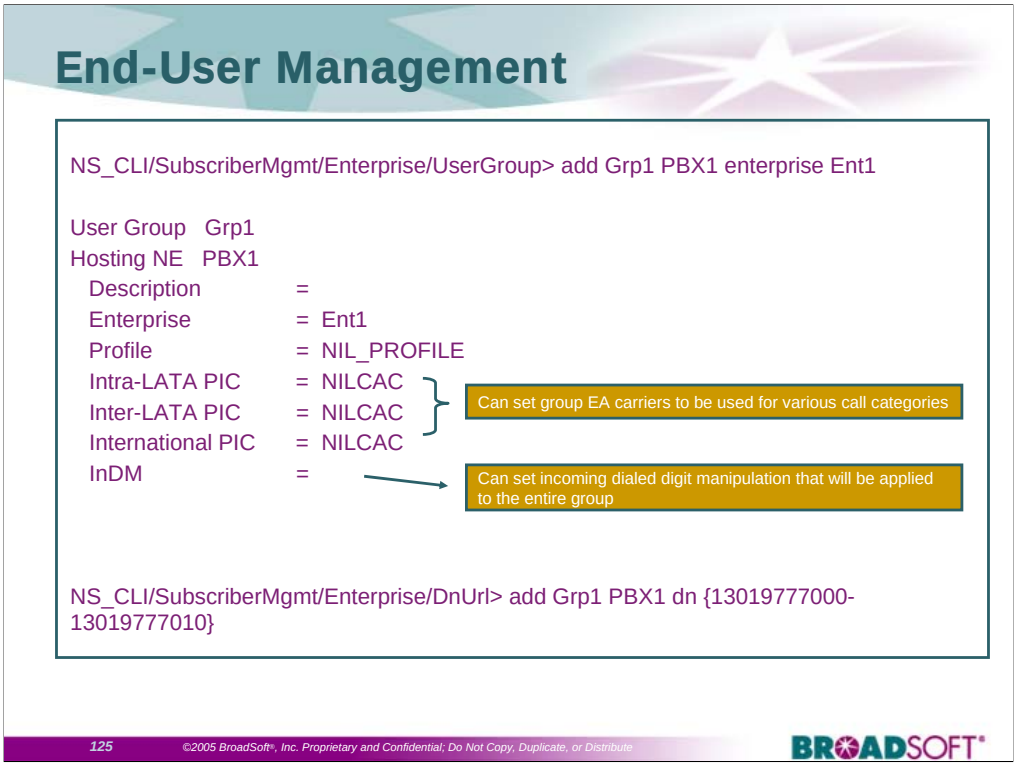


The add command and the following fields are used to add a network element route:

neString	The network element name.
from	The starting phone number of the range.
to	The ending phone number of the range.
cost	The associated cost code for the phone number range.
weight	The relative value to randomize distribution of traffic.
tag	*For future use*.
farendCategory	One of the following:

LOCAL	This allows a route to be flagged as local.
NATIONAL	This allows a route to be flagged as national.
INTERLAT	This allows a route to be flagged as inter-LATA.
INTRALAT	This allows a route to be flagged as intra-LATA.
INTERNAT	This allows a route to be flagged as international.
PRIVATE	This allows a route to be flagged as private.
OTHER	This allows a route to be flagged as other.
EMERGENCY	This allows a route to be flagged as emergency.

farendDMI	The digit manipulation index allowing digit manipulation on the routing entry.
nearendDMI	The digit manipulation index allowing digit manipulation on the routing entry.

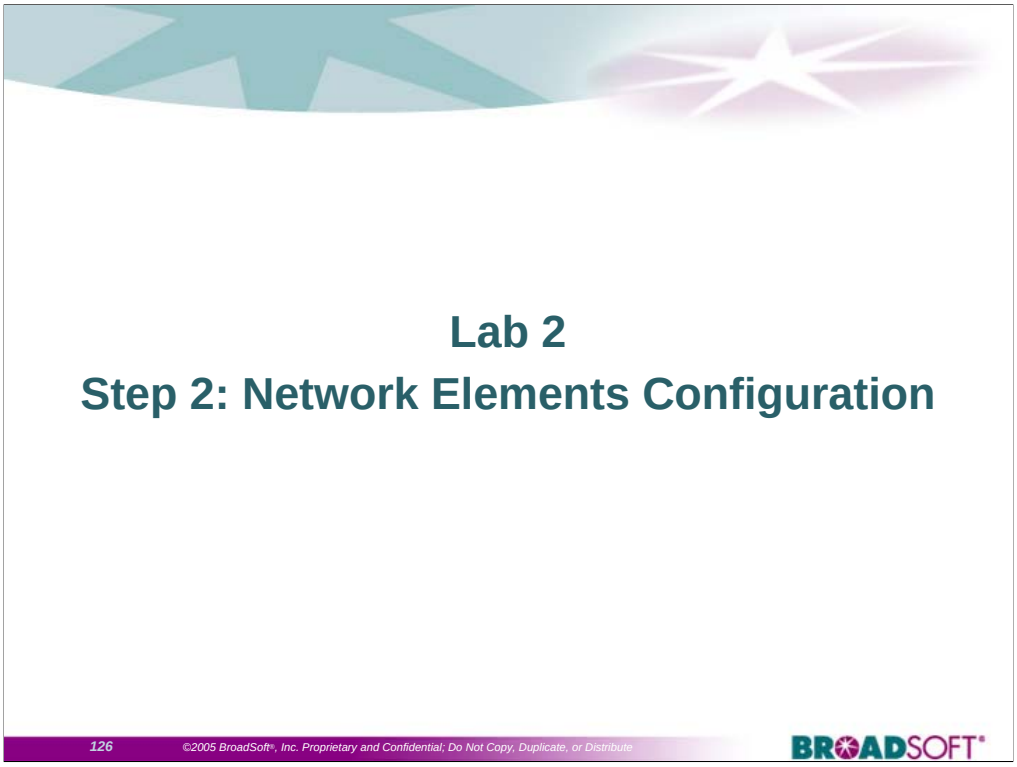


The add command and the following fields are used to add a group.

groupId		The ID of the user group.
hostNE		The network element hosting the user group.
attribute	enterprise	The enterprise to which the user group belongs.
	groupName	The name of the user group.
	profile	The routing profile to be used by the user group.
	lcaid	The LCA name.
	intraPic	The carrier to be used for intra-LATA calls.
	interPic	The carrier to be used for inter-LATA calls.
	intlPic	The carrier to be used for international calls.
	InDM	The digit manipulation algorithm for incoming calls to the user group.
	sourceId	The originating trunk group (OTG). This is another means of identifying an enterprise, user group or site in the system. The same sourceID can be used to identify many enterprises, groups, or sites.

The add command and the following fields are used to add directory numbers:

group		The name of the user group.
hostNE		The network element hosting the group.
address	dn	The site where these numbers are used and DNs belonging to this user group site.
	ext	The site where these extensions are used and the extensions belonging to this user group site.
	url	The site where these URLs are used and the URLs belonging to this user group site.



Step 2: Create Network Elements

The Network Server has a network topology view of the entire BroadWorks network. There are three categories of NEs: Resource NE, Routing NE, and Hosting NE.

Media Servers

MS0 has been added and configured as the default Media Server by your instructor. Each team will add a dummy Media Server that will be returned as part of the Media Server Selection return contact list.

1. Under NS_CLI/System/Device/ResourceNE, each team creates a Media Server resource with the following parameters:

Team	MS Name	IP Address	Location	Polling	Static Cost	Weight
Team 1	DUMMYMS1	192.168.7.103	1240364	false	2	50
Team 2	DUMMYMS2	192.168.7.104	1240364	false	2	50
Team 3	DUMMYMS3	192.168.7.105	1240364	false	3	99
Team 4	DUMMYMS4	192.168.7.106	1240364	false	3	1
Team 5	DUMMYMS5	192.168.7.107	1240364	false	4	50
Team 6	DUMMYMS6	192.168.7.108	1240364	false	4	50
Team 7	DUMMYMS7	192.168.7.109	1240364	false	5	50
Team 8	DUMMYMS8	192.168.7.110	1240364	false	6	50
Team 9	DUMMYMS9	192.168.7.111	1240364	false	7	50

Routing Network Elements

NGW1 has been added by the instructor and has PSTN connectivity. Each team will add a dummy Routing NE that will be returned in the contact list depending on the dial plan.

– For all teams, 911 calls from 240364xxxx use a SCRL for each team's DUMMY<Team#> routingNE after prepending 99 to the dialed digits (SvcCtrRtg).

1. Under NS_CLI/System/Device/RoutingNE, each team creates a network gateway resource with the following parameters:

Team	NGW Name	IP Address	Location	Profile	Static Cost	Weight	Polling	Status
Team 1	DUMMY1	192.168.7.121	1240364	ROUTE_1	1	50	false	Online
Team 2	DUMMY2	192.168.7.122	1240364	ROUTE_2	1	50	false	Online
Team 3	DUMMY3	192.168.7.123	1240364	ROUTE_3	1	50	false	Online
Team 4	DUMMY4	192.168.7.124	1240364	ROUTE_4	1	50	false	Online
Team 5	DUMMY5	192.168.7.125	1240364	ROUTE_5	1	50	false	Online
Team 6	DUMMY6	192.168.7.126	1240364	ROUTE_6	1	50	false	Online
Team 7	DUMMY7	192.168.7.127	1240364	ROUTE_7	1	50	false	Online
Team 8	DUMMY8	192.168.7.128	1240364	ROUTE_8	1	50	false	Online
Team 9	DUMMY9	192.168.7.129	1240364	ROUTE_9	1	50	false	Online

Private Network Gateways

Private network gateways are used by private policies, such as FarEndHopOff, to route calls to a customer-owned CPE gateway. Private network gateways are defined as Hosting NEs on the Network Server.

– FarEndHopOff to support routing calls to the 514 NPA through private gateway (PRIV_1 to PRIV_9)

1. Under NS_CLI/System/Device/HostingNE, each team creates a private network gateway resource with the parameters shown in the following table. Each gateway overlays on the same IP address (using the same IP address as NGW1).

Team	NGW Name	IP Address	Profile	Polling	Status	Type	CC	Default Enterprise/ Routing	Default Site/ Routing
Team 1	PRIV_1	192.168.2.133	HOST_1	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 2	PRIV_2	192.168.2.133	HOST_2	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 3	PRIV_3	192.168.2.133	HOST_3	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 4	PRIV_4	192.168.2.133	HOST_4	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 5	PRIV_5	192.168.2.133	HOST_5	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 6	PRIV_6	192.168.2.133	HOST_6	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 7	PRIV_7	192.168.2.133	HOST_7	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 8	PRIV_8	192.168.2.133	HOST_8	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE
Team 9	PRIV_9	192.168.2.133	HOST_9	false	Online	other	1	NIL_ENTERPRISE	DFLT_ SITE

Create Enterprise

- Enterprises must be created to associate subscribers and groups to routing profiles

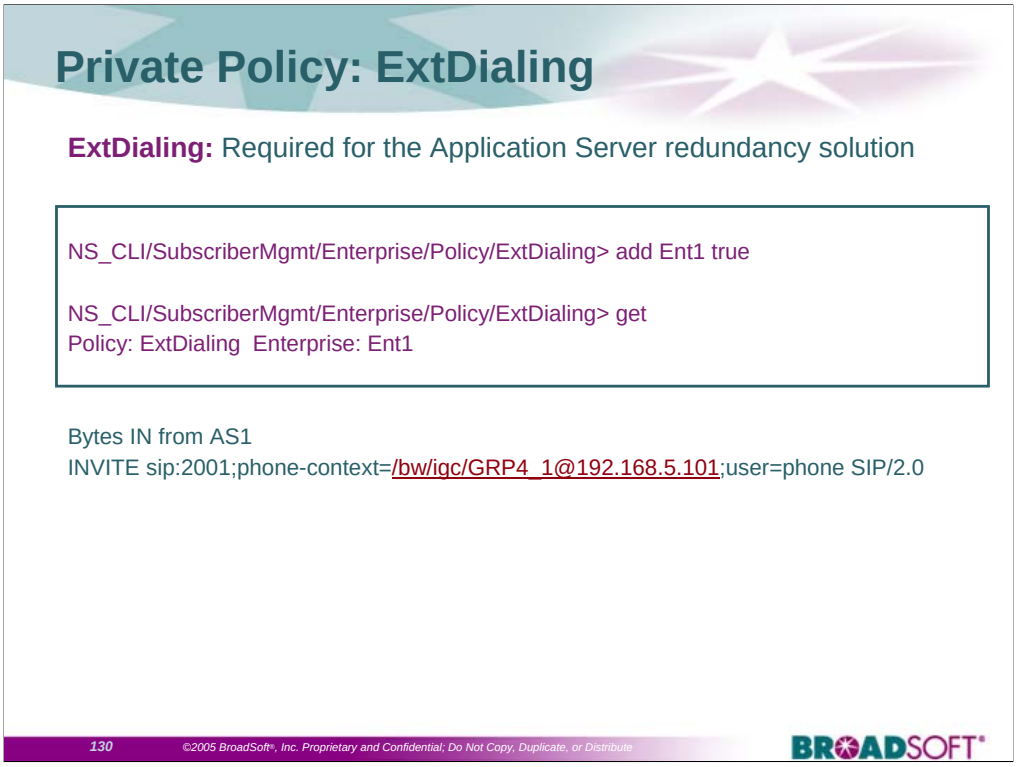
Enterprise Private Policy Configuration

```
NS_CLI/SubscriberMgmt/Enterprise> add Ent1 profile Hosting
NS_CLI/SubscriberMgmt/Enterprise> get
Enterprise  Ent1
  Call Logging       = Disabled
  Description        =
  Intra-LATA PIC     = NILCAC
  Inter-LATA PIC     = NILCAC
  International PIC  = NILCAC
  Routing profile    = Hosting
  Private policies   = {}
```

Can set enterprise EA carriers to be used for various call categories

The add command and the following fields are used to add an enterprise:

enterprise	The name of the new enterprise.		
attribute	intraPic	The carrier to be used for intra-LATA calls.	
	interPic	The carrier to be used for inter-LATA calls.	
	intlPic	The carrier to be used for international calls.	
	profile	The routing profile for this enterprise.	
	lcaid	The LCA name.	
	desc	Descriptive information about the enterprise.	
	callLog	disabled	Call logging is turned off.
		enabled	Call logging feature is on.
	sourceId	The originating trunk group (OTG).	



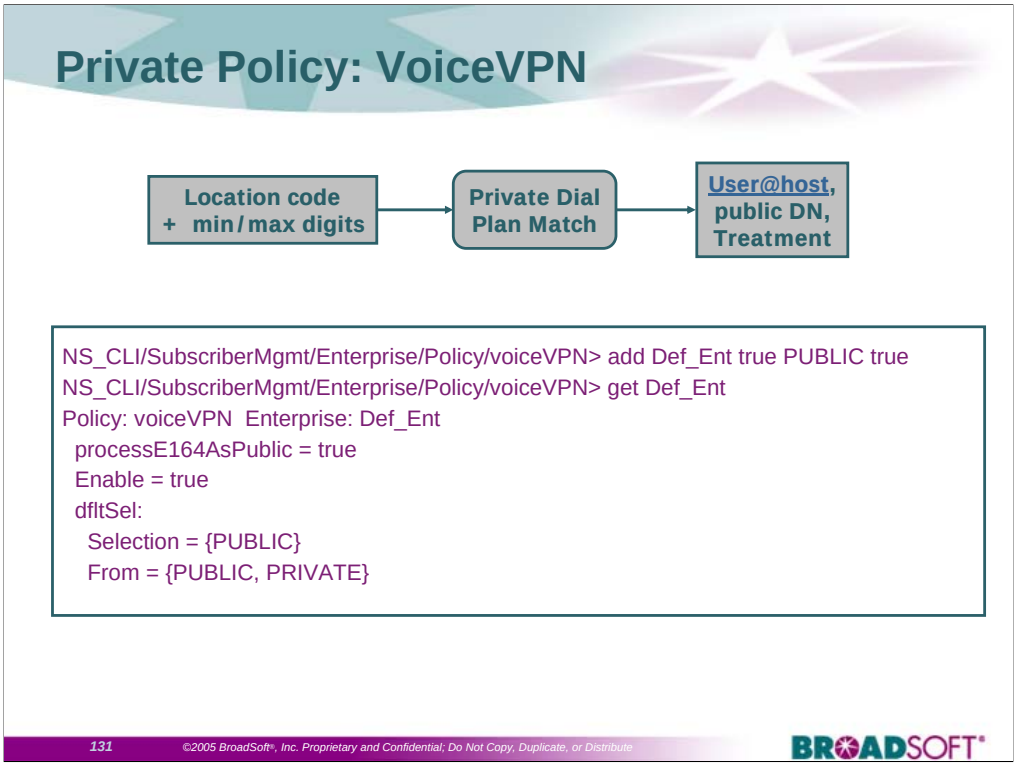
Private Extension Dialing Policy

Provides support for intra-group extension dialing for the Application Server redundancy solution.

Uses a proprietary extension to the SIP phone-context to exchange intra-group calls between Application Servers.

The add command and the following fields are used to add an instance of the policy:

enterprise		The enterprise name.
Enable	false	The instance is not active (off).
	true	The instance is active (on).



The add command and the following fields are used to add a policy instance:

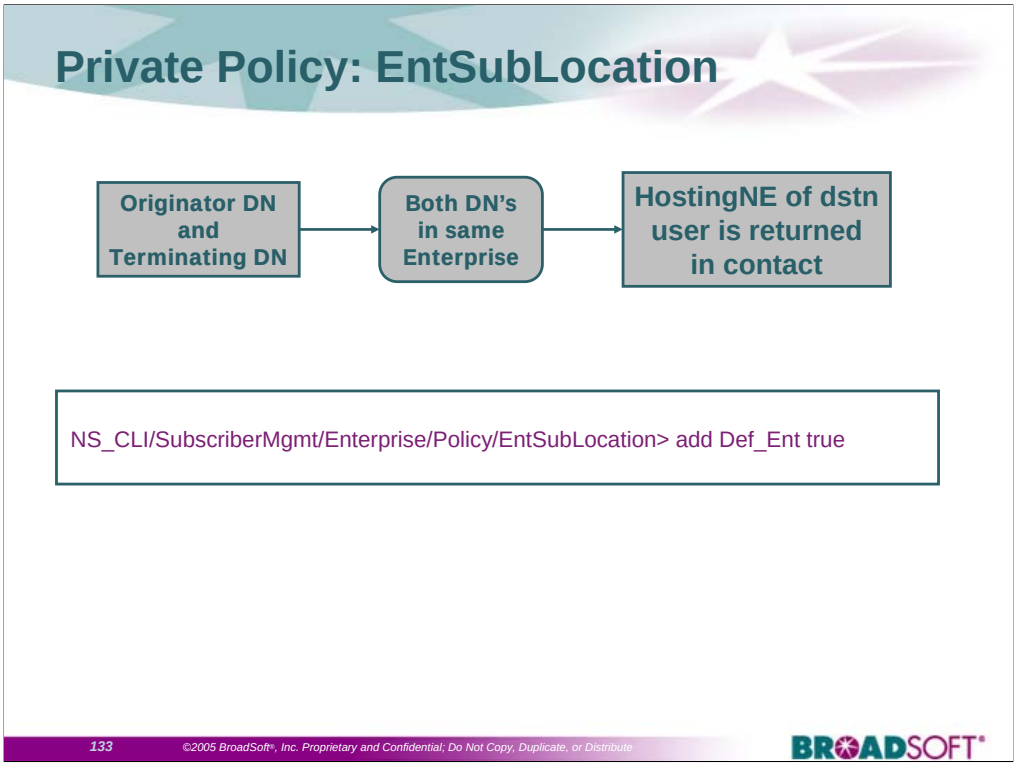
enterprise	The enterprise name.	
Enable	false	The instance is not active (off).
	true	The instance is active (on).

The add command and the following fields are used to a dial plan:

enterprise	The enterprise name.	
locCode	The code for the site location.	
extMin	The minimum number of digits for an extension.	
extMax	The maximum number of digits for an extension.	
selector	PRIVATE	Use only private policies to process calls.
	PUBLIC	Continue through all available policies starting with private policies first, then public ones.
	ROUTE	Route calls with redirect.
	TRMT	Treat calls using the corresponding treatment (trmtID).
attribute	dm	The digit manipulation string.
	hostId	The hosting network element. (Can only be changed when the selector is ROUTE and is mandatory.)
	grpId	The group ID. (Can only be changed when the selector is ROUTE and is mandatory.)
	trmtId	Dynamically generated: tmpun, bdreq, or frbdn. The error code of the treatment to be used.
	desc	The description of the dial plan entry. Use “ ” to enclose text.

Private Policy: VoiceVPN Dial Plan

```
NS_CLI/SubscriberMgmt/Enterprise/Policy/voiceVPN/DialPlan>
add Ent1 2 3 3 route hostId IHApp grpId Grp3 desc "4 digit extn to grp2“

 locCode extMin  extMax  selector    dm  hostId  grpId  trmtId        desc
 ========================================================================
 2         3         3         {ROUTE}       IHApp   Grp3        {}       4 digit extn to grp3
 4         3         3         {ROUTE}       IHApp   Grp2        {}       4 digit extn to grp2
 411       0         0         {PUBLIC}                          {}
 7         3         3         {PUBLIC}    INS(301977)           {}       4 digit extn to grp1
 9         7         20        {PUBLIC}    DEL(1)                {}
 911       0         0         {PUBLIC}                          {}
```



Enterprise Subscriber Location Routing Policy

Performs intra-enterprise subscriber location routing (that is, on-net dialing).

Routes calls within the same enterprise using the hosting network element as the destination.

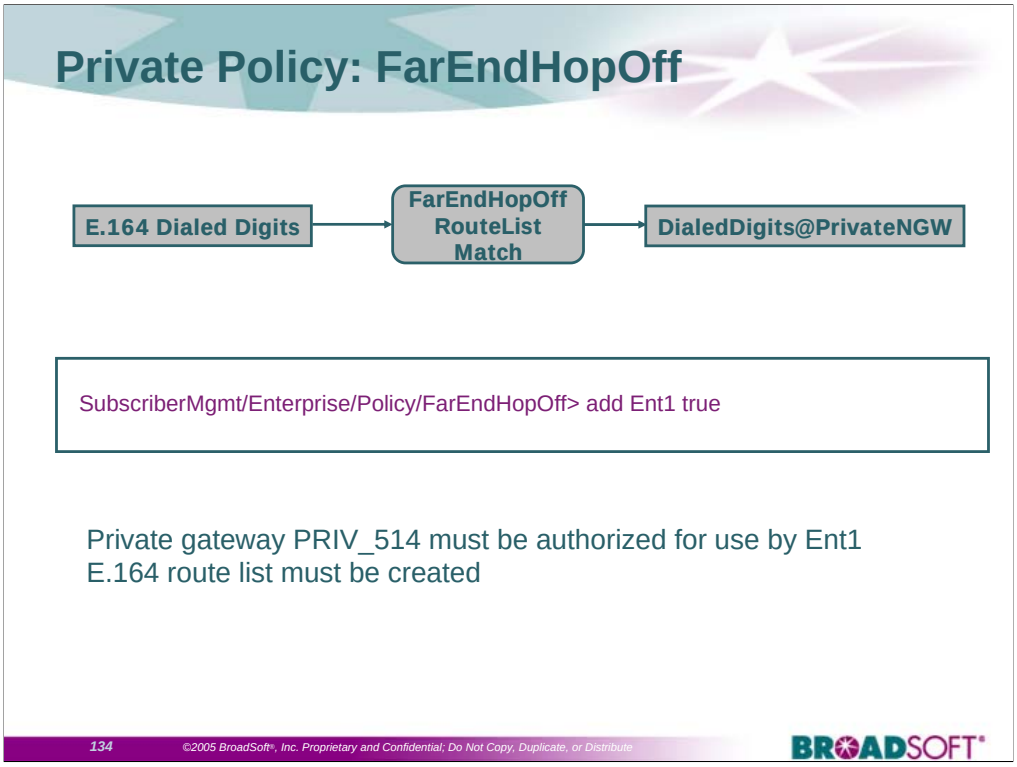
Bypasses public translations when both the call originator and destination are in user groups part of the same enterprise.

Using the enterprise of the caller, this policy searches through the DNs and URLs defined for the enterprise (in its user groups) and tries to find a match with the called DN or URL.

If a match is found, the HostingNE of the destination user is returned in the contact list.

The add command and the following fields are used to add a policy instance:

enterprise	The enterprise name.	
Enable	false	The instance is not active (off).
	true	The instance is active (on).



Far-End Hop-Off Routing Policy

Allows an enterprise to route public calls through private gateways using their own facilities.

Private gateways are defined as HostingNEs and then authorized for use by a specific enterprise.

An enterprise can use their own facilities to perform “toll bypass” based on the E.164 representation of the dialed digits.

For example, company with offices in the US and UK wants all UK traffic (country code 44) to be sent on-net to a private NGW located in the UK. All other PSTN calls will use public routing.

Digit manipulation operations can be performed on the dialed digits.

If a permissive Voice VPN dial plan is enabled, routing will continue to public policies and append PSTN routes.

The add command and the following fields are used to add a policy instance:

enterprise		The enterprise name.
Enable	false	The instance is not active (off).
	true	The instance is active (on).

FarEndHopOff Private Policy Configuration

Authorize Ent1 to use the Priv_514 gateway

```
NS_CLI/SubscriberMgmt/Enterprise/Policy/FarEndHopOff/AuthHost>
add Ent1 PRIV_514
```

Add E164 route list

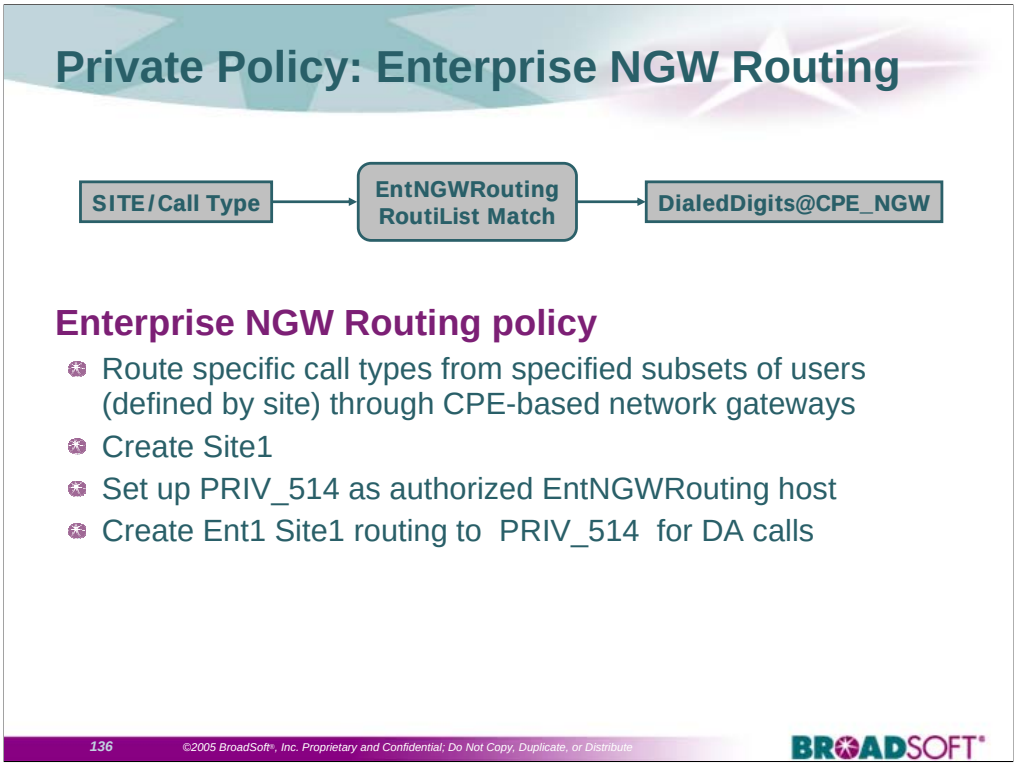
```
NS_CLI/SubscriberMgmt/Enterprise/Policy/FarEndHopOff/RoutingList>
add Ent1 PRIV_514 1514 1514 OutDM "del(1)"
```


The add command and the following fields are used to authorize an enterprise to use a gateway:

enterprise	The enterprise name.
AuthHost	The network element name.

The add command and the following fields are used to add a routing list:

enterprise		The enterprise name.
AuthHost		The network element name of a pre-authorized host.
From		Digit sequence defining the beginning of a range of digits.
To		Digit sequence defining the end of a range of digits.
attribute	OutDM	The digit manipulation algorithm to be applied against the requested digits.



Enterprise NGW Routing Policy

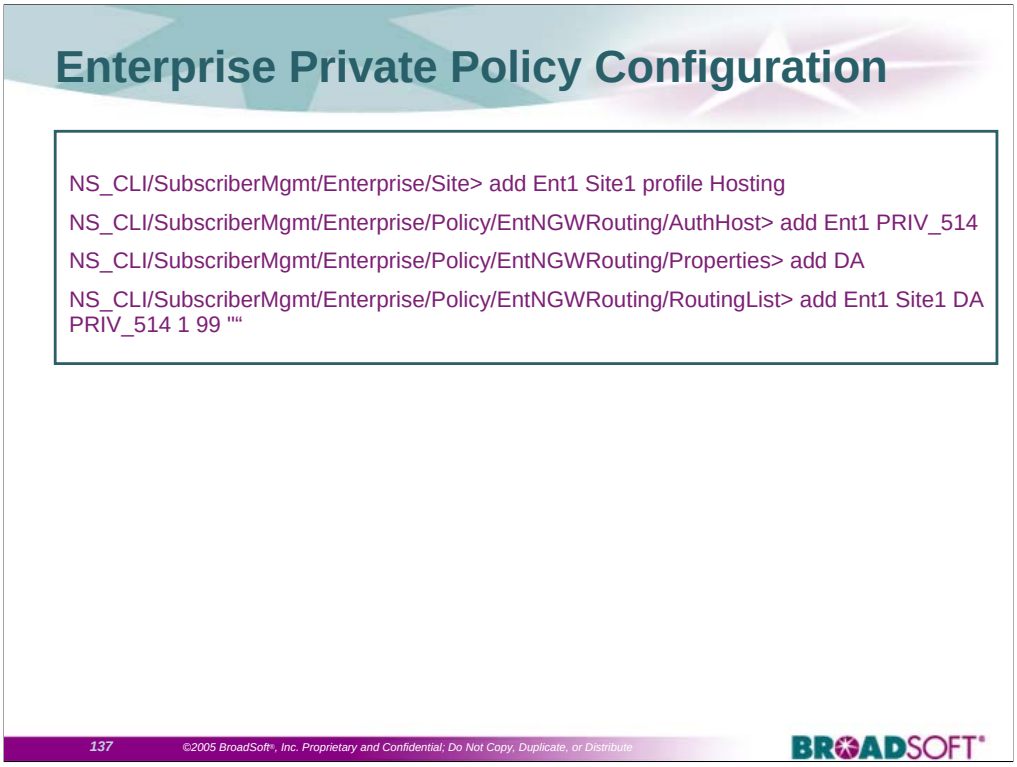
Route specific call types from specified subsets of users (defined by site) through CPE-based network gateways.

Users are associated with a site.

CPE gateways are defined as HostingNEs and then authorized for use by a specific site.

NGW Routing policy allows for routing specific call types through the CPE gateways, while other call types continue to use public routing policies.

Digit manipulation operations can be performed on the dialed digits.



The add command and the following fields are used to authorize an enterprise to use a specific gateway:

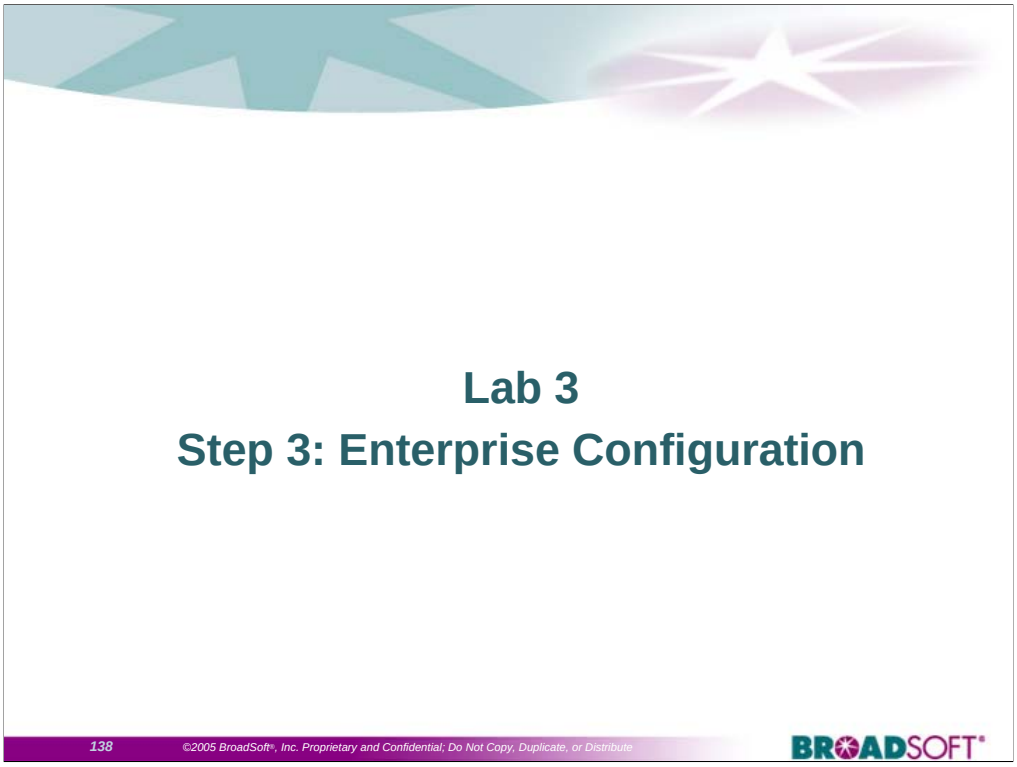
enterprise	The enterprise name.
authHost	The network element name.

The add command and the following fields are used to add call types:

callType	The type of call.
desc	Description of the new call type property.

The add command and the following fields are used to add a routing list:

enterprise	The enterprise name.
site	The enterprise site name.
callType	The type of call.
authHost	The network element name of a pre-authorized host.
cost	The associated cost code for the gateway.
weight	The relative value to randomize distribution of traffic along this route.
outDM	The digit manipulation algorithm to be applied against the requested digits.



Enterprise Creation and Private Policy Association

Network Server enterprises allow private policies to be shared by groups. Groups can be assigned to different enterprises and have unique private dial plans.

Each team's enterprise will have the following private policies:

– ExtDialing assigned to support redundancyVoiceVPN, which supports the following private dial plan:
  - 5XXX/9XXX extension dialing between 240364xxxx users in groups belonging to the enterprise
  - 01144 international calls will be blocked
– FarEndHopOff to support routing calls to the 514 NPA through private gateway (PRIV_1 to PRIV_9)
– EntSubLocation to support on-net calling between users in the same enterprise

Enterprise Creation

1. Under NS_CLI/SubscriberMgmt/Enterprise, using the add command, each team creates an enterprise with the following parameters:

Team	Enterprise Name	Public Profile	Call Logging	EA PICs
Team 1	ENT_1	HOST_1	Disabled	NILCAC
Team 2	ENT_2	HOST_2	Disabled	NILCAC
Team 3	ENT_3	HOST_3	Disabled	NILCAC
Team 4	ENT_4	HOST_4	Disabled	NILCAC
Team 5	ENT_5	HOST_5	Disabled	NILCAC
Team 6	ENT_6	HOST_6	Disabled	NILCAC
Team 7	ENT_7	HOST_7	Disabled	NILCAC
Team 8	ENT_8	HOST_8	Disabled	NILCAC
Team 9	ENT_9	HOST_9	Disabled	NILCAC

Private Policy Association

1. Under the corresponding NS_CLI/SubscriberMgmt/Enterprise/Policy level, each team associates EntSubLocation, voiceVPN (dfltSel is set to “PUBLIC” and processE164AsPublic is set to “true”), FarEndHopOff, and ExtDialing private policies to their enterprise.
2. Example: NS_CLI/SubscriberMgmt/Enterprise/Policy/ExtDialing> add ENT_# true

FarEndHopOff Configuration

1. Under the NS_CLI/SubscriberMgmt/Enterprise/Policy/ FarEndHopOff/ AuthHost level, each team adds their PRIV_<Team#> private NGW as a valid host for their enterprise.
2. Example: NS_CLI/SubscriberMgmt/Enterprise/Policy/FarEndHopOff/AuthHost> add ENT_# PRIV_#
3. Under the NS_CLI/SubscriberMgmt/Enterprise/Policy/ FarEndHopOff/ RoutingList level, each team creates a route list entry to return their PRIV_<Team#> gateway in the contact list for calls to the 514 area code.

(NOTE: The “From/To range” is E.164-based.)

4. Example:

   NS_CLI/SubscriberMgmt/Enterprise/Policy/FarEndHopOff/ RoutingList add ENT_2 PRIV_3 1514 1514 OutDM DEL(1)

VoiceVPN Configuration

1. Under the NS_CLI/SubscriberMgmt/Enterprise/Policy/voiceVPN/ DialPlan level, each team creates the enterprise dial plan to match the private dial plan described in section 2.1.1.1.1 Private Policies. Use the following table:

LocCode	ExtMin	ExtMax	Selector	DM	HostId	GrpId	TRMT
5	3	3	Private	INS(240364)	-	-	-
91	2	2	Public	INS(240364)			
92	2	2	Private	INS(240364)			
01144	8	8	trmt	-	-	-	frbdn

Public Static Route List Creation

1. The Network Server supports both dynamic public route selection (through location routing and the NNACL file) and static public routes. The FarEndRtg, NearEndRtg policies share a common system-wide route list. The SvcCtrRtg policy is used to apply instance-specific route lists to a call.

Near-End and Far-End Static Routing

1. All calls from 240364xxxx users use a static route list of ngw1(NearEndRtg) with the exception of Teams 1,2,3 and 4 who set toll calls for all users to use ngw1 (FarEndRtg). Teams 5, 6, 7,8 and 9 set International calls for all users to use ngw1 (FarEndRtg).
2. Under NS_CLI/System/Device/RoutingNE/Routing, add the following far-end routing static routes. Enter the tags {} and cost and weight of 1 and 99. Your instructor added the default near-end routing route for all calls from 1240364 users.

TEAM	NE	FROM	TO	farendCategory	farendDMIs	nearendDMI
TEAM 1	NGW1	1978	1978	NATIONAL	-1	-1
TEAM 2	NGW1	1201	1201	NATIONAL	-1	-1
TEAM 3	NGW1	1212	1212	NATIONAL	-1	-1
TEAM 4	NGW1	1202	1202	NATIONAL	-1	-1
TEAM 5	NGW1	1819	1819	NATIONAL	-1	-1
TEAM 6	NGW1	1613	1613	LOCAL	-1	-1
TEAM 7	NGW1	1514	1514	LOCAL	-1	-1
TEAM 8	NGW1	2	9	INTERNATIONAL	-1	-1
TEAM 9	NGW1	1301	1301	NATIONAL	-1	-1

Service Center Routing Static Route List

– For all teams, 911 calls from 240364xxxx use a SCRL for each team's DUMMY<Team#> routingNE after prepending 99 to the dialed digits (SvcCtrRtg).

– For all teams, 411 calls from all users use ngw1 after 411 has been replaced by 18005551234 routing number to the preferred OA carrier (SvcCtrRtg).

1. Under the NS NS_CLI/System/CallP/DMI level, each team creates a DMI entry to "prepend" 99 to the dialed digits (each team should use their team number as the DM index number).
2. Under the NS_CLI/Policy/SvcCtrRtg/SCRL level, each team creates the following SCRL entries for their team's SvcCtrRtg instance to support the public dial plan.

CallType	FROM	TO	callSelector	Address	RoutingNE	DMI
EM	1240364	1240364	ALL	-	DUMMY<Team#>	<Team#>
DA	1240364	1240364	ALL	18005551234	-	-

Questions