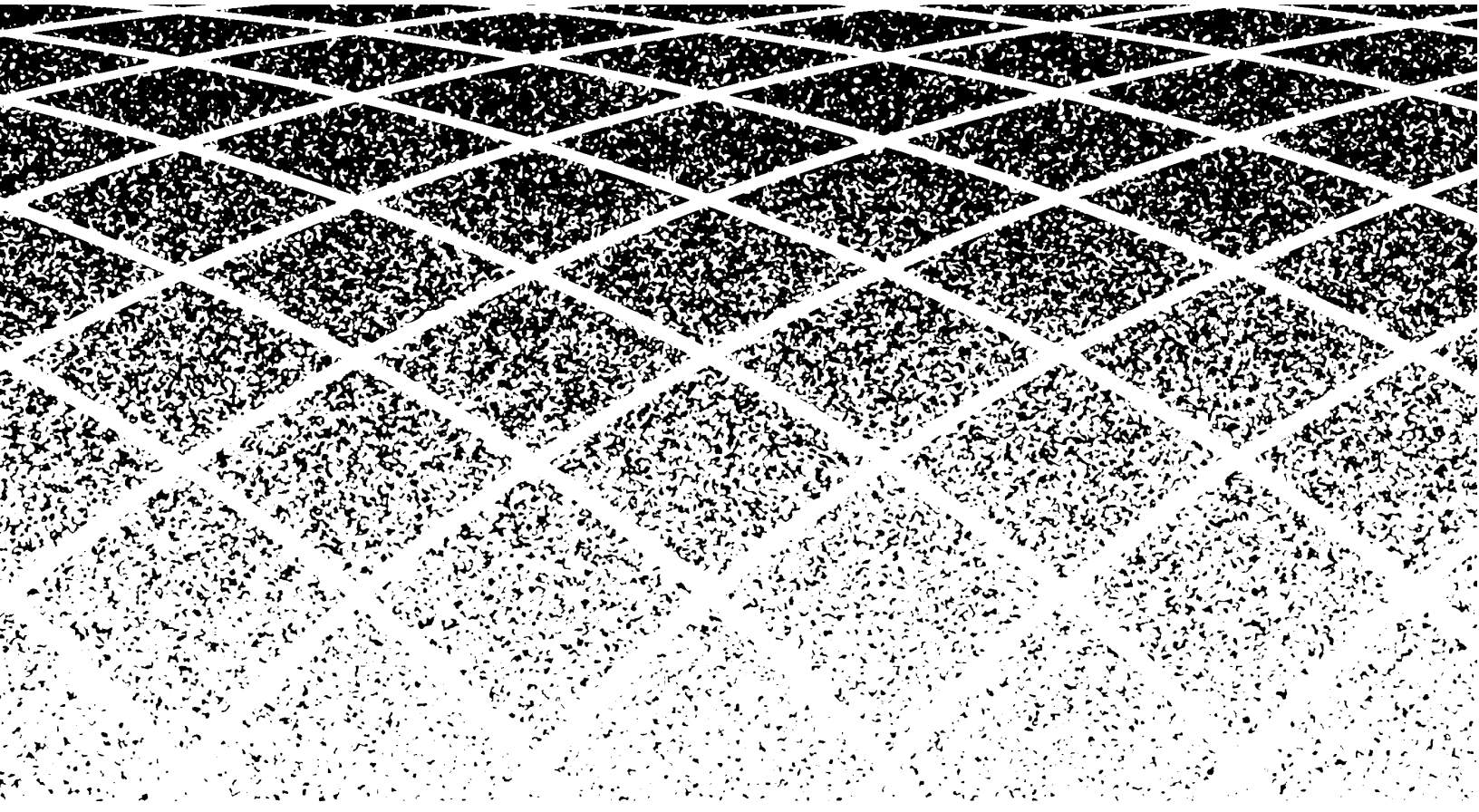
Version 2012.2
June 2012

AT&T
Voice DNA® on AT&T VPN
Customer Configuration Guide



© 2012 AT&T Intellectual Property. All rights reserved.
AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

AT&T Voice DNA® on AT&T VPN Service
Customer Configuration Guide

Contents

List of Figures

List of Tables

AT&T Voice DNA® on AT&T VPN Service Customer Configuration Guide

1. About This Guide

This guide is a technical configuration guide to assist the installation of the AT&T Voice DNA® on AT&T VPN Service at a customer premises. This guide does not address the configuration of specific features of Voice DNA onto particular phones; this is addressed in separate management and end-user guides identified in this document.

This Customer Configuration Guide ("CCG") is offered as a convenience to AT&T customers. The specifications and information regarding the product in this CCG are subject to change without notice. All statements, information, and recommendations in this CCG are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided “AS IS”. Users must take full responsibility for the application of the specifications and information in this CCG.

In no event shall AT&T or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage arising out of the use or inability to use this CCG, even if AT&T or its suppliers have been advised of the possibility of such damage.

Also please note that while AT&T Voice DNA supports E911/911 calling capabilities, there are circumstances when that E911/911 service may not be available, as stated in the Service Guide for AT&T Business Voice over IP Services found in the SG Library at *http://new.serviceguide.att.com*. Such circumstances include, but are not limited to, relocation of the end user’s CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer’s location in the automatic location information database. Please review the AT&T Business Voice over IP (BVoIP) Services Service Guide in detail to understand the limitations and restrictions.

1.1 Audience

This guide should assist the network engineers who will prepare the customer premises network for operation of the AT&T Voice DNA on AT&T VPN Service. The "network engineers" are either customer personnel, for example, in an Information Technology (IT)

department, or an AT&T employee who is installing the service in conjunction with customer personnel. This guide assumes that the reader understands how to make network connections and understands basic networking concepts.

1.2 Contents

This guide is organized as follows:

- **About This Guide —** This section provides information about the audience and document contents.
- **Introduction to AT&T Voice DNA —** This section provides a brief overview of the Voice DNA service on AT&T VPN and the features provided with this service.
- **Overview of the AT&T Voice DNA Installation and Turnup Process —** This section describes at a high level the tasks to perform in the installation and turnup of the service.
- **Network Configuration and Planning —** This section provides information on typical network configuration scenarios, details on customer premises setup, and various notes on network planning considerations.
- **Index —** This section provides an alphabetical list of words and related page number(s) for easy access to terms in this guide.

2. Introduction to AT&T Voice DNA® on AT&T VPN Service

AT&T Voice DNA is a virtual, network-hosted Voice over Internet Protocol (VoIP) service for AT&T business customers. AT&T Voice DNA Personal Web Sites are provided for end-users, and AT&T Voice DNA Administrator Tools are provided for office phone managers.

The AT&T Voice DNA service provides the following:

- Carrier-class primary local service and features (e.g., N11, 8YY, Public Switched Telephone Network [PSTN] off-net, etc.)
- Line-side features (e.g., Call Hold, Call Waiting, etc.)
- Advanced features (e.g., Locate Me, Click-to-Call, etc.).

AT&T Voice DNA on AT&T VPN provisions a Managed Integration Device (MID) between the Customer Edge (CE) router and LAN switch, which functions as the AT&T demarcation point. The VoIP Demarc/Site Survivability option is required with this service arrangement and is described in more detail later in this document. Please note that the customer is not required to use the backup capability of Site Survivability. AT&T Voice DNA on AT&T VPN is available in the Domestic United States (48 states) within the Business Voice Over IP (BVOIP) service area.

The following AT&T VPN transport service arrangement is supported:

- T1, NxT1, T3 sub-rate T3, OC3, and OC12 transport speeds
- PPP/MLPPP and Ethernet access types

Customers will have options for different types of CPEs, including SIP-enabled IP phones, analog phones and faxes supported by an adapter, and a PC-based softphone. The

Customer Premises Equipment (CPE) Configuration Guide defines the various CPEs supported.

The LAN interface functions of the CE router will move to the MID. The CE router, either client or AT&T Managed, must be prepared to interface directly with the MID.

When planning for Voice DNA on AT&T VPN implementation, keep in mind the following points:

- COS1 must be provisioned on the AT&T VPN service. COS package Multimedia High or Multimedia Standard is required. The COS profile must be 101-117.
- Ensure that sufficient bandwidth is allocated to support the number of concurrent calls expected on the AT&T VPN service.
- Port Type must be PPP, MLPPP or Ehternet
- Access is T1, NxT1, sub-rate T3, OC3, or OC12
- The CE router must be configured to support the AT&T MID
- AT&T will assign two Public IP addresses: one IP address to be provisioned on the AT&T or customer managed router LAN interface, and the second to be provisioned on the MID WAN interface.
- The CE router will no longer perform DHCP, tagged VLANS, or NAT functions. These functions will be performed by the MID.

2.1 Voice DNA Personal Web Sites, Administrator Tools, and User Guides

AT&T Voice DNA on AT&T VPN service includes two web-based interfaces: the AT&T Voice DNA Administrator Tool and the AT&T Voice DNA Personal Web Site. The AT&T Voice DNA Administrator Tool is used by office phone managers to:

- Configure end-users (employees)
- Configure company-wide phone features and services
- Assign the features and services to individual phones

Once configured, end-users can use the AT&T Voice DNA Personal Web Site to configure their own personal phone features.

Separate user guides are available. The *AT&T Voice DNA Administrator Guide*[1] is intended for company administrators and provides detailed information regarding using the AT&T Voice DNA Administrator Tool to configure each of the AT&T Voice DNA line side features. The *AT&T Voice DNA User Guide*[2] is intended for end-users and provides detailed instructions for customizing the AT&T Voice DNA features using the AT&T Voice DNA Personal Web Site and supported phones.

1. Available on the AT&T Voice DNA Administrator Tool
2. Available on the AT&T Voice DNA Personal Web site.

3. Overview of the AT&T Voice DNA Installation and Turnup Process

This section gives an overall perspective of the installation and operational readiness of the AT&T Voice DNA on AT&T VPN service. At a high-level, the activities can be logically organized into the following hierarchy (see Figure 1).

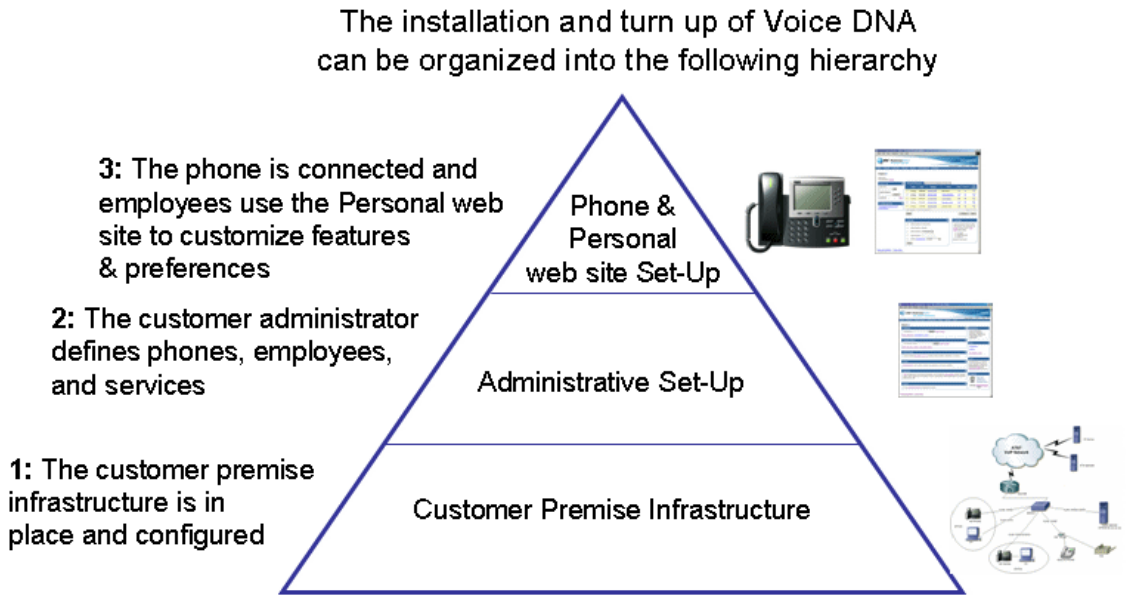


Figure 1. Installation Process

4. Network Configuration and Planning

AT&T Voice DNA on AT&T VPN provides a fully hosted network-based VoIP service. It provides local service and features (such as 8YY), PSTN offnet and line sides features (such as call holding and call waiting), and other advanced features (such as Find Me and Follow Me).

AT&T Voice DNA on AT&T VPN is an MPLS enabled VPN. The customer connects to the AT&T VPN network via the use of PPP/MLPPP or Ethernet access type and transport speeds of T1,NxT1, T3, sub-rate T3, OC3 or OC12, over single or multiple logical channels. The customer or AT&T may own and manage the router on their premises used to connect to the AT&T Managed Integrated Device (MID). Both BGP and static routes can be used to connect the managed router.

The specific requirements for customer setup and configuration depend on a couple of factors. The first of these factors is whether the Managed Interface Device (MID), the EdgeMarc (EM), is local to the CE router (CE-Local) within the same layer 3 domain, or is remote to the CE router (CE-Remote) behind another workgroup router in the customer

network. The second factor is whether the CE router is customer managed or AT&T managed.

This section describes the following:

- Network Planning Considerations

☞ **IMPORTANT:**
All IP addresses used in this document are for example only unless otherwise indicated.

4.1 Set Up

AT&T will provide the following:

- Assignment of the public IP address sub-net required for the EdgeMarc (MID) WAN side IP address.
- The Ethernet cable between the EdgeMarc (MID) and the CE router, which can either be a straight-through or crossover, since the EdgeMarc (MID) port is auto MDI/MDIX (for an AT&T managed router).
- One of the following three types of addressing schemes:
  - Type A: with /30 prefix supporting one EdgeMarc (MID)
  - Type B: with /29 prefix supporting up to 5 EdgeMarcs (MIDs)
  - Type C: with /28 prefix supporting up to 12 EdgeMarcs (MIDs)

  The decision as to which type will be designed or chosen for a site will be performed by AT&T while documenting the customer's network design and defining the sizing for the site. This information will be captured during the ordering process as Campus Type. The number of EdgeMarcs (MIDs) required for a customer's Voice DNA on AT&T VPN solution will determine the Campus Type and the IP prefix assigned.

The AT&T Voice DNA on AT&T VPN customer must provide the following:

- AT&T VPN Transport
- Broadband Internet access – needed to access the Voice DNA Administrator and User Portals
- A dedicated POTS line to be used for modem access to the EdgeMarc (MID) for maintenance.
- An PRI or POTS line(s), if desired, for Site Survivability
- The Ethernet cable between the EdgeMarc (MID) and the CE router that can either be a straight-through or crossover, since the EdgeMarc (MID) port is auto MDI/MDIX (for a customer managed router)

Other Information:

- EdgeMarc (MID) will perform DHCP for the IP phones and data devices on the EdgeMarc LAN.
- The only network interface supported on the EdgeMarc (MID) 4608 will be Ethernet 10/100/1000.

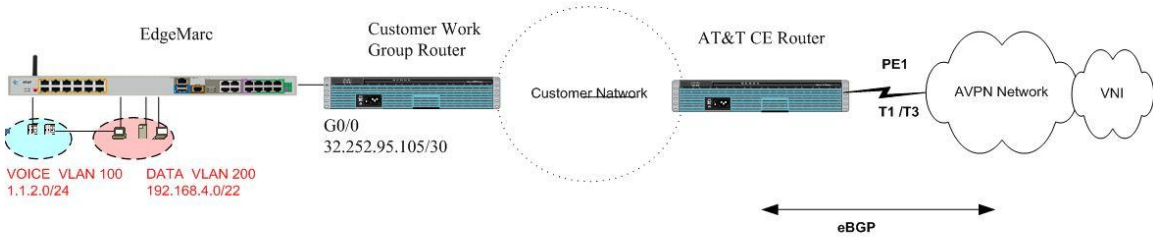


Figure 2. Set up – AT&T MID (EdgeMarc) and Customer managed router

Troubleshooting and management of the MID will be performed either via an IPSec tunnel through AT&T VPN, or via the remote access capability using the external or built-in modem access to the MID console port.

NOTE:

If the CE router is not directly connected to the MID, then static routes and/or dynamic routes for the AT&T Public IP address block must be configured between the customer managed workgroup router and the CE router.

4.2 Configuration

These are the configuration steps required to connect the MID (EdgeMarc). The configuration is based on the Cisco router IOS commands.

The configuration steps the customer is required to perform within this section are identified in the table below.

Table 1. MID (EdgeMarc) Connection Configuration Steps

CE Router Management	MID Location CE-Local or CE-Remote	Required Steps
AT&T Managed	CE-Local	No customer changes required - AT&T is responsible.
AT&T Managed	CE-Remote	Customer must implement 4.2.1 in the work group router in front of the MID. AT&T will implement the remaining configuration steps.
Customer Managed	CE-Local	Customer must implement all steps in Sections 4.2.1, 4.2.2, and 4.2.3 in the CE router.
Customer Managed	CE-Remote	Customer must implement 4.2.1 in the work group router in front of the MID. Customer must implement all remaining steps in Sections 4.2.2 and 4.2.3 in the CE router.

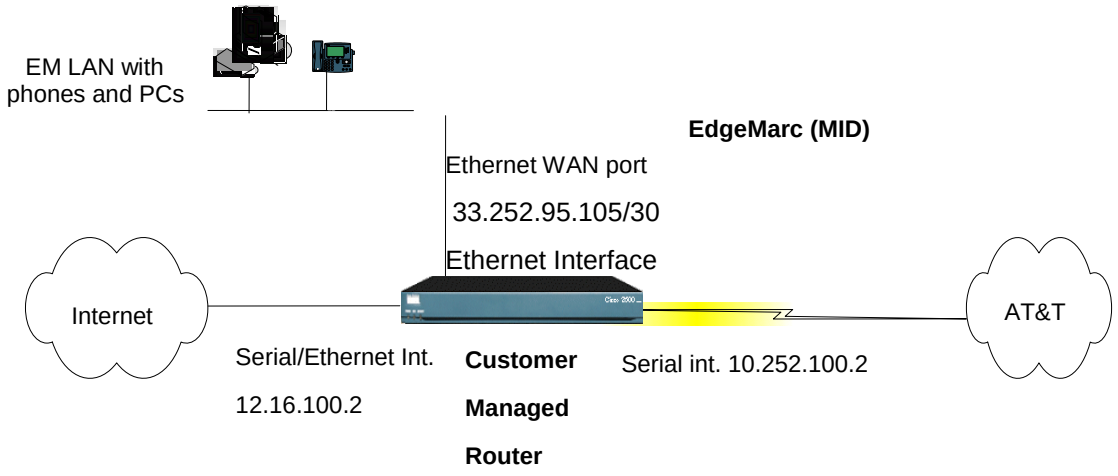


Figure 3. AT&T MID (EdgeMarc) and Customer Managed Router Configurations

4.2.1 Ethernet Interface to LAN

Configure the Ethernet primary or secondary IP address of the router with the first available IP address from the / Public IP address assigned.

interface GigabitEthernet 0/0

ip address 32.252.95.105.255.255.255.252

4.2.2 Serial (or Ethernet) Interface to AT&T VPN

Configure the private IP address to connect the router to the AT&T VPN Provider Edge (PE) router. This may be in place already if there is existing service.

interface Serial 0/0

ip address 10.252.100.2.255.255.255.252

4.2.3 Routing

To allow connectivity, static and BGP routing will typically be used.

4.2.3.1 Default Static Route

The default static route for the AT&T VPN CE router must point to the AT&T VPN PE router.

Default routes will be used to forward the signaling and management traffic to the AT&T VPN CE router. The default route **MUST** point to the AT&T VPN PE router.

ip route 0.0.0.0 0.0.0.0 10.252.100.1

To allow the EdgeMarc (MID) to properly communicate with the Cisco ASA in the AT&T work center, add the following route to the CE router:

- ip route 32.95.217.109 255.255.255.255 10.252.100.1

NOTE:
The Cisco ASA at the AT&T work center is 32.95.217.109 and is the ACTUAL outside address of the Cisco ASA facing probe.

Replace the 10.252.100.2 IP with the AT&T VPN neighbor IP address.

4.2.3.2 BGP Routes

The following BGP statements should be added to the CE router. AT&T will assign AS# from the private range (between 65000 through 65030).

router bgp 65000

no synchronization

bgp log-neighbor-changes

network 10.252.100.0 mask 255.255.255.0 #Customer LAN

network 32.252.95.104 mask 255.255.255.252 #/30 Assigned for this service

neighbor 10.252.100.2 remote-as 13979 #AS 13979 is the actual PE AS value

redistribute connected

no auto-summary

NOTE:
BGP customers will receive many subnets that AT&T uses for Voice DNA service and life cycle management.

4.3 Policy-based Routing

Policy-based routing or routing control can be implemented on the CE router. The objective is to ensure that the correct traffic originating from a given EdgeMarc (MID) is sent via a given Logical Channel (LC) to a given VPN Routing Forwarding (VRF).

1. **Create access-lists to match the source EdgeMarcs (MIDs) IP address.**

   access-list 101 remark MID#1 traffic

   access-list 101 permit ip host 10.1.1.10 any

   !

   access-list 102 remark MID#2 traffic

   access-list 102 permit ip host 10.1.1.20 any

2. **Create route maps.**

   Route-map map1 permit 10

   Match ip address 101

   Set ip next-hop 172.16.10.2

Route-map map 1 permit 20

Match ip address 102

Set ip next-hop 172.16.10.2

3. **Apply policy map to the physical interface towards the AT&T PE router.**

   Interface Pos 0/1/0

   Ip policy route-map map1

4. **Configure sub-interfaces on the AT&T PE router.**

   Interface Pos 0/1/0

   ip address 172.16.10.1

   Description LC#1 to VRF#1

   Bandwidth 10000

   Interface Pos 0/1/02

   ip address 172.16.20.1

   Description LC#2 to VRF#2

   Bandwidth 20000

4.4 Quality of Service (QOS) Considerations

Most VoIP deployments use some kind of Quality of Service/Class Of Service methodology to provide priority to the voice traffic over the data traffic. AT&T Network (PE) routers (that the CE router connects to) are configured with Class Of Service (COS) options to provide priority to the voice signaling and media traffic destined to the CE router.

All customer routers and switches in the path between the EdgeMarc (MID) and the AT&T PE router should be configured to provide 90% of the traffic for real time handling. It is up to the customer to decide how to configure all the routers and switches to provide priority to the voice signaling and media traffic. SIP and RTP traffic from the EdgeMarc WAN public address should be prioritized. The standard port for SIP is 5060 and RTP ports are 16384-32767.

4.5 Network Address Translation (NAT) Overview

SIP aware NAT or SIP Application Later gateway function (SIP ALG) must be **disabled** in the routers in the path between the EdgeMarc (MID) and the AT&T PE router. Here is an example for the command used in the Cisco router:

- no ip nat service sip udp port 5060

4.6 Firewall Rules or Access-Lists

If there is an access-list used on the internet serial interface of the customer managed routers in the path between the EdgeMarc (MID) and the AT&T PE router, then the customer must open the following ports. These are used for signaling and voice payload protocols and the IPSec tunnel which is used by AT&T to manage and maintain the MID (Edgemarc).

The following ports must be allowed through the router:	
Protocol	**Ports**
TFTP	UDP 69
HTTPS/TLS	TCP 443
HTTP	TCP 80
SIP signaling	UDP 5060
RTP media	UDP 16384-32767
IPSec (ESP/AH)	IP ports 50 and 51
ISAKMP	UDP 500
ICMP	echo/echo-reply

4.7 Multi-Site Scenario

For Multi-site scenarios where traffic from the branch office goes through the AT&T VPN network, the customer must redistribute the static routes to BGP on the headquarters router.

This is the configuration step:

router bgp 65000

redistribute static

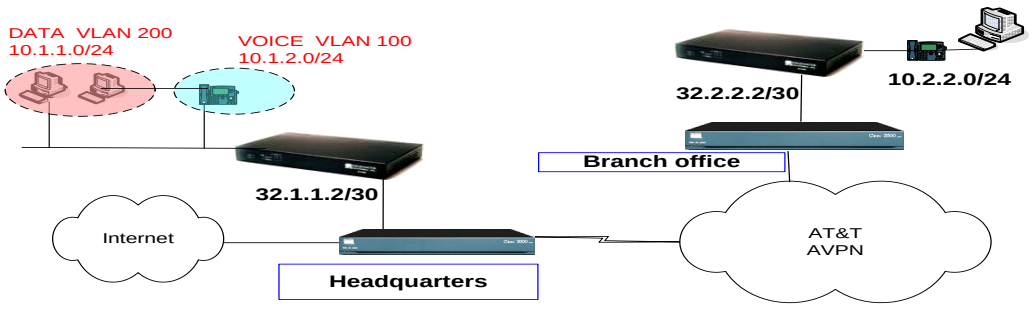


Figure 4. Multi Site Scenario Configuration

5. VoIP Demarc/Site Survivability Mandatory

As noted earlier, VoIP Demarc/Site Survivability is required for AT&T Voice DNA on AT&T VPN.

VoIP Demarc/Site Survivability is provided by deploying an EdgeMarc device, also called the AT&T Managed Integration Device (MID), at the customer's premises. The MID functions as the service demarcation point for Voice DNA. The MID is managed by AT&T. The MID's role as a demarcation device is to allow AT&T to manage the customer's Voice DNA network based service, including:

- Maintenance of MID
- 911 move detection and restriction
- Performance reporting
- Site Survivability (optional) via POTS or PRI access to the MID
- MID-HA (optional), see **6. Managed Internet Device – High Availability** (MID-HA) on page 19

IP addresses assigned to the MID by AT&T will be publicly routable and unique to the customer's site. IP addresses will not be accessible via the Internet due to the AT&T VPN service arrangement.

The MID will perform DHCP and NAT functions on the customer's network and will also function as a full, stateful customer-managed firewall.

Additionally, if the customer procures backup POTS or PRI service, then the MID acts as a failover device. Site Survivability is designed to provide continuity of service in the event of a failure of connectivity to AT&T Voice DNA. The MID will attempt to route calls through the Public Switched Telephone Network (PSTN) until your service is restored.

The MID is designed via Site Survivability, to detect certain events that could cause an interruption of your AT&T VOICE DNA service, including failure in any of the following service components:

- AT&T Virtual Private Network (VPN) circuit
- Customer Managed CE router on the Customer premises
- AT&T provider-edge Router
- IP Border Element – (IPBE)
- AT&T Voice DNA application server, which provides features and routing, and hosts the Administrator web site and User's AT&T Voice DNA personal web sites.

The MID-HA protects against an EM failure as well as lost local connectivity to the customer WAN network. (See section **6. Managed Internet Device – High Availability** (MID-HA) on page 19.)

The MID does not detect other potential failures or service degradation in the IP network and the PSTN.

When the MID detects loss of connectivity to the AT&T network, it switches to the survivability mode and provides:

- Intra-site calls:
  - MID supports call setup between IP devices on the LAN
  - Bearer path completes directly on-LAN.
- Off-net calls:
  - The number of off-net calls limited by the number of POTS lines or PRI connected to the available FXO ports (2 or 6 depending on the EdgeMarc model).
  - The customer will have control over how many POTS lines or PRI are required and used for PSTN calling.
  - 911 calls prioritized
    - When all FXO ports are in use, the longest duration call is dropped to allow the 911 call to complete.
    - Established 911 calls will never be dropped in order to route a new 911 call.
- Inter-site AT&T Voice DNA calls
  - Calls are routed to PSTN via FXO port/POTS line or PRI.
  - PSTN completes a call or provides treatment (e.g., busy tone or announcement)
  - Call completes only if destination site is reachable.
- Inbound PSTN calls:
  - Calls dialed using a POTS line or PRI telephone number (TN) will route to the FXO port.
  - Incoming calls to AT&T Voice DNA TNs completed *ONLY IF* forwarded to a POTS line or PRI TNs connected to Edgemarc FXO ports.
  - MID routes incoming call to the customer specified AT&T VOICE DNA TN.

In general, AT&T's network is designed with high reliability and is centrally monitored and supported on a 7x24 basis by the AT&T Global Network Operations Center (GNOC).

The following items describe important details of the AT&T Voice DNA with AT&T VPN VoIP Demarc/Site Survivability feature:

- The customer must order the Demarcation Site Survivability. The AT&T professional services team will install the AT&T Voice DNA on AT&T VPN service, including the MID, at the customer site. The MID is configured, staged, and shipped to the customer site per the customer's specific LAN configuration.
- There are two AT&T MID devices available: EdgeMarc models 4608T4W and 4562T4W. In normal mode, the MID is transparent to the functions of the network.
- The MID is managed by AT&T. AT&T provides ongoing maintenance for the MID.

- If the customer utilizes the Site Survivability feature of the MID, the Customer is responsible for purchasing the appropriate number of POTS or PRI lines for their back-up, and ensuring that 3-way calling is ordered for all lines. The EdgeMarc model 4608T4W supports two POTS or PRI lines, while the EdgeMarc model 4562T4W supports six POTS or PRI lines.
- The G.729 codec will be used for Voice calls and the G.711 codec will be used for Fax transmissions.
- AT&T does not guarantee or warrant that the MID will operate in all instances of network degradation or outage.
- Site Survivability protection will not be available in the event of a failure of the MID itself. The functioning of the MID is also dependent on the availability of necessary resources, such as electrical power and active connection to a functioning PSTN.
- If the customer utilizes the MID devices for Site Survivability, in addition to the mandatory demarcation, they should specify the AT&T Voice DNA TN that the MID should route incoming POTS calls to in the event of a fail-over condition. If the AT&T Voice DNA TN is not specified, the MID will route incoming calls to the Location Default calling number.
- The customer must provide a POTS line dedicated to the MID to enable AT&T service management and maintenance access.

5.1 AT&T-Managed Integrated Device (MID)

The MID is one of the following EdgeMarc devices:

Model	FXO Ports	FXS Ports
4608T4W	2	6
4562T4W	6	2

5.2 MID Capabilities

The MID functions as the demarcation point for AT&T Voice DNA on AT&T VPN service on the customer's site. In addition, it enables AT&T to perform service management and maintenance of the customer's AT&T Voice DNA on AT&T VPN service and enable 911 move detection and restriction capability.

- Each MID is equipped with a number of FXO ports and FXS ports.
- Each FXO port is used for a connection to the PSTN. Each connection is through a Plain Old Telephone Service (POTS line) or Primary Rate Interface (PRI) and all available lines must be connected via the POTS line or PRI in order for the Site Survivability off-net function to be invoked. Each POTS line or PRI must be provisioned with 3-Way Calling.
- Each FXS port can be used as an Integrated Access Device, or IAD, to connect analog phones or faxes.

- Onboard fully stateful firewall capability of the MID will be utilized for voice calls and data traffic.
- The DHCP (Dynamic Host Configuration Protocol) capability used to assign dynamic IP addresses to devices (e.g. SIP phones or PC's) will be provided by the MID instead of the Customer's LAN.
- NATing is provided by the MID. Voice traffic is NAT'd at layers 3 and 5.

5.3 Enabling FXO Ports

The EdgeMarc device is connected to the PSTN network by POTS lines or PRI. This is a requirement for the Site Survivability option. **You (the customer) are responsible for ordering the POTS lines or PRI and having them installed at your premises**.

One POTS line or PRI is required for each active FXO port on the EdgeMarc device. The number of POTS or PRI lines required depends on the EdgeMarc router model you are using.

It is important to note that a POTS line or PRI **must** be connected to **each active** FXO port. If a port on the EdgeMarc is **not** connected to a POTS line or PRI, AT&T Professional Services must **disable** the port at the time of installation.

In addition, **the customer must order three-way calling for each POTS line or PRI** in order for 911 calls to be completed correctly. **If PRI is used for Site Survivability, it needs to deliver 10 digits for the DID numbers to map to 10-digit AT&T VOICE DNA numbers so it can deliver incoming calls in survivability mode. From 1 to 100 mappings of PRI numbers can be specified using the Voice DNA Administrator Portal. No more than 100 numbers should be ordered with the PRI. The only PRI configuration supported is 23B + D - a subset of channels is not supported. Normal ESF framing and B8ZS line encoding is expected and no other special features are required.**

5.4 Service Features

If the Site Survivability option is enabled when connection to the AT&T virtual private network (AT&T VPN) fails, many AT&T Voice DNA features will still be available. However, the availability of some features, such as Locate Me, depends on the type of failure. Some features that may not be available include:

- Extension dialing to other service locations
- Abbreviated dialing to non-AT&T Voice DNA users
- Dialing using speed dial or other star codes
- AT&T Voice DNA operator or custom 911 calling destinations

In addition, you will not be able to configure new AT&T Voice DNA phones or perform some other administrative tasks.

5.5 Call Flows During Survivability Mode

For all AT&T Voice DNA calls:

- Calls on the LAN will continue. Off LAN calls may fail.
- All calls will survive going from survivability mode to normal mode upon recovery from the network failure.
- There is no indicator on the phone that will show that the site is in survivability mode.

Intra-site AT&T Voice DNA calls:

- MID sets up SIP call between IP phones.
- Bearer path completes on-LAN.

Off-net calls:

- The number of offnet calls is limited by the number of POTS lines and/or PRIs (2 or 6 depending on the particular EdgeMarc model).
- 911 calls will be prioritized. A 911 call will cause the call that is in progress the longest to be dropped.

Inter-site AT&T Voice DNA calls:

- If the failure is with the originating site's AT&T Virtual Private Network (AT&T VPN) service, the call will route via PSTN and complete if dialed using the seven digit local number, or 1 plus ten digits, for a long distance call.
- If the failure is somewhere within the AT&T VOIP network, the terminating site's VOIP endpoints will not be reachable. Calls will route according to the users' alternate routing settings (e.g., Locate Me, Fwd to VM). Calls to designated POTS and/or PRI TNs configured on the receiving site's MID will complete if ports are available.
- If the failure is with the AT&T Voice DNA Server, only calls to the POTS lines and/or PRIs will complete, and the users' alternate routing settings in their Voice DNA personal web page will not be invoked.

Inbound calls:

- If the site's AT&T VPN connectivity is down, calls to the Voice DNA TNs will be routed per the user's Locate me profile or transferred to Voicemail.
- If the failure is within the AT&T VOIP network, calls to the Voice DNA TNs will be routed per the user's Locate Me profile or transferred to Voicemail.
- If the failure is within the AT&T Voice DNA Application Server, only calls to the POTS lines and/or PRIs will complete. The calls are routed to the DCN and can then be forwarded by the person answering the DCN phone.

5.6 Site Survivability Configuration

Error! Reference source not found. shows a typical configuration using the Site urvivability feature and Figure 6 shows the configuration when in Network Failure mode.

5.6.1 Normal Condition

With AT&T Voice DNA on AT&T VPN, an MID is installed between the LAN switch and Customer Managed CE Router. The MID may be connected to the PSTN network by a number of POTS lines and/or PRIs. The MID provides DHCP capability, instead of your company's LAN.

Under normal conditions, calls will pass through the MID, bypassing the POTS/PRI lines.

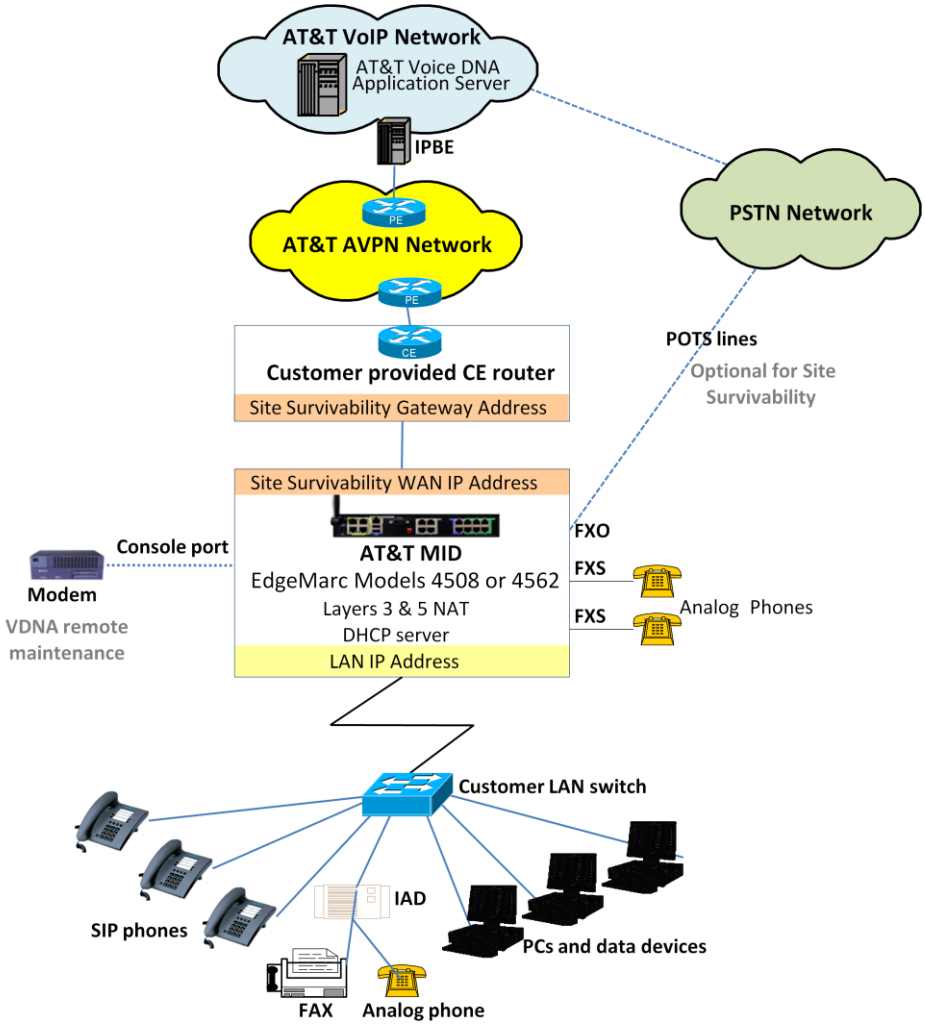


Figure 5. Site Survivability Configuration (Normal)

5.6.2 Network Failure Scenario

In the event that the connection to the AT&T network **fails** for any reason, the MID is designed to detect the failure and begin to route calls through the PSTN, until service is restored. The MID is connected to the PSTN via the POTS and/or PRI lines.

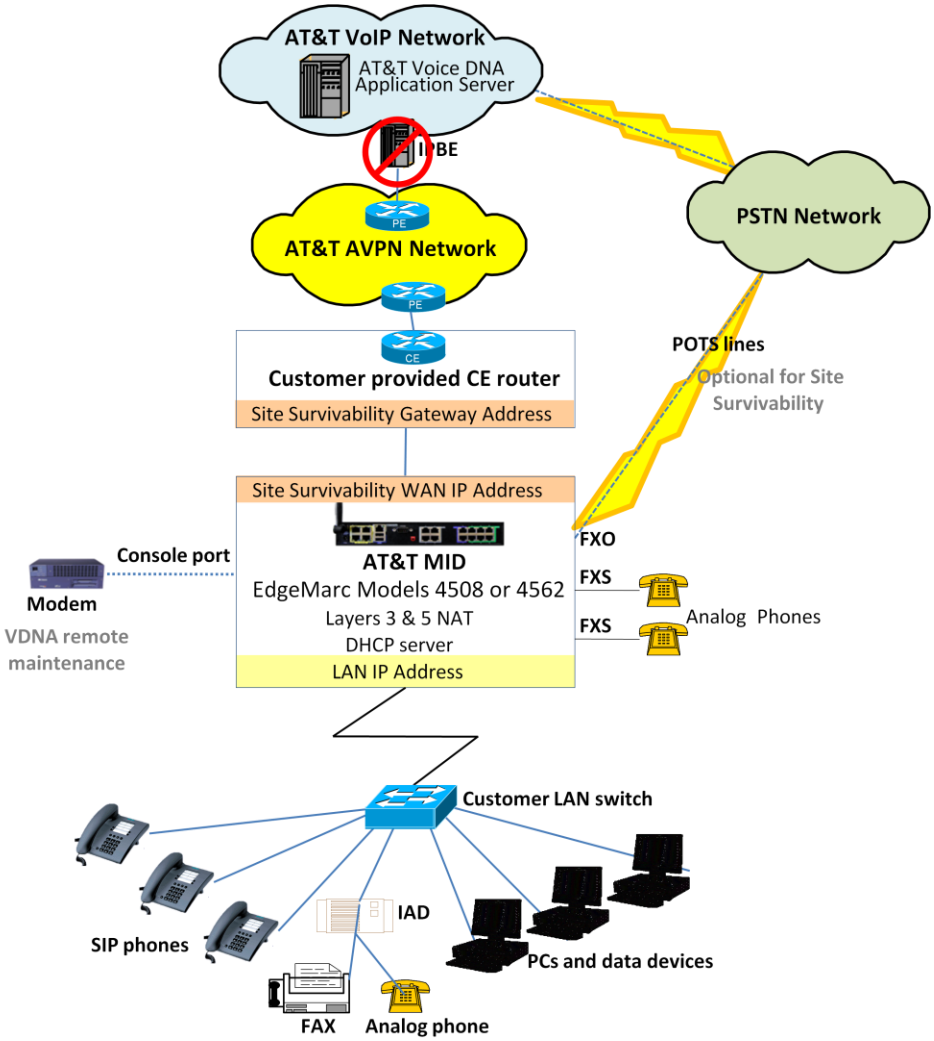


Figure 6. Site Survivability Configuration (Network Failure)

Survivability Mode Phone Feature Matrix

Table 2. Phone Feature Matrix

Feature	Aastra 6757i/ 6757iCT	Cisco 7940 7960	Polycom 301 320 321 330 331 560 600 601 650	Polycom 4000/6000	LG 6812 6830	VG224 (IAD)	EdgeMarc 200EW IAD	Cisco ATA IAD	Citel Phone Adapter (IAD)	Counter Path eyeBeam	Survivable mode Note: Feature only available if supported by phone
Bridged Line Appearance (BLA)	√	X	√	X	√	X	X	X	X	X	√
Call Hold	√	√	√	√	√	Varies	√	√	√	√	√
Call Logs	√	√	√	√	√	X	X	X	X	√	Call logs in phone are supported but not on the AT&T Voice DNA Personal Web Site
Call Transfer Blind	√	√	√	√	√	√	√	√	√	√	√
Call Transfer – Consultative	√	√	√	√	√	Varies	√	√	√	√	√
Conferencing (via SIP phones up to 3 call legs)	√ but NOT hand-set	√	√	√	√	X	√	√	X	√	√
Direct Outward Dialing (DOD)	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	√
Do Not Disturb – Phone	√	√	√	√	√	√	√	√	√	√	√* * Voicemail will not be available
Multiple Line Appearances — Basic	√	√	√	X	√	X	X	X	X	X	√
Multiple Line Appearances — Repetitions	√	X	√	X	√	X	X	X	X	√	√
SIP Forking	√	√	√	√	√	X	√	√	X	X	√* * Limited to BLA functionality for LAN
Station to Station Dialing	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	√

6. Managed Internet Device – High Availability (MID-HA)

The Managed Internet Device – High Availability (MID-HA) capability is an orderable feature available for the VDNA Transport Agnostic Service. The MID-HA feature eliminates the EdgeMarc (EM) device as a potential single point of failure by allowing two EdgeMarc devices at the customer premise location. One EM device functions as the primary, while the other device is the backup. The attached LAN and the far-end Wan devices do not detect two EM devices. Instead, the two devices appear as a single device by using a Virtual WAN IP and LAN IP address.

EM1 and EM2 exchange "state" information. When one of the failure conditions occurs on the primary device, or the primary device is administratively put into disabled mode for maintenance, the secondary device takes over as the primary device. Once back online, the original primary device can be configured to remain in backup mode, or revert back to primary mode (see Figure 7).

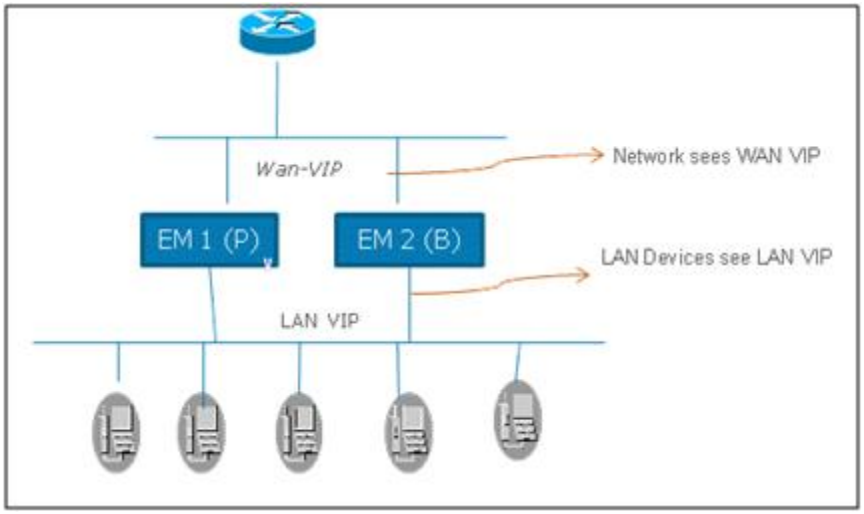


Figure 7. MID-HA configuration

The MID-HA capability protects against the following types of failures/conditions:

- Physical (chassis or power failure)
- Data Link (Ethernet link failure) – cut, broken, or disconnected EM WAN port to WAN network
- Operating System problems
- Active EM, administratively disabled for maintenance

The MID-HA capability is available on the following two EM models:

- 5300LF2
- 4608T4WDPoE

The 5300LF2 also protects against a cut, broken, or disconnected cable connecting the EM LAN port to the LAN network.

The 4608T4WDPoE12 has an integrated LAN PoE switch, and a failure or restart of this switch causes the Primary EM to relinquish its active state, and the back-up EM becomes the active EM. However, a failure at any single LAN switch port only affects the devices connected via that port, and the MID-HA will not be invoked (the Primary EM remains active).

MID-HA EM 4608T4WDPoE and Site Survivability

For the EM 4608T4WDPoE MID-HA arrangement with site survivability, only the Primary 4608T4WDPoE requires a PSTN facility (for example, FXO or PRI), and nothing is connected to the FXO or PRI on the MID-HA EM 4608T4WDPoE. This provides PSTN access when the Primary EM goes into Site Survivability local mode. If the site goes into local mode while the secondary EM 4608T4WDPoE is the active device, the customer still has on-LAN calling, but will not have PSTN access to complete other types of calls via the PSTN.

For the EM 4608T4WDPoE MID-HA arrangement, only the Primary 4608T4WDPoE has FXS connected devices. (There are no FXS devices connected to MID-HA EM 4608T4WDPoE.) This means that if the customer has a mission-critical analog device, the device must be connected via an IAD to remain online during a failover to the MID-HA EM device.

Index