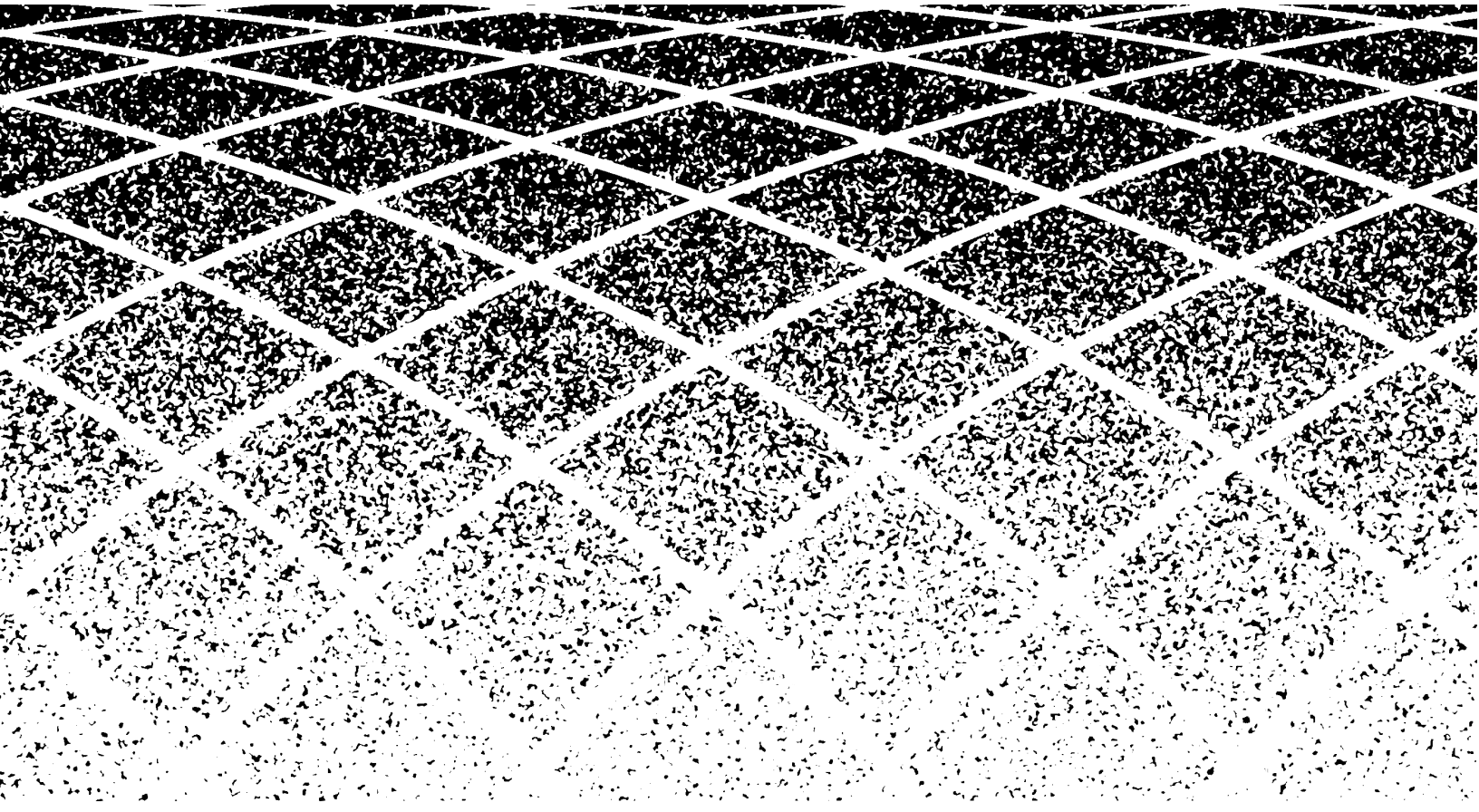
Version 2012.2
March 2012

AT&T
Voice DNA® on MIS/PNT
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 MIS/PNT
Customer Configuration Guide

Contents

1. About This Guide 1
- 1.1 Audience 1
- 1.2 Contents 1

2. Introduction to the Voice DNA Service 2
- 2.1 Voice DNA Personal Web Sites, Administrator Tools, and User Guides 2

3. Overview of the Voice DNA Installation and Turnup Process 3

4. Network Configuration and Planning 4
- 4.1 Network Planning Considerations 4
- 4.1.1 DHCP Servers 5
- 4.1.2 Customer Managed Firewall 7
- 4.1.3 Network Address Translation (NAT) 9
- 4.1.4 Switches 9
- 4.1.5 LAN Switches approved for use with AT&T Voice DNA Service 10
- 4.1.6 Hubs 11
- 4.1.7 Other Networking Considerations 12
- 4.2 Typical Network Configurations 12
- 4.2.1 Definitions of Terms 13
- 4.2.2 MIS Access with ASA Firewall 14
- 4.2.3 MIS Access with DMZ 15
- 4.2.4 MIS Access with VLAN (Recommended) 16
- 4.2.5 PNT Configuration 17

5. Site Survivability Option (SSO) 17
- 5.1 AT&T-Managed Integrated Device (MID) 20
- 5.2 EdgeMarc Capabilities 21
- 5.3 Additional Functions and Constraints 21
- 5.4 Ordering POTS Lines 22
- 5.5 Service Features 22
- 5.6 Call Flows During Survivability Mode 23
- 5.7 Site Survivability Configuration 24

5.7.1 Normal Condition 24
5.7.2 Network Failure Scenario.....25
5.8 Survivability Mode Phone Features 26

Index Index-1

List of Figures

1. About This Guide 1
2. Introduction to the Voice DNA Service 2
3. Overview of the Voice DNA Installation and Turnup Process 3
Figure 1.Installation Process 3
4. Network Configuration and Planning 4
Figure 2.Example of SIP Phones on the Outside of the Firewall 7
Figure 3.MIS Access with ASA Firewall 14
Figure 4.MIS Access with DMZ 15
Figure 5.MIS Access with VLAN 16
Figure 6.PNT LAN Configuration 17
5. Site Survivability Option (SSO) 17
Figure 7.Site Survivability Configuration (Normal) 24
Figure 8.Site Survivability Configuration (Network Connection Failure) 25

List of Tables

1. About This Guide 1
2. Introduction to the Voice DNA Service 2
3. Overview of the Voice DNA Installation and Turnup Process 3
4. Network Configuration and Planning 4
Table 1.Supported DHCP Configurations 5
Table 2.DHCP Settings 6
5. Site Survivability Option (SSO) 17
Table 3. Survivability Mode Phone Feature Matrix 26

AT&T Voice DNA® on MIS/PNT
Customer Configuration Guide

1. About This Guide

This guide is a technical configuration guide to assist the installation of the AT&T Voice DNA® Managed Internet Service (MIS)/Private Network Transport (PNT) 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 a separate management and end-user guides identified in this document.

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 service. The "network engineers" are either customer personnel in, for example, an Information Technology (IT) department, or AT&T-approved partners 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 the AT&T Voice DNA Service** — This section provides a brief overview of the Voice DNA service and features.
- **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 setups, and various notes on network planning considerations.
- **Appendix** — This section provides information on AT&T Voice DNA Line Features supported by the various IP phones.

- **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 the Voice DNA 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 has service access options, including MIS with VoIP and PNT with VoIP. The customer will be provided with an AT&T Managed Customer Edge Router that connects directly to a LAN on the customer premises.

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.

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

AT&T Voice DNA 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 office phone managers 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 Voice DNA Installation and Turnup Process

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

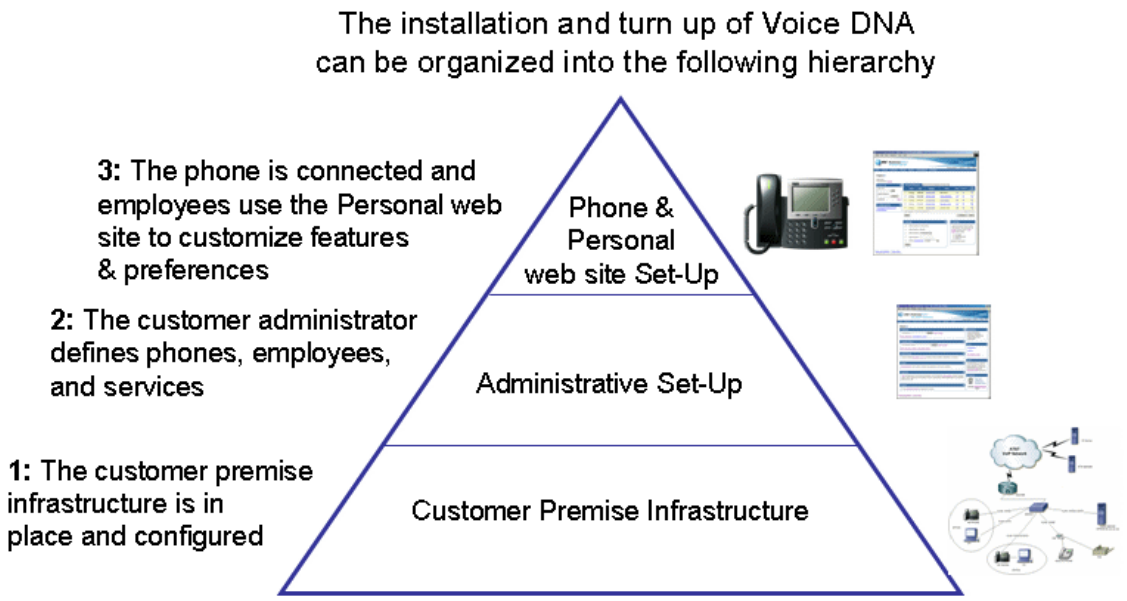


Figure 1. Installation Process

The following sections provide a brief overview of the associated activities.

4. Network Configuration and Planning

AT&T Voice DNA service is available with the AT&T MIS (Managed Internet Service) and AT&T PNT (Private Network Transport) or AT&T AVPN (Virtual Private Network) access types. It provides a network hosted PBX solution for the SIP phones and terminal adapters that can provide the service to analog phones.

AT&T Voice DNA with MIS access provides Internet connectivity and AT&T Voice DNA service features.

AT&T Voice DNA with the PNT provides intra-company connectivity and Voice DNA service features. PNT inherently is a secure network because it is based on the MPLS VPN enablement of the AT&T IP backbone. No general internet access is available with PNT. Even if internet access is available via the customer LAN (apart from the VDNA PNT service), it will most likely not be accessible to the VDNA voice traffic. As a result, VDNA customers with PNT will most likely not have access to the DNS that would be used for FQDN and domain name resolution. Special consideration for PNT customers (e.g., customers whose voice traffic cannot access DNS for FQDN and domain name resolution) are noted throughout the document.

An AT&T managed router is required at the customer site for all AT&T Voice DNA with MIS and AT&T Voice DNA with PNT. The AT&T managed router provides the real-time high priority Class of Service for voice traffic as well as Layer 3 NAT (Network Address Translation) function for the voice signaling and media traffic.

AT&T Voice DNA service uses the SIP protocol for VoIP signaling and RTP for the voice media packets.

This section describes the following:

- Network Planning Considerations
- Typical Network Configurations

4.1 Network Planning Considerations

Typical components of a customer's Local Area Network may include a DHCP server, a firewall, a NAT device, LAN switches, a Virtual Local Area Network (VLAN) setup for voice/data separation, and cabling for PCs and phones.

4.1.1 DHCP Servers

DHCP servers may be embedded in the AT&T managed MIS or PNT routers or deployed on separate hardware. DHCP servers may be centralized, supporting multiple locations, or there may be separate DHCP servers at each location. The same DHCP server can be used for data devices (for example, computers, and printers) as for VoIP devices (that is, SIP phones) or separate DHCP servers can be deployed. If separate DHCP servers are deployed for voice and data, it is the customer's responsibility to partition their network, configure routers and DHCP relay agents to send DHCP requests to the proper servers. Address blocks can be shared between voice and data devices, but there are some advantages, especially regarding Quality of Service (QoS), that may be achieved through using separate address blocks (along with separate VLANs) for voice and data.

A customer IT administrator is responsible for configuring the DHCP server(s) with appropriate addresses, lease times, options, etc. to meet that customer's networking needs. Given the variety of available DHCP servers, configuration may vary by type of server.

Table 1 describes three supported DHCP configurations.

Table 1. Supported DHCP Configurations

Option	AT&T Managed Router	Customer DHCP	Notes
1	No DHCP	On-site DHCP server	The customer has an on-site DHCP server.
2	DHCP relay function	Remote DHCP server	The AT&T Managed router can be configured to provide DHCP relay functions, if the customer has a remote DHCP server. This will require configuration on the AT&T managed router.
3	DHCP	No DHCP server	If the customer does not have a DHCP server, the AT&T Managed Router will provide DHCP for both voice and data. **NOTE:** A split scenario, where the customer provides DHCP for data and AT&T provides DHCP for VoIP is not supported at this time.

The DHCP server should be configured to send DHCP Options noted in Table 2 to SIP[3] devices. If there are any other devices on the customer's network that use these DHCP options for other purposes (e.g., DHCP option 66 for configuration of local printers), the DHCP server should be configured to distinguish between device types and only deliver the AT&T specified options to the SIP devices.

[3] The AT&T server will not deliver configuration files for any devices except for AT&T Voice DNA SIP devices (phones and adapters).

This can be accomplished by

- putting SIP phones on dedicated LAN segments or VLANs and delivering the AT&T specified DHCP options to DHCP requests originating on those LAN segments or VLANs.

Or

- having the DHCP server use the contents of DHCP Option 60 (*Vendor Class Identifier*) to determine what device has originated the request and only return the AT&T specified DHCP options for SIP devices (phones or adapters).

In some situations, DHCP may not be used or it may not be possible to configure the DHCP server to return the DHCP options as defined in Table 2. Then, each phone would need to be individually configured via its local configuration interface with the necessary information.

For customers who have their own DHCP server, Table 2 shows the DHCP options to be configured on the DHCP server:

Table 2. DHCP Settings

Option	Description
Option 150 AT&T DCB Server	**MIS access 12.194.22.33** **PNT access 12.194.22.33**
Option 66 AT&T DCB Server	**MIS access tftpr2vdna.att.com** **PNT access 12.194.22.33**
Option 159 AT&T HTTP server name	**MIS access — http://sasvpdlr2vnda.att.com/bdl** **PNT access — http://12.194.240.28/bdl**
Option 160 AT&T HTTPS server name	**MIS access — https://sasvpdlr2vnda.att.com/bdl** **PNT access — https://12.194.240.28/bdl**
Option 6 Domain Name Servers	The DNS server IP addresses. Customers that do not have DNS servers must use **MIS:** , and **MIS:**
Option 42 NTP Servers	Option 42 should be set to the LAN IP address of the AT&T Managed Router. **Note that a missing or invalid Option 42 setting will negatively impact phones that use HTTPS for configuration.** These phones will not be able to download configuration files or new phone software because the certificate handshake will fail.

4.1.2 Customer Managed Firewall

AT&T Voice DNA sites with PNT access generally do not require firewalls due to the underlying architecture of the VPN setup. Sites with MIS access are recommended to deploy a firewall to adequately secure their internal networks but it is required that SIP-aware Network Address Translation [NAT] be disabled on the firewall. Please consult your firewall vendor on how to configure that in the firewall. The AT&T Managed router deployed at the site performs Layer 3 NAT but all SIP aware NAT function is done in the AT&T network. This ensures all features of the service will work per the specifications.

NOTE:

AT&T strongly suggests the use of a firewall when MIS access is utilized. Any firewall make/model may be utilized; however, the configuration of the firewall must allow the VoIP traffic to bypass the firewall controls and inspection. The AT&T managed router protects the Voice traffic from being manipulated, while the firewall is designed to protect the data traffic (see **Guidelines**).

Here is the scenario for AT&T Voice DNA sites with firewall:

SIP Phones on the Outside of the Firewall

The SIP phones are placed on a separate LAN segment than the data network.

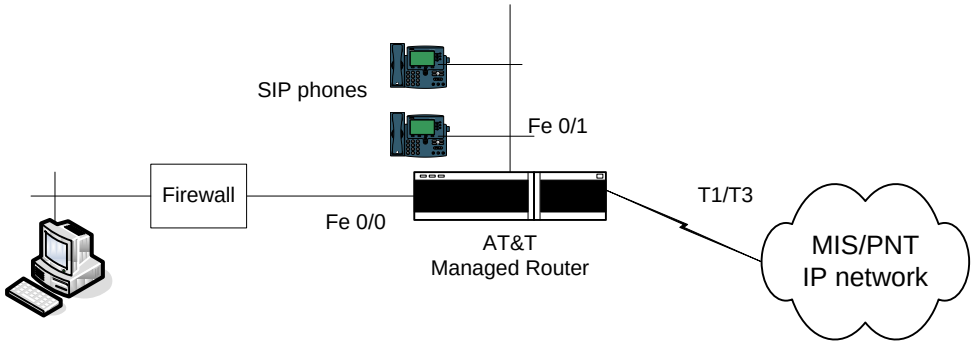


Figure 2. Example of SIP Phones on the Outside of the Firewall

Guidelines

Customers can continue to use the existing firewall in place or choose to deploy any firewall that meets the business security needs. Any firewall can be used since the VoIP packets are NATed by the AT&T managed router.

NOTE:

AT&T does not recommend placing SIP phones on the inside of the firewall, even with SIP ALG and packet inspection disabled, as RTP and SIP packets may arrive out of order and cause voice quality issues. AT&T Voice DNA recommends that the AT&T Managed Router protect the Voice traffic though its series of security checks and configurations.

For reference, the following are the details of the signaling and voice payload protocols.

These must be allowed in the firewall rules.

The following ports must be allowed through for SIP Phones:		
Protocol	**Ports**	**Notes**
TFTP	UDP 69	
HTTPs/TLS	TCP 443	Polycom Phones only
SIP signaling	UDP 5060	
RTP media	UDP 16384-32767	
NTP	UDP 123	

The following are required if the indicated platform is being used:		
Platform	**Protocol**	**Notes**
Cisco VG224	SIP & RTP	See ports above
Cisco ATA-186	SIP & RTP	See ports above
Edgemarc 200 IAD	SIP & RTP	See ports above
CounterPath Eyebeam softphone	SIP & RTP	See ports above

Routing – The firewall must have a default route to the AT&T managed router or have specific routes for the following subnets pointing to the AT&T managed router. These routes must not apply any ACL or inspection parameters.

4.1.3 Network Address Translation (NAT)

The AT&T Device Configuration and Bootstrapping Servers do not initiate any requests to SIP phones, but merely respond to requests for AT&T server file downloads, so it is not required that addresses of SIP phones on customer LANs be published externally (e.g., in DNS). A public IP address must appear as the source address for AT&T Device Configuration and Bootstrapping (DCB) Server requests from a SIP phone. The responses from the AT&T server addressed to that public IP address must be able to reach the SIP phone, hence a requirement for Network Address Translation, or NAT. It may be possible to map internal (e.g., private) IP addresses of multiple phones to the same public IP address, but only if the NAT device does intelligent port mapping so that UDP AT&T Device Configuration and Bootstrapping (DCB) Server responses to arbitrary ports are mapped back to the proper phone. NATing should not present problems for device configuration and bootstrapping[4] of SIP phones for AT&T Voice DNA service as long as each SIP phone can be independently addressed from servers on the AT&T network.

NATing for Voice DNA

For Voice DNA, the most common and recommended NATing option is the NATing provided in the AT&T Managed Router for both MIS and PNT customers.

4.1.4 Switches

It is recommended that the data switch provides inline power (802.1af called Power over Ethernet or PoE) and has a back-up power source. In this configuration, the SIP phones receive power over the LAN's Ethernet connection; without inline power from the switch, each phone must have a separate power connection to an electrical outlet.

NOTE 1:

The LAN trunk port or switch port connecting the AT&T Managed Router **MUST** be set to 100Mb Full Duplex.

NOTE 2:

The AT&T Managed Router port is set to 100Mb Full Duplex, all downstream customer owned devices such as firewalls and LAN switches MUST be set to 100Mb Full Duplex. There are known issues with setting the downstream ports to Autosense

NOTE 3:

Port to ATT MIS or PNT router should be set to 100Mb Full Duplex. For devices, the ports where ATA's are terminated should be auto negotiate or 10Mb Half Duplex.

[4] Bootstrapping refers to a process whereby, a device such as a SIP phone or a TA (Telephone Adapter) booting up, looking for a network server providing configuration information, receives an appropriate response from the AT&T server.

4.1.5 LAN Switches approved for use with AT&T Voice DNA Service

The following switches have been approved for use with AT&T Voice DNA Service. Special dispensation may be required to use a non-standard switch, up to and including, a liability waiver. Custom design and or special handling of non-standard switches may also be required.

- Cisco 2960 (Standard Image)
- Cisco 3550 (Standard Image)
- Cisco 3560 (Standard Image)
- Cisco 3560-X (Standard Image)
- Cisco 2950 (Standard Image)
- Cisco 3750 (Standard Image)
- Cisco 3750V2 (Standard Image)
- Cisco 4500 Chassis Switch (Supervisor Engine IV or >)
- Cisco 6500 Chassis Switch (Supervisor Engine 32 or >)
- Adtran NetVanta 1335 PoE (802.3 af + Cisco Proprietary)
- Adtran NetVanta 1234 PoE
- Adtran NetVanta 1238 PoE
- Adtran NetVanta 1524 PoE
- Adtran NetVanta 1534 PoE Gigabit
- Adtran NetVatan 6355 PoE Multi-Functional
- Adtran 3430 Gateway (Used in custom designs)
- Adtran 4430 Modular (Used in custom designs)
- HP ProCurve 2600 Series
- HP ProCurve 3500yl Series
- HP ProCurve 5400zl Series

NOTE:

Cisco 2950 and Cisco 3550 switches MAY be an older model which do not support 802.3af standard Power over Ethernet (PoE). It is recommended that customer's wishing to use existing 2950 or 3550 models, which do not support standard 802.3af PoE, upgrade to the newer 2960 or 3560 Layer 2 switch models. Mid-span PoE injectors can be used in certain circumstances but are not generally recommended.

NOTE:

Edge switches (i.e. non-Chassis switches) should not be stacked more than 7 times in-line. If 7 or greater switches are required to be stacked, a chassis switch should be utilized instead of additional edge switches. This is not a hardware limitation but a procedural issue to keep the lead switch's processor and memory from being overburdened during heavy usage.

4.1.6 Hubs

For proper functioning of IP phones with AT&T Voice DNA Service, it is recommended that there be no hubs in the network between the AT&T network and the IP phones. Switches must always be used to ensure consistent voice paths.

4.1.7 Other Networking Considerations

- The network should use a VoIP prioritization if it is shared with data applications.
- It is recommended that the network employ a dedicated voice VLAN.
- All voice ports must be full duplex, with the exception of those supporting ATAs, as described in Note 3 in section **4.1.4 Switches**.
- All switch uplink connections should be 100Mb or greater, although 10Mb is acceptable in some circumstances.
- Switches should be chained no more than 7 deep and spanning tree must be disabled on all ports where IP phones are connected.
- Routers and firewalls must be capable of supporting not just IP voice bandwidth but larger than normal numbers of packets without adding jitter. Most network equipment can support this, provided policies requiring software packet inspection are not implemented.
- If an IP phone shares the network connection with the computer at the desktop, the NIC on the computer must be 10/100/1000 auto-negotiable capable. 100Base-T is occasionally required for power users with very high network demands. One Gigabit NIC connection can be employed to take full advantage of the added LAN speed.
- The Ethernet switch to IP phone connection must not exceed 330 feet including all patch cables when using CAT5 or CAT5E. CAT6 and CAT6E should not exceed 550 feet. CAT5 UTP cable may be used with both 10Mb and 100Mb. The CAT3 UTP cable should not be used for VoIP connections.
- Recommended maximum sizing for T1 and T3s:
  - For a T1, you can have 50 - 200 TNs and 50 concurrent calls and no data usage.
  - For a T3, you can have up to 5000 TNs and 700 concurrent calls and no data usage.
- Cabling which connects the Router directly to the switch should utilize a Cat 5 UTP or better rated straight cable.
- Cabling which connects the Router directly to the Firewall, should utilize a Cat 5 UTP or better rated crossover cable.

4.2 Typical Network Configurations

Some typical network configurations with MIS access are described in this section:

- with ASA Firewall
- with Demilitarized Zone (DMZ)
- with VLAN
- with PNT

4.2.1 Definitions of Terms

AT&T Voice DNA

The network-based service platform that provides the AT&T Voice DNA application.

Router

AT&T-managed Edge Router on the customer premises, and the AT&T MIS/PNT access arrangement.

The Router's LAN side interface is connected to a switch.

The model of the Managed Router will be based on the numbers of users. Current supported models are:

- Cisco 2811
- Cisco 2821
- Cisco 3845

LAN

Customer's Local Area Network in which each SIP phone unit is directly connected via an Ethernet cable to the switch. Some SIP phones are equipped with an additional RJ-45 jack that allows a Personal Computer (PC) connection through the phone with a single connection to the switch. The PC can also be connected to the same switch via a separate Ethernet connection. Analog phones and faxes require an IAD module such as a Cisco VG 224, Cisco ATA 186 or an Edgemarc 200 IAD in order to utilize AT&T Voice DNA Service.

An active Dynamic Host Configuration Protocol (DHCP) server is required on the LAN. Refer to Table 2 for the DHCP server settings.

IAD (Integrated Access Device)

The IAD is an adapter that provides support for analog phones and faxes. (See Figure 3 below.) The Cisco VG224, Cisco ATA 186 and Edgemarc 200 IAD are the only supported IADs at this time.

4.2.2 MIS Access with ASA Firewall

The following figure shows a network that is configured with a separate firewall, in this case, a ASA firewall.

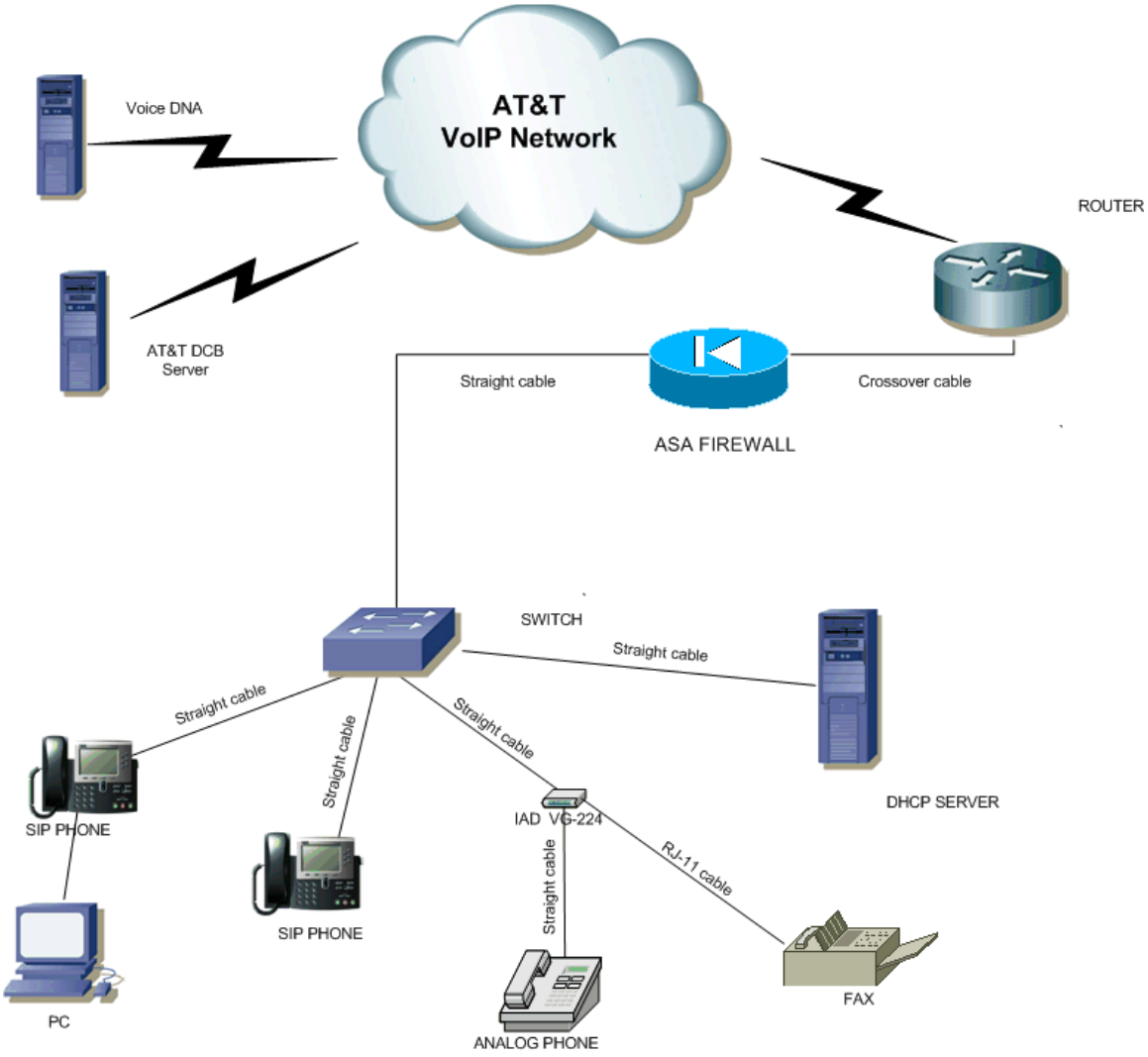


Figure 3. MIS Access with ASA Firewall

The ASA firewall must be configured to allow SIP signaling messages and RTP media between the phones and the VoIP network [from the AT&T Device Configuration and Bootstrapping (DCB) Server].

If the DHCP server is remotely located (i.e. at another site), the firewall and the AT&T managed router must be configured to support DHCP pass through/relay. Additionally, the firewall needs to be configured to allow a search for a download of configuration information from the AT&T Servers (without the need for an HTTP proxy).

4.2.3 MIS Access with DMZ

The following figure shows a network that is configured with a DMZ.

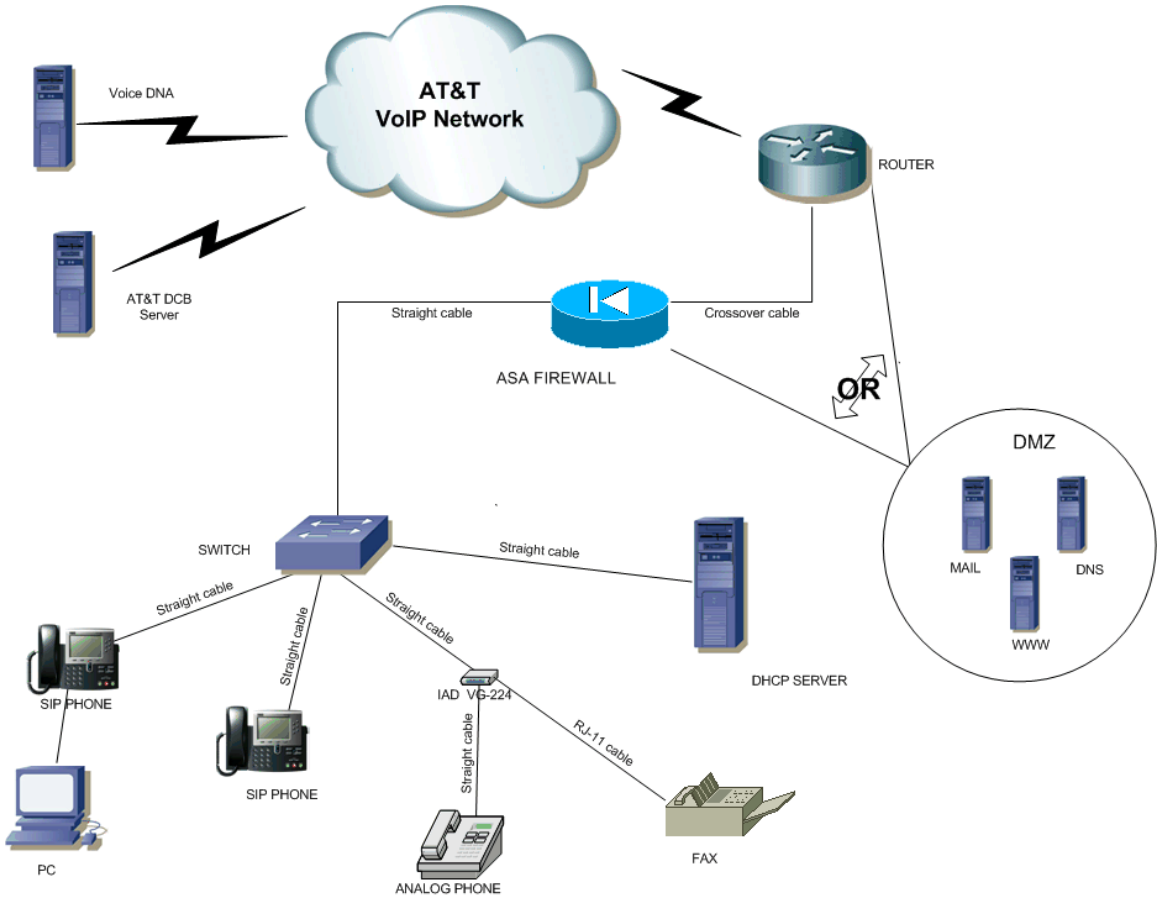


Figure 4. MIS Access with DMZ

The DMZ can be connected to the router or to the firewall. In either scenario, a third interface would be required for the DMZ (e.g., soft port or a physical DMZ port). Routing needs to be configured appropriately for the DMZ to function correctly.

Optional:

If the DMZ is connected directly to the router, configure the interface connected to the DMZ accordingly.

ASA FIREWALL

Optional:

If the DMZ is connected directly to the firewall, configure the filtering and packet routing accordingly.

4.2.4 MIS Access with VLAN (Recommended)

The following figure shows a network that is configured with a VLAN. This configuration separates voice and data traffic on the LAN.

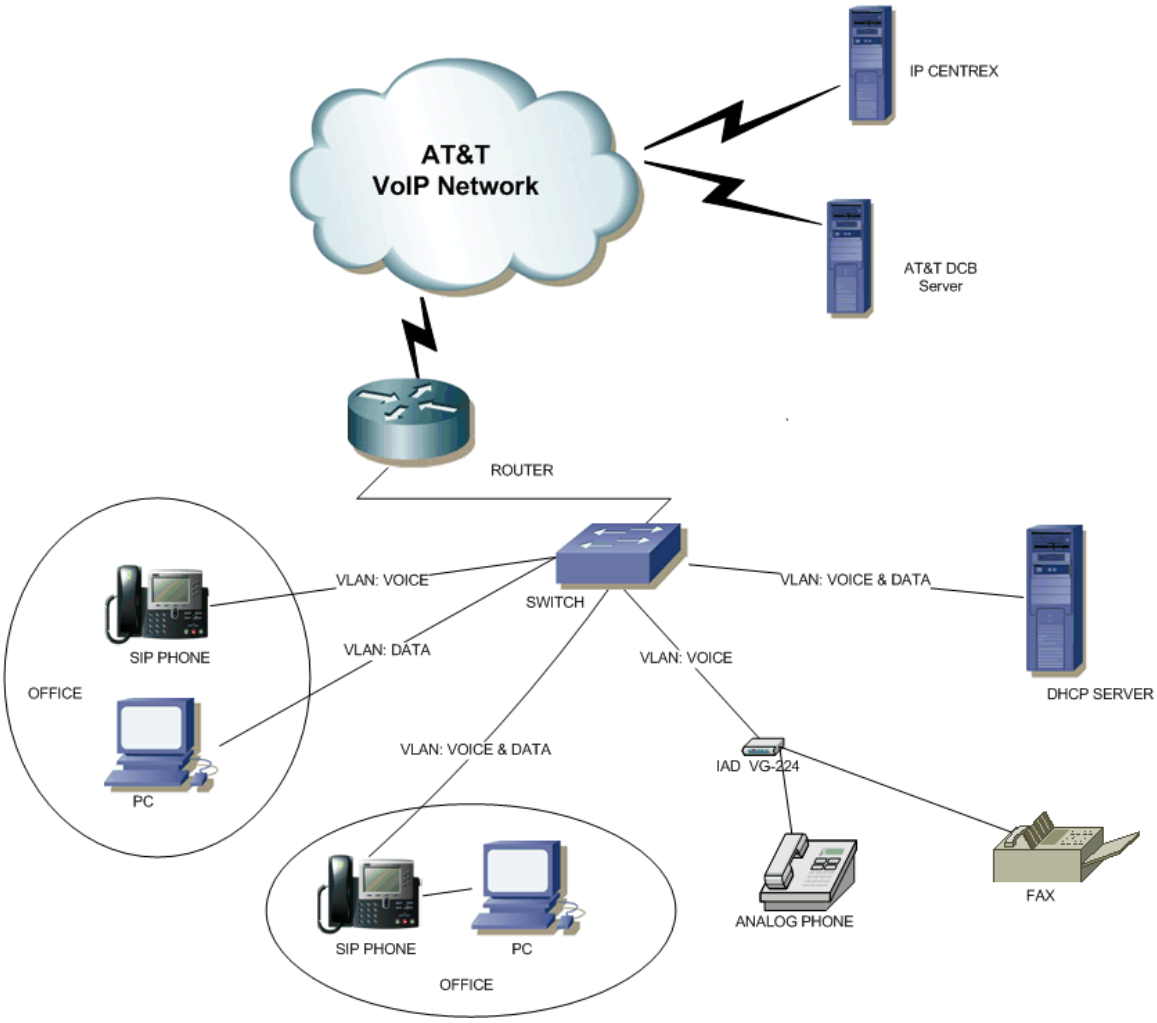


Figure 5. MIS Access with VLAN

Each SIP phone unit is directly connected via an Ethernet cable to the switch and it is required to connect PCs and phones to separate VLANs. The switch can be configured to support separate VLANs.

Analog phones are connected through an IAD (such as a Cisco VG224 or EdgeMarc 250IAD) and should be configured for the same VLAN as SIP phones.

A DHCP Server providing an AT&T Device Configuration and Bootstrapping Server option should be configured for the same VLAN as SIP phones. If there is only one DHCP server distributing DHCP addresses for the entire LAN, it may need to be configured for multiple VLANs.

4.2.5 PNT Configuration

Private Network Transport (PNT) is an AT&T MPLS-enabled VPN service. It does not provide access to the Internet. PNT customers generally do not deploy a firewall.

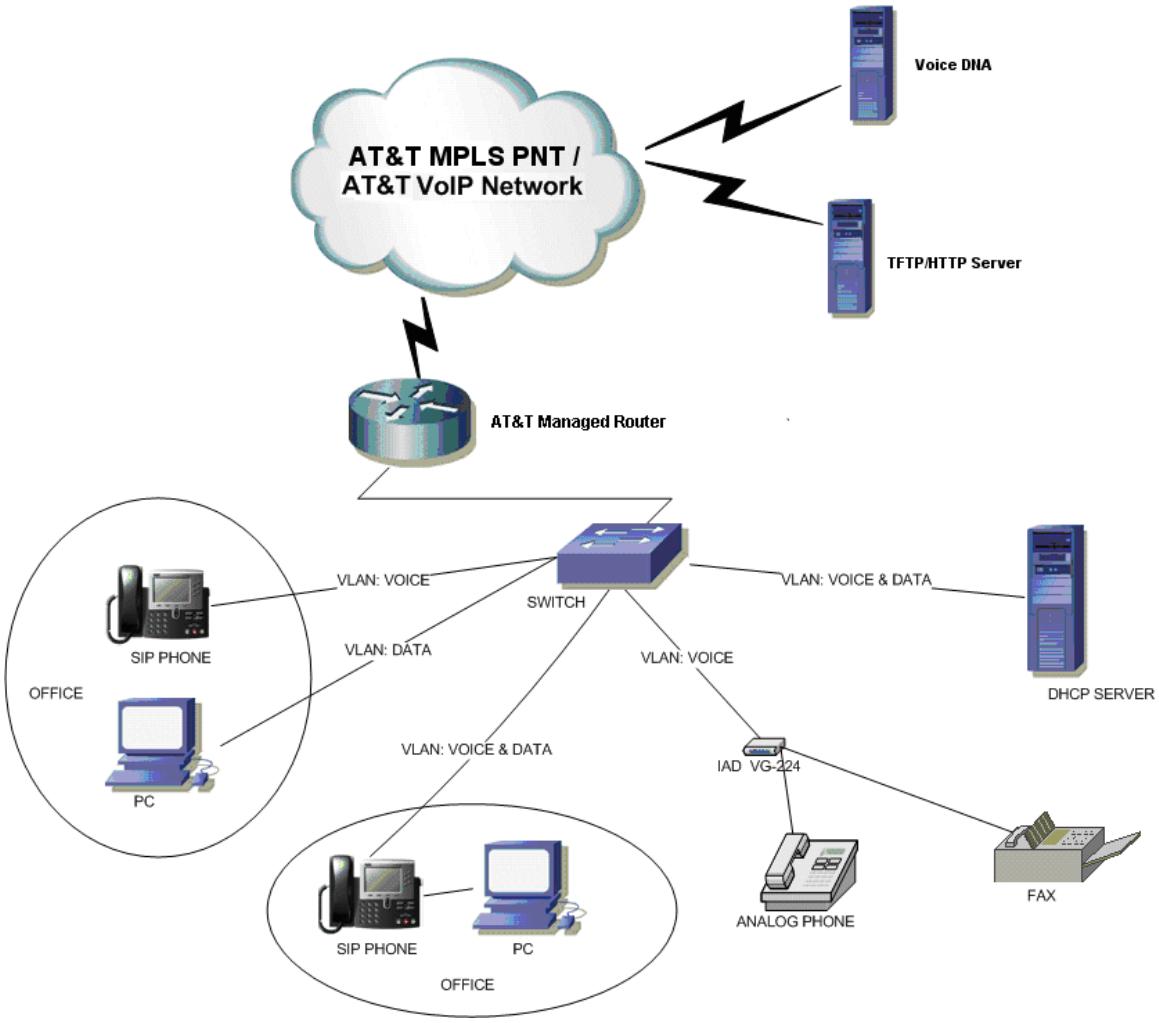


Figure 6. PNT LAN Configuration

5. Site Survivability Option (SSO)

The Site Survivability Option (SSO) is an optional feature for AT&T Voice DNA on MIS/PNT. This feature provides continuity of service in the event of a failure of your company's connectivity to the AT&T network.

This feature employs an AT&T Managed Integration Device (MID) which is an EdgeMarc router that is installed at your premises and managed by AT&T. In the

event of a failure of connectivity, the MID detects the failure and routes calls through the Public Switched Telephone Network (PSTN), until your service is restored.

The MID has been designed to detect the failure of:

- AT&T MIS or PNT circuit
- AT&T Managed router on the customer premise
- AT&T provider edge Router
- IP Border Element - IPBE
- AT&T Voice DNA application server

Specifically, the feature provides call routing under 3 scenarios:

- On-LAN calls
- Off-LAN calls over POTS lines to PSTN network
- Incoming calls on POTS lines routed to the location's Default Calling Number (DCN).

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

- Intra-site calls:
  - EdgeMarc supports calls setup between IP devices on the LAN
  - Bearer path (media – all of the voice data packets between the phones are send on the LAN) completes directly on-LAN.
- Off-net calls:
  - The number of offnet calls limited by the number of POTS lines connected to the available FXO ports (2 or 6 depending on the EdgeMarc model).
  - 911 calls prioritized
    - When all FXO ports in use, the longest duration call is dropped to allow the call to complete.

- Inter-site AT&T Voice DNA calls
  - Call is routed to PSTN via FXO port/POTS line.
  - PSTN completes call or provides treatment (e.g., busy tone or announcement)
  - Call completes only if destination site is reachable.
- Inbound PSTN calls:
  - Calls dialed using POTS line TN route to the FXO port
  - EdgeMarc routes incoming call to DCN

The EdgeMarc device will not detect other potential failures in the IP network and the PSTN. In general, these networks are designed with 99.999% reliability, are centrally monitored and supported on a 7x24 basis at the AT&T Global Network Operations Center (GNOC).

The following items describe important details of the Site Survivability feature:

- This feature is offered as an optional feature with the AT&T Voice DNA Service.
- The customer must order AT&T Professional Services with the Site Survivability option. AT&T Professional Services will install the AT&T Voice DNA service including the EdgeMarc device at the customer site. The EdgeMarc device is configured, staged, and shipped by the vendor (Edgemarc Networks) per customer's specific LAN configuration.
- AT&T recommends the customer, if enabling VLAN support, use the following naming convention:

  VLAN100 – for voice traffic

  VLAN200 – for data traffic
- There are two supported models. Both EdgeMarc devices support up to 30 concurrent calls during normal (non-survivability mode) mode. In normal mode, the EdgeMarc device is transparent to the functions of the network.
- The EdgeMarc device is managed by AT&T. AT&T provides ongoing Maintenance for the EdgeMarc device.
- The customer is responsible for purchasing the appropriate (2 for 4508T4W, 6 for 4562T4W model) number of POTS lines and ensuring that 3-way calling is ordered for all lines. All FXO ports on a device must be enabled with a POTS connection. As all ports are active you will need to order a POTS line for each FXO port.
- G.729 will be used for Voice and G.711 will be used for Fax Codec support
- Onboard firewall capability of the EdgeMarc devices will be utilized for voice calls and will be used for data traffic. If the data traffic is also going the firewall is will used.
- The DHCP capability will be provided by the EdgeMarc device instead of the customer's LAN.

- 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 the PSTN.

5.1 AT&T-Managed Integrated Device (MID)

With the Site Survivability Option, an AT&T-Managed Integrated Device (MID), is installed between the LAN switch and Managed Router at your premises. As described above, in the event of a failure of connectivity, this device detects the failure and routes calls through the Public Switched Telephone Network, or PSTN.

The MID is one of the following EdgeMarc devices:

Model	FXO Ports	FSX Ports
4508T4W	2	6
4562T4W	6	2

5.2 EdgeMarc Capabilities

- Each EdgeMarc device 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 line, or POTS line and all available lines must be connected via the POTS line in order for the Site Survivability function to be invoked.
- Each FXS port can be used as an Integrated Access Device, or IAD, to connect analog phones or faxes.

5.3 Additional Functions and Constraints

When planning for your Site Survivability implementation, keep in mind these points:

- The number of POTS lines determines the number of calls that can be supported if you lose the connection to the AT&T VoIP network.
- During survivability mode, 911 calls are prioritized and if all POTS lines are being utilized, the EdgeMarc device drops the call that has been in progress the longest in order to complete the 911 call.
- During *normal* conditions, calls *pass through* the EdgeMarc device to the AT&T VoIP network. Note that during normal operating mode or pass-through mode, the EdgeMarc device supports a maximum of 30 concurrent calls.
- In a Site Survivability configuration, the EdgeMarc device will provide DHCP capability.
- The EdgeMarc firewall capability will be used for voice calls.

5.4 Ordering POTS Lines

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

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

It is important to note that a POTS line **must** be connected to **each active** FXO port. If a port on the EdgeMarc is **not** connected to a POTS line, 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** in order for 911 calls to be completed correctly.

5.5 Service Features

In the event of a connectivity failure, many AT&T Voice DNA service features will still be available. 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.

5.6 Call Flows During Survivability Mode

For all 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 Voice DNA calls:

- EdgeMarc 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 (2 or 6 depending on the particular EdgeMarc model)
- 911 calls will be prioritized. A 911 call will cause the call in progress the longest to be dropped.

Inter-site Voice DNA calls:

- If the failure is with the originating site's Managed Internet Service/Private Network Transport (MIS/PNT) 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 TNs configured on the receiving site's EdgeMarc device will complete if ports are available.
- If the failure is with the AT&T Voice DNA Server only calls to the POTS lines 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 MIS/PNT 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 will complete. The calls are routed to the DCN and can then be forwarded by the person answering the DCN phone.

5.7 Site Survivability Configuration

Figure 7 shows a typical configuration using the Site Survivability feature.

5.7.1 Normal Condition

With the Site Survivability Option, an EdgeMarc device is installed between the LAN switch and Managed Router The EdgeMarc device is connected to the PSTN network by a number of POTS lines. The EdgeMarc device provides DHCP capability, instead of your company's LAN.

Under normal conditions, calls will pass through the EdgeMarc device, bypassing the POTS lines.

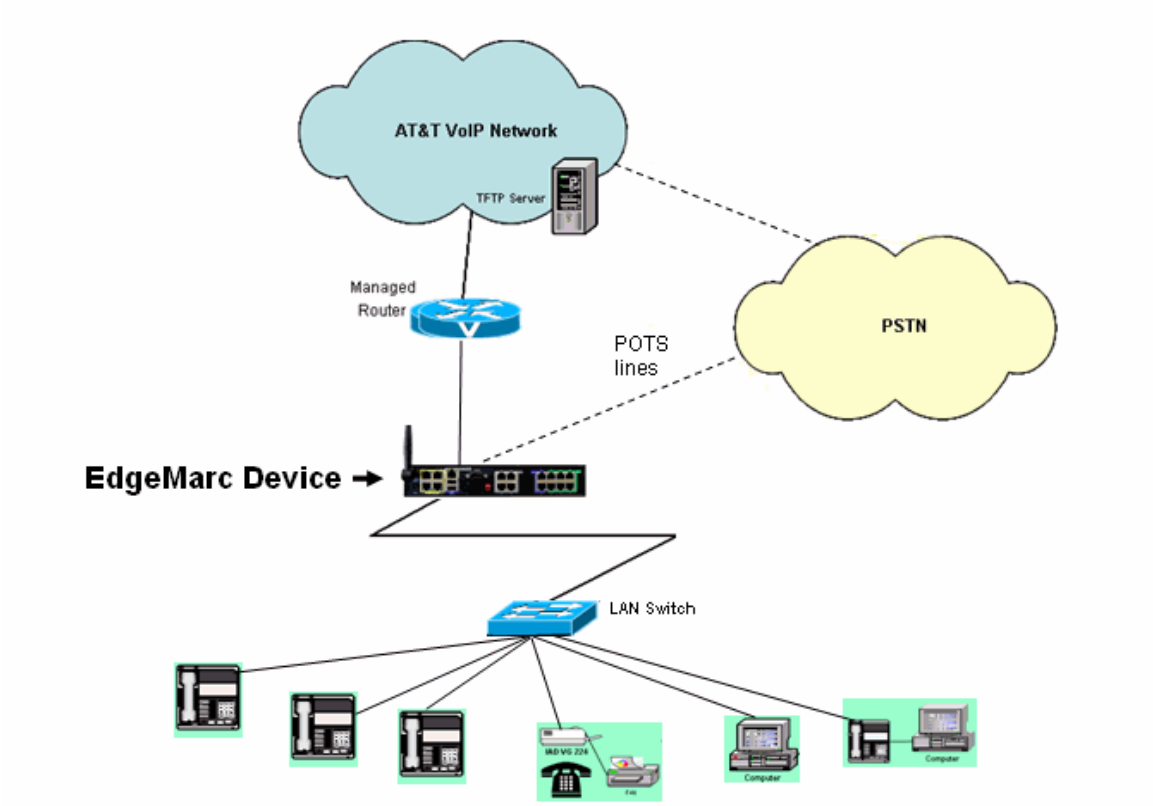


Figure 7. Site Survivability Configuration (Normal)

5.7.2 Network Failure Scenario

In the event that the network connection **fails**, the EdgeMarc device will detect the failure and begin to route calls through the PSTN.

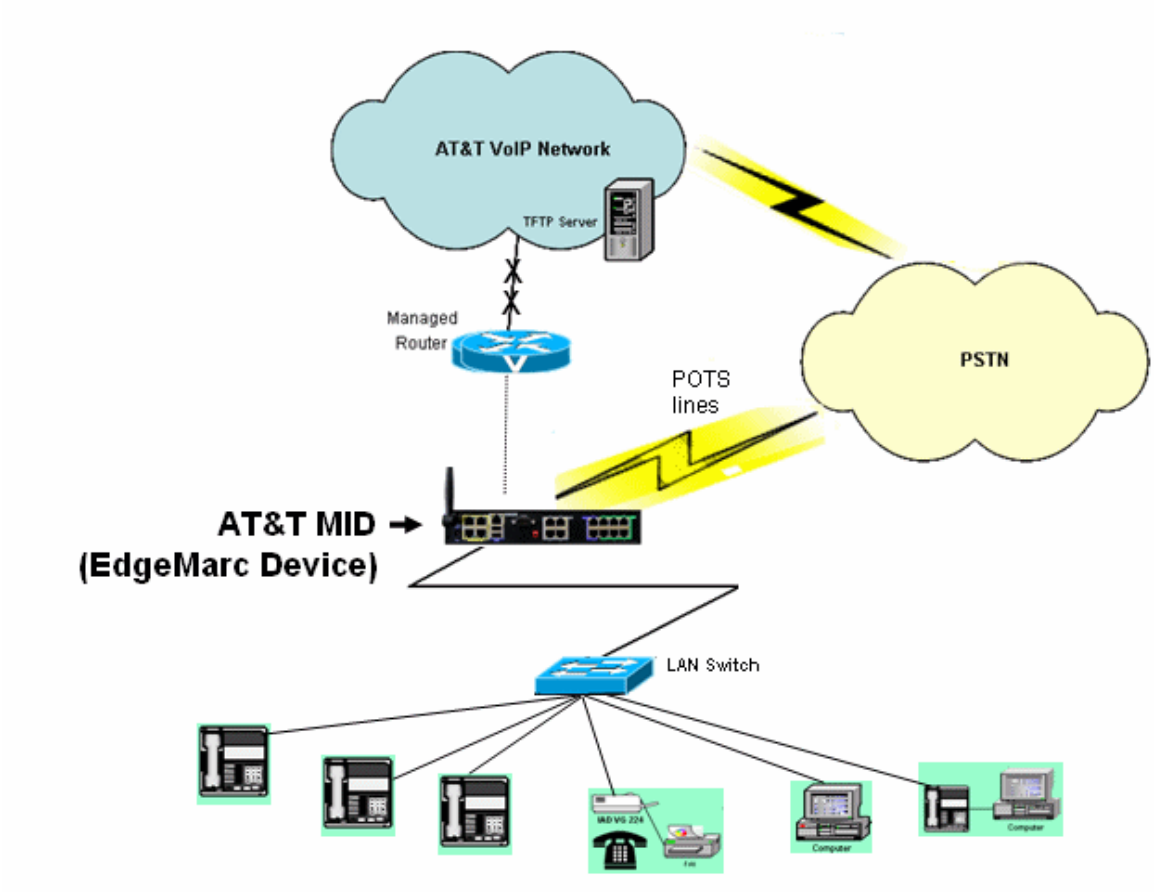


Figure 8. Site Survivability Configuration (Network Connection Failure)

5.8 Survivability Mode Phone Features

Table 3. Survivability Mode 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	Counter Path eyeBeam	**Survivable mode** Note: Feature is only available if supported by phone
Bridged Line Appearance (BLA)	√	X	√	X	√	X	X	X	X	√
Call Hold	√	√	√	√	√	Varies	√	√	√	√
Call Logs	√	√	√	√	√	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 handset	√	√	√	√	X	√	√	√	√
Direct Outward Dialing (DOD)	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	√
Multiple Line Appearances — Repetitions	√	X	√	X	√	X	X	X	√	√
SIP Forking	√	√	√	√	√	X	√	√	X	√* * Limited to BLA functionality for LAN
Station to Station Dialing	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	Ind	√

Index

—A—

About This Guide – 1
ASA firewall – 12
ASA FIREWALL – 15
AT&T Device Configuration and Bootstrapping (DCB) Server – 6, 9, 14, 16
AT&T Device Configuration and Bootstrapping Servers – 9
AT&T-Managed Integrated Device (MID) – 20
Audience – 1

—C—

Call Flows During Survivability Mode – 23
CAT3 UTP cable – 12
Contents – 1
Customer Managed Firewall – 7

—D—

Definitions of Terms – 13
DHCP – 5, 13, 16
DHCP options – 5
DHCP Servers – 5
DMZ – 12, 15
Dynamic Host Configuration Protocol – 13

—E—

EdgeMarc Capabilities – 21
Ethernet switch – 12

—H—

Hubs – 11

—I—

IAD – 13
IAD (Integrated Access Device) – 13
Integrated Access Device – 13
Introduction to the Voice DNA Service – 2

—L—

LAN – 13
LAN – 13
LAN Switches approved for use with AT&T Voice DNA Service – 10

—M—

Managed Customer Edge Router – 13
MIS Access with ASA Firewall – 14
MIS Access with DMZ – 15
MIS Access with VLAN (Recommended) – 16

—N—

NATing for Voice DNA – 9
Network Address Translation – 9
Network Address Translation (NAT) – 9, 12
Network Configuration and Planning – 4
Network Configurations – 12
Network Planning Considerations – 4

—O—

Other Networking Considerations – 12
Overview of the Voice DNA Installation and Turnup Process – 3

—P—

PIX firewall – 15
PNT Configuration – 17

—R—

Router – 13
Routers – 12

—S—

Site Survivability Option (SSO) – 17
SSO - Additional Functions and Constraints – 21
SSO - Network Failure Scenario – 25
SSO - Normal Condition – 24
SSO - Ordering POTS Lines – 22
SSO - Service Features – 22
Survivability Mode Phone Feature Matrix – 26
Switches – 9

—T—

Turnup process – 3
Typical Network Configurations – 12

—V—

VLAN – 12, 16
Voice DNA Personal Web Sites, Administrator Tools, and User Guides – 2
Voice over Internet Protocol – 2
VoIP – 2