IED Network Requirements

Introduction

IED's dependence on end-user network installations has greatly increased. With the Introduction of the GLOBALCOM vACS, enhancements to the 510ACS, Titan Distribution, IP Paging Stations, Enterprise and Visual Information Systems, properly certified and documented network cabling has become more important than ever.

In preliminary summarization, IED requirements are very simple and somewhat non-typical. In most systems from small to large, IED needs (1) One Managed VLAN operating on Layer 2 and considered flat with QoS Guaranteed service (also called hard QoS). Latency from point to point should not exceed 3.4ms. No Routers are allowed due to the complex use of technology from Cirrus Logic known as CobraNet. This technology operates only on Layer 2 and cannot be routed. In extremely large systems the use of multiple VLANs are recommended.

The GLOBALCOM vACS now allows the use of Layer 3 routing to connect audio between GLOBALCOM systems. The devices within each GLOBALCOM system will still be limited to Layer 2 for Cobranet but the GLOBALCOM units will then handle the conversion to a Layer 3 (RTP) protocol that can be routed across VLANS to link GLOBALCOM systems. RTP is described in more detail later in this document. Please consult the factory for advice on systems which require the use of multiple VLANs or audio routing using RTP on Layer 3.

The balance of this document is intended to offer more specifications and requirements. They are intended for your project's Network Engineer's use. Please forward as needed.

IED Equipment Terms & Definitions

- ***500ACS/510ACS*** – 500 Series Announcement Control System: All aspects of the paging system are managed by the ACS 510CPU or 520CPU.

- ***520CPU, 510CPU*** – The CPU processor and hard drive in the 500/510ACS. Project may or may not have a redundant CPU.

- ***510N*** – CobraNet Network Interface Card used in the 500ACS/510ACS which routes broadcast quality audio dynamically routed between all network audio devices. Technology is from Cirrus Logic and known as CobraNet.

- ***GLOBALCOM vACS*** – GLOBALCOM Series Announcement Control System: All aspects of the paging system are managed by the GLOBALCOM controllers.

- ***ACS 591 Server*** – The system server that supports the database for the entire system and provides underlying services for system operation and management. It also provides web services for any browser applications and may be redundant.

- ***ACS 591 Client*** – For extending system operations of the server to remote office or additional ACS Locations.

- ***591 DDC*** – Digital Display Controller
- ***T-CAS*** – Courtesy Announcement System Application that may include a Text-to Speech Engine.
- ***VIS*** – Visual Information System. This may include visual paging, flight information display, gate information display, etc.

Network Requirements

IED is not responsible for the network cable or installed cable plant. Therefore we have no requirements other than a fully operational and correctly installed cable plant to the applicable adopted standards which govern this industry. Please be advised that failure of the paging system due to improperly installed cable plant is not considered an IED failure and we reserve the right to be compensated for engineering time spent to Troubleshoot, Consult, and/or repair the network cable plant.

IED requires printed or electronically transmitted copy of testing results of the installed cable/fiber plant and to forward to IED for review prior to Site Visit. These test results should include Connectivity, Loss, OTDR tests. All Cable Plant shall meet or exceed the Performance Standards Adopted by the industry or authority having jurisdiction. Please request a copy of "Network Testing Standards for IED Systems" if you need further information on testing requirements.

Ethernet Switches

High quality Ethernet Switches are necessary for reliable performance. Consumer and value-priced commercial switches are practical only when longer latency, dropped frames, or full buffers are not noticeable. Regular business applications, internet browsing, files transfers, etc. can tolerate limited performance from the switches and network; our audio network cannot.

With an Networked IED PA system, Network switch quality is critical for reliable performance. The switches must support the following features:

- Non-Blocking Switch Fabric Speed (Backplane speed)
- Allows assignment of switch IP addresses for Remote Monitoring and Configuration via GUI interface
- Allows assignment of Manual Port Speed and Negotiation
- Supports VLAN's and Tagging
- Supports Port Monitoring Capability
- Supports Quality of Service
- Supports Spanning Tree Protocol
- Allows Manual Configuration of the MAC Aging Timeout (IED recommends a setting of the maximum amount of available limits, preferably unlimited)
- Allows deactivation of the Link Aggregation Control Protocol (LACP) which is known to cause interference in networks environments that rely on multicasts for system communication.

- Support multicast and Unicast filtering of ports. **Note:** This is **Port Based Filter** and will only be required on devices which are not utilizing the CobraNet Audio or control.
- Includes a minimum of 32Mb of Ram for Data Buffering

Depending on the size and complexity of the network, switches may be designated with one of up to three “roles”: Core, Intermediate, & Edge.

- **Core** – The core switch is located at the ER or MDF. The system Server and an ACS will normally be directly wired to this switch. This switch will connect to other switches at a speed of at least 1000Mbps (1Gbps).

- **Intermediate** – Intermediate switches are often found in larger, more complex networks. There are two advantages to using intermediate switches. The first is to extend the media beyond its maximum distance. The second is to increase the manageability of the network by breaking down logical or physical segments. The presence of intermediate switches almost always represents a Hierarchical Star Topology. Additional ACS’s would normally be installed directly connected to an Intermediate Switch.

- **Edge** – The edge switch is so named because it typically resides at the outer “edge” of a network. The actual devices, such as microphone paging stations and Titan network power amplifiers are connected here

Regardless of the role the switch plays in the overall network design, there are specific requirements it must meet.

1. **Managed Switch** – A managed switch can be assigned an IP address to make monitoring and configuration easier.

2. **Port Configuration** - Manual port speed and negotiation settings. It is often necessary to manually set the port speed on certain devices to ensure proper communication.

3. **VLANs -** VLAN creation and assignment for segregating traffic to its own “network” inside the switch. If a dedicated network is not available or feasible, then a VLAN becomes a requirement. In a shared network environment the IED system must be on it’s own VLAN(s).

4. **Port Monitoring** - Port monitoring or “mirroring” gives an administrator the capability to watch traffic on a specific port. This helpful when try to troubleshoot network communication issues.

5. **QoS** - Quality of Service (QoS) allows specific protocols or switch ports a higher priority on the network. This ensures that crucial traffic, such as voice data and/or CobraNet, is delivered without any transmission retries or packet loss. IED must have QoS Guaranteed service (also called hard QoS).

6. **Spanning Tree Protocol** - Spanning Tree Protocol (STP), also known as meshing, provides redundant paths for fault tolerance. One path has a higher priority than the other. This priority makes sure that only one path is open for data travel at a time, avoiding network loops, also known as broadcast storms. This allows for a more simplified configuration deployment.

7. **Switch Memory** - A minimum of 32Mb RAM allows for data buffering and contributes to the overall efficiency of the switching fabric.

8. **Layer 2** – Switches by nature are layer 2 however it must be noted that the Technology IED uses from Cirrus Logic, known as CobraNet, operates only on Layer 2.

Virtually any Layer 3 switch can meet the requirements listed above. IED recommends the use of Cisco 29xx (or higher) series of switches.

Endpoint Devices

Endpoint devices, or just endpoints, refer to components that involve some sort of user interaction. Examples are computer workstations, IED 528 Series Paging Stations, and Titan Distribution Devices. Typically, endpoints are connected to the LAN through an edge switch. Each endpoint is connected to the network switch using UTP certified to Category 5e standards or better.

Endpoints also require power to operate. 528 and/or 524 Paging Stations and Titan Collector devices such as the T9032NS, T9016RY, T9032LVIO, T9040NLR etc do not receive power in the conventional fashion. Instead a PoE switch port provides power using the UTP network cable. This power must meet IEEE/ANSI 802.3af standards or be connect to a separate modular power supply.

Logical Topology

Logical topology deals with how the components of a LAN are configured and utilized, rather than their physical location. A well thought-out logical topology will greatly improve LAN manageability. Expansion and troubleshooting can also benefit from this proper planning.

Naming Conventions

Proper device naming is critical to LAN management. Naming occurs at two levels: Switches are named using their proprietary interface. See the switch manufacturer's documentation for specific instructions. When naming a device, use something that denotes the device's location. However, keep in mind that names are limited to a total of 15 characters. IED recommends keeping the end user in mind during the development of this naming convention. This simplistic approach allows for long-term ease of understanding.

For example: An edge switch is located in the East Wing, 2nd Floor, and closet 206. Its name could be "E-WING-F2-C206" which fully describes the location in less than 15 characters.

After deciding on a naming scheme, make sure it is fully documented and that all device names are clearly labeled on the component itself as well as recorded electronically in a spreadsheet, drawing, etc.

IP Addressing

Since IP addresses define whether devices on a LAN can communicate with each other, it's imperative that these are assigned properly. IP addresses can be assigned using one of two methods: Static and dynamic addressing. In an IED Paging System, all IP addresses are Static or assigned by the ACS(s) within the address range assigned to the paging system. We also recommend a plan for facilitating all the devices in some plan. In Small Systems this will be much simpler as the entire system will live in one octet. In Larger systems it may be better to setup several octets in the same VLAN.

Examples of IP structure on the same VLAN

10.200.240.101 through 200 for Mic Stations
10.200.240.020 through 099 for 9160's, 9032NS, 9032LVIO's, 9032RY, 9040NLR's at the Endpoints
10.200.240.002 through 10 for MDF Central Equipment (Main ACS Equipment)
10.200.240.201 through 255 for Non-IED Network Equipment/Switches/Array Speakers and such
10.200.241.001 through 255 for Visual Devices such as DDC's, GIDS, FIDS, BIDS, and similar equipment.

Another example would split the IP's to allow for easy location verification, again all in the same VLAN.

10.200.240.001 through 255 for Terminal A
10.200.241.001 through 255 for Terminal B
10.200.242.001 through 255 for Terminal C
10.200.243.001 through 255 for Landside
10.200.244.001 through 255 for Customs
10.200.245.001 through 255 for TSA

VLANs

A VLAN is an effective way to segregate devices and their data traffic on a network. VLANs can provide increased security since their components are not discoverable from other networks.

In addition to increasing security, VLANs keep data isolated between networks. In order for data to travel from one VLAN to another, it must be routed. This is not typically possible due to the use of CobraNet which transports audio on a dynamic basis via Unicast and Multicast network traffic. Multiple VLANs can be supported, and cross-VLAN communication can be accomplished through Layer 3 routing by utilizing correctly configured RTP. The Multiple VLANS will be required to be available at each network switch at each ACS equipment room.   This optional equipment may not be part of your project and may be required. Please consult your IED Applications Engineer for additional information.

Protocols otherwise known as PORTS

The following table illustrates network protocols necessary for an ACS installation to properly function:

Protocol	Description	Type	Port Number(s)
HTTP	Standard web protocol for communicating between ACS Server and client PCs. Used with T-CAS product.	TCP	80
IEDNet	Proprietary protocol for data communication between endpoints and their associated ACS.	UDP	3048,3049
SNMP	Simple Network Management Protocol. Used for network device discovery.	UDP	161,162
ICMP	Allows network "ping" to other devices.	TCP/UDP	7,8

Other network protocols and ports may be required depending on the remote access software that is utilized.

Bandwidth

At a minimum, the bandwidth between switches must be at least 1Gbps. Bandwidth requirement to endpoint devices is 100Mbps. Latency cannot exceed 3.4ms between points. Any 10Mbps device connections will become oversaturated by CobraNet traffic, causing data loss. Slower links should be segregated from the audio traffic by VLANs or protocol filtering. As defined by Cirrus Logic, there can be no more than six (6) network "hops" between source and destination communication points.

Audio Communication

Audio is transmitted and received on the LAN or VLAN using the CobraNet protocol. CobraNet is an audio networking technology for delivery and distribution of real-time, high quality, uncompressed digital audio using a standard Ethernet network. It is implemented using a combination of hardware, firmware, and the CobraNet protocol.

In addition to the high degree of audio routing flexibility that CobraNet provides, the technology also incorporates the ability to monitor and control CobraNet devices remotely.

CobraNet provides this capability by implementing Simple Network Management Protocol (SNMP). SNMP is a standard protocol typically used for monitoring network devices such as Ethernet switches. In the case of CobraNet, it allows users to communicate with any CobraNet device using standard SNMP tools.

For further information visit about the CobraNet Protocol, http://www.cobranet.info.

Bundles & Packets

Over CobraNet, all audio channels are packaged into groups called Bundles for transmission over the Ethernet network. A bundle can contain from one to eight audio channels.

A CobraNet system is coordinated by one of the devices called the conductor. When two or more CobraNet devices are interconnected properly, one of the devices will be elected the network conductor based on a priority scheme.

Each CobraNet device has the ability to send and receive a fixed number of Bundles. The Bundle number tells the CobraNet conductor which specific CobraNet device is trying to communicate with which other CobraNet device(s) over the network. Use of Bundle numbers removes the necessity of the user having to tell the devices the Ethernet hardware addresses of the other devices with which it is trying to communicate. As long as the CobraNet devices are all set to the same Bundle number, the CobraNet system takes care of the rest of the technical details of setting up an audio path over Ethernet between the devices.

A given Bundle can have only one transmitter that places it onto the network. Unicast Bundles may have only a single receiver. Multicast Bundles may have multiple receivers.

The CobraNet protocol operates at the Data Link Layer (OSI Level 2). CobraNet uses three basic packet types. All packets are identified with a unique protocol identifier (0x8819) assigned to Cirrus Logic. CobraNet does not transport audio as IP traffic. CobraNet is a Local Area Network (LAN) technology not a Wide Area Network (WAN) technology. This means that CobraNet packets will not pass through a router.

CobraNet data consists of one of the following packet types:

- **Beat Packet –** These packets contain network operating parameters, clock and transmission permissions. The beat packet is transmitted from a single CobraNet device on the network and indicates the start of the isochronous cycle. Since the beat packet carries the clock data for the network, it is sensitive to delivery delay variation. Failure to meet the delay variation specification may prevent devices from being able to lock their local sample sync to the network clock. The beat packet is typically small (100 bytes) but can be large on a network with numerous active bundles, reaching a maximum size of approximately 1500 bytes on a very busy system.

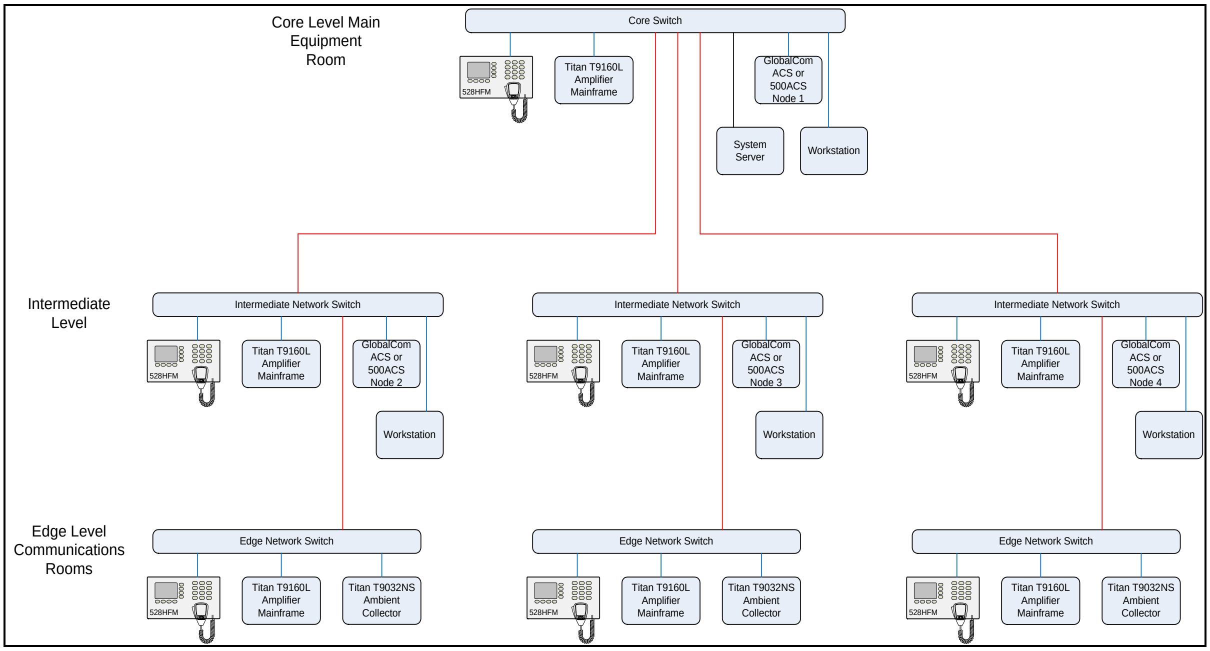
- **Isochronous Data Packet -** Multicast or unicast destination addressed (depending on number of destinations and bundle type). Buffering is performed in the CobraNet devices thus out of order delivery of data packets is acceptable. To keep overhead in check, data packets are typically large (1000-1500 bytes).

- **Reservation Packet -** CobraNet devices typically transmit a reservation packet once per second. On networks with large numbers of Cobranet devices (over 100), the reservation packet transmissions are slowed down to once every 8-10 seconds. The reservation packet is never large.

Forwarding Delay

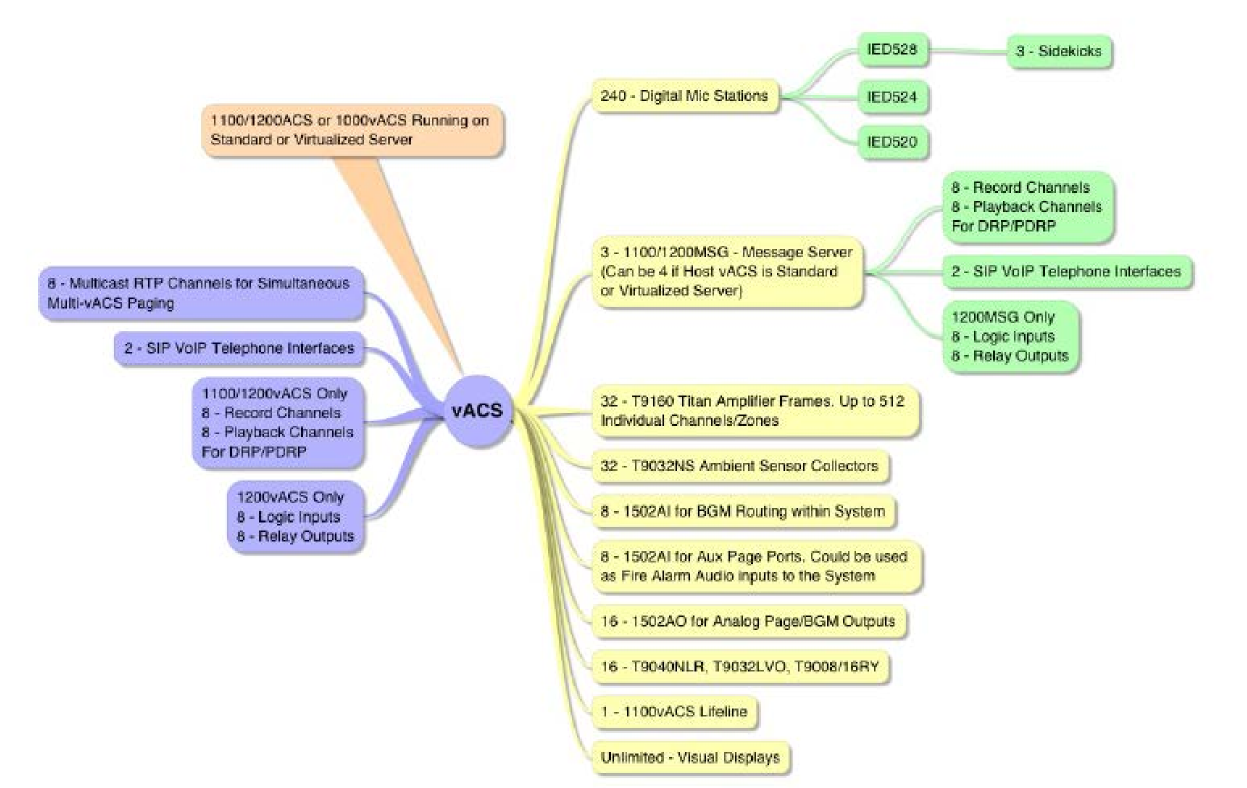
Proper operation of CobraNet depends on basic CobraNet timing specifications. Every time an Ethernet frame (CobraNet bundle or beat packet) traverses a switch, some forwarding delay is introduced**. It is important that the aggregate delay from any two points on the extremes of the network diameter not exceed the maximum allowed delay of 3.4ms.** Operating beyond the recommended six (6) switch hops introduces the potential to exceed the maximum allowable delay of 3.4 ms.

Sample Network Diagram


Core Level Main Equipment Room
Core Switch
528HFM
Titan T9160L Amplifier Mainframe
GlobalCom ACS or 500ACS Node 1
System Server
Workstation
Intermediate Level
Intermediate Network Switch
Titan T9160L Amplifier Mainframe
GlobalCom ACS or 500ACS Node 2
GlobalCom ACS or 500ACS Node 3
GlobalCom ACS or 500ACS Node 4
Workstation
Edge Level Communications Rooms
Edge Network Switch
Titan T9032NS Ambient Collector

The diagram above shows a facility network laid out in a Hierarchical Star topology. In this example, the distances between the core and intermediate switches exceed 100 meters, requiring the use of fiber. The same is true of the distance between the intermediate and edge switches. The Console PC and microphone station are connected to an intermediate switch because of its proximity to the admin office where the equipment is located. *Note: Many installations will not utilize intermediate switches. They are shown here for illustrative purposes only and not as a requirement.*

Basic System Capacity


1100/1200ACS or 1000vACS Running on Standard or Virtualized Server
8 - Multicast RTP Channels for Simultaneous Multi-vACS Paging
2 - SIP VoIP Telephone Interfaces
1100/1200vACS Only 8 - Record Channels 8 - Playback Channels For DRP/PDRP
1200vACS Only 8 - Logic Inputs 8 - Relay Outputs
vACS
240 - Digital Mic Stations
IED528
3 - Sidekicks
IED524
IED520
3 - 1100/1200MSG - Message Server (Can be 4 if Host vACS is Standard or Virtualized Server)
8 - Record Channels 8 - Playback Channels For DRP/PDRP
2 - SIP VoIP Telephone Interfaces
1200MSG Only 8 - Logic Inputs 8 - Relay Outputs
32 - T9160 Titan Amplifier Frames. Up to 512 Individual Channels/Zones
32 - T9032NS Ambient Sensor Collectors
8 - 1502AI for BGM Routing within System
8 - 1502AI for Aux Page Ports. Could be used as Fire Alarm Audio inputs to the System
16 - 1502AO for Analog Page/BGM Outputs
16 - T9040NLR, T9032LVO, T9008/16RY
1 - 1100vACS Lifeline
Unlimited - Visual Displays

Legend

- **Included with vACS**
- **Audio Input/Output and Aux Devices**
- **Device Specific Data**
- **Comments**

Multi-vACS/Legacy ACS Communication

Multi-vACS Communication

Audio Communications between vACS systems is accomplished via full-bandwidth networked audio. For systems residing on the same LAN/VLAN, CobraNet may be used for this. Between systems on separate LAN's/VLAN's, IED uses layer 3 RTP audio over IP. Up to 8 channels per vACS are available for simultaneous transmission of RTP audio. Because Multicasting is used as the transport method, only one channel is used by the sending and receiving device regardless of the number of vACS systems that are receiving the audio transmission. For example; One vACS can simultaneously send an audio stream to two or more remote vACS devices and it is still only utilizing one channel.

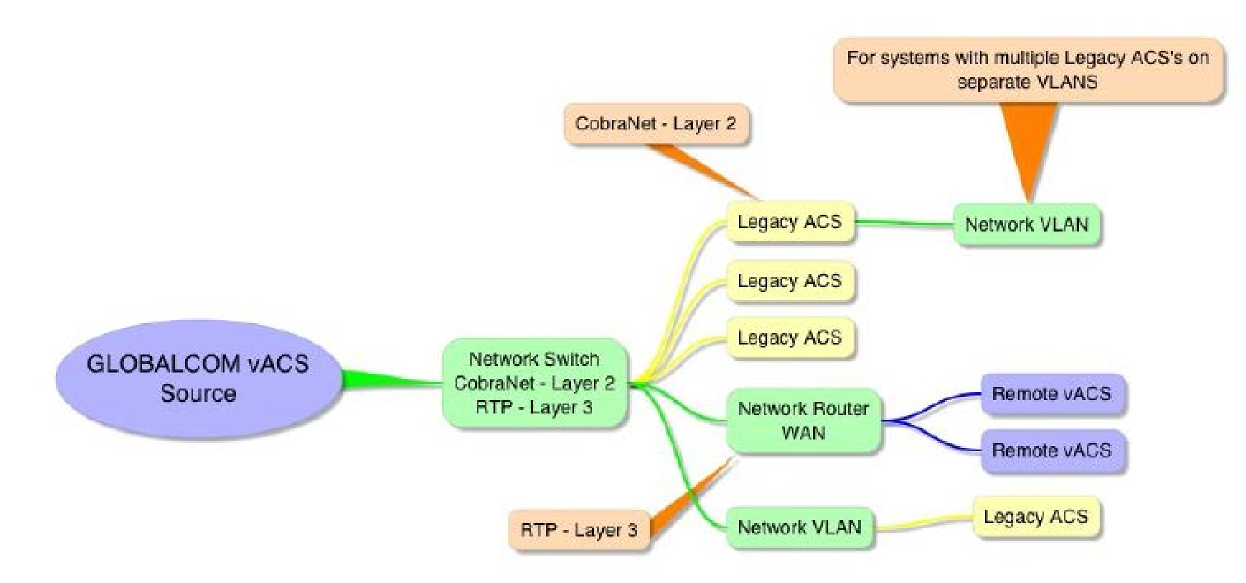
* The number of vACS's that can be connected together for paging over a wide area network (WAN) is limited only by the network. In all cases, a qualified network engineer should be consulted to determine practical limits for the specified equipment.

vACS-Legacy ACS Communication

If installing a vACS into a facility with an existing 510ACS the vACS MUST BE CONNECTED TO THE SAME LAYER 2 NETWORK to facilitate CobraNet audio transmission between the vACS and the 510N card of the legacy ACS.

* There are several factors that contribute to the practical limit of vACS to Legacy ACS connections including but not limited to Network Topology, Bandwidth and Total Number of CobraNet Devices on the LAN/VLAN.

Sample Multi-System Layout



Multi-vACS Multicast System Requirements

For vACS <—> vACS audio transport between VLANs, IP Multicast is used. This enables one vACS to source audio that may be received by {n} receivers. There are prerequisite network equipment and configuration which must be in place. Each vACS has up to 8 separate paging channels. In the vACS Configuration Console, these are called RTP Transmitters. Each RTP Transmitter requires its own Multicast Group to function.

Switches

Switches must support IGMP. The current standard is IGMPv3, but versions 1 and 2 are compatible.

Multicast Router

To route multicast traffic between subnets and maintain multicast group membership lists, a multicast capable router is required. If more than one router is necessary, the routers must communicate multicast information to each other. This is typically done using Protocol Independent Multicast (PIM). There are several types of PIM. One common type is Sparse Mode, typically referred to as PIM-SM.

Multicast Groups

Multicast groups are generated using Class D network addresses (224.0.0.0 – 239.255.255.255) in combination with a port number. In a VLAN situation, 224.0.0.X addresses cannot be used. The default vACS multicast group is 239.192.0.x where x is the system number.

The RTP port number is used along with the multicast group IP address to uniquely identify the audio channel. The default port number is calculated using the following formula:

4000 + (1000 x {system number}) + {ID}

For example, transmitters 1 and 2 on system 1 would use ports 5001 and 5002. Transmitters 1 and 2 on system 2 would use ports 6001 and 6002.

Example Default Configuration for a 2-vACS System

System 1	System 2	System 3
239.192.0.1:5001	239.192.0.2:6001	239.192.0.2:7001
239.192.0.1:5002	239.192.0.2:6002	239.192.0.2:7002
239.192.0.1:5003	239.192.0.2:6003	239.192.0.2:7003
239.192.0.1:5004	239.192.0.2:6004	239.192.0.2:7004
239.192.0.1:5005	239.192.0.2:6005	239.192.0.2:7005
239.192.0.1:5006	239.192.0.2:6006	239.192.0.2:7006
239.192.0.1:5007	239.192.0.2:6007	239.192.0.2:7007
239.192.0.1:5008	239.192.0.2:6008	239.192.0.2:7008

* The multicast address and/or port can be changed to match a customer’s networking requirements.