



This Document Is Intended To Be Viewed In PDF Format

Rev 2023-1.04

Preparation for Valcom Engineered Solutions IP Emergency Mass Notification and Intercom Systems

Don't Delay Cutover- Deliver this document to the Network Administrator and Installation Crew IMMEDIATELY

Reading this document before beginning system installation will save you time, money and effort.

Valcom does not manufacture, specify, or endorse specific network switching hardware. We do specify network speed, port access and protocols that will be required for successful operation of your Valcom system. Your network may be comprised of simple un-managed PoE switches or may involve numerous routers and multiple types of infrastructure including wireless and fiber connectivity. What is of utmost importance is that your networks comply with the network requirements herein.

This document provides prerequisite steps to preparing for installation of a Valcom Engineered Solutions VoIP communication system. The information in this document should be provided to all parties involved in the project. Network preparation for many government and secure private networks often require additional time due to scrutiny of those tasked with protecting the network.

Note that if you plan to use a simple dedicated network comprised solely of unmanaged PoE switches that natively support the protocols required for Valcom devices (802.3 PoE, multicast, etc.), and your system will not require routing to additional networked resources (NTP, DNS, Mail Servers, etc.), then no additional network preparation will be required.

Table of Contents

INTRODUCTION	3
NETWORK REQUIREMENTS FOR MANAGED VOIP	5
DEFAULT DHCP	6
VIP STATUS MONITOR	7
NETWORK MANAGEMENT	7
NETWORK SECURITY	7
INTERNET AND MAIL SERVER ACCESS	7
POE.....	8
MULTICAST	8
MULTICAST SECURITY MYTHS	9
DIFFERENTIATED SERVICES CODE POINT (DSCP)	10
SPANNING TREE¹	10
BROWSER CHOICES.....	11
SECURITY	11
LIVE ANNOUNCEMENT ACCESS	11
SIP (SESSION INITIATION PROTOCOL)	11
NON-SIP TELEPHONE ACCESS	11
SERVERLESS DESIGN	12
MULTI-FACILITY SYSTEMS	12
GLOBAL ANNOUNCEMENTS	13
INITIAL ONSITE CHECKLIST	14
INSTALLATION CHECKLIST	14
INITIAL SYSTEM SETUP CHECKLIST	15
SYSTEM BALANCING AND VERIFICATION CHECKLIST.....	18
VIP-102B GROUP PRIORITIES VS. SERVER GROUP PRIORITIES.....	19
INITIAL AUDIO LEVEL SETUP.....	19
PRIORITY OVERRIDES.....	21
VE602X/VE6030 PORT REQUIREMENTS	22
VIP-102B IP SOLUTIONS SETUP TOOL NETWORK COMMUNICATIONS	23
VE602X/VE6030 SERVER NETWORK COMMUNICATION.....	24
VE6023 SERVER NETWORK COMMUNICATION (AVAYA).....	25
VE6023 SERVER NETWORK COMMUNICATION (CISCO)	26
VALCOM V-ALERT MOBILE APP NETWORK REQUIREMENTS	27
VIRTUAL VEXXX SERVER HARDWARE REQUIREMENTS.....	27

Introduction

Valcom IP Mass Notification/Intercom systems differ from analog wired systems in numerous ways.

Using the IP network to support facility systems, including mass notification and intercom has caused the role of Network Administrator to gain increased prominence in every professional and government organization. One reason for this is the fact that hosting facility systems on a LAN/WAN provides many benefits, not the least of which - long term cost savings. Managing multiple IP based systems typically requires fewer personnel due the fact that most adjustments and diagnostics may be performed remotely. That means less time lost driving to sites, fewer service vehicles required, less vehicle insurance cost, less fuel cost, and more multitasking.

Unlike analog systems, Valcom IP Mass Notification/Intercom systems do not require a central control system. They are hosted on the LAN/WAN, therefore the physical location of endpoints and their proximity to each other is irrelevant. Also, unlike analog systems, system size constraints are essentially non-existent. These systems are easily deployed on a facility, enterprise and/or global scale.

Valcom's server-less design means that if properly configured network connectivity exists between endpoints, they will be able to communicate. This robust, redundant strategy coupled with inherent supervision, explains why Valcom IP Mass Notification/Intercom systems are utilized in some of the most vital facilities in the world.

A full complement of one way or intercom POE speaker and horn endpoints are available to suit any area. These speakers and horns may be selected in any combination conceivable for announcements to a single area, multiple areas, or everywhere. Access may be via single line POTS type telephones, FXO ports, loop start C.O. line ports, loop start trunk ports, SIP, microphone or analog station ports (FXS) featuring [Open Loop Disconnect](#).

Visual notification endpoints, such as LED displays, may easily be incorporated into your design to deliver messages to high noise areas, to benefit hearing impaired individuals, or anywhere that visual alerting is desired.

Input/Output [gateways](#) allow users to launch messages from panic buttons or automatically from 3rd party monitoring devices. They also provide switch outputs to control electric door locks, lighting or any other facility system.

Audio gateways allow the introduction of music, microphone or other external audio sources. They may also provide audio outputs to facilitate integration of existing legacy analog paging systems, radio systems, etc.

Although the Valcom IP Mass Notification/Intercom systems feature a server-less design, there are Application servers available to provide desirable features.

Telephone Paging Servers allow the broadcast of system announcements through the speakers of many existing IP telephones. This simple addition adds audio coverage to private offices and other areas that may not be close to a system speaker.

Application Servers may be added to provide scheduled tones, music, prerecorded or live announcements. They also provide a graphical browser interface to launch messages or monitor call status. Application servers feature the ability to monitor data feeds such as syslog, RSS, ATOM or CAP feeds to automatically launch one or more messages to speakers/horns, IP telephone speakers, text to LED signs, as well as screen pop ups on PCs. All the messaging modes may be simultaneously initiated from a single user action.

Advanced Servers allow users to launch their own emergency announcements via CAP, RSS and/or ATOM feeds. This allows the incorporation of any system capable of responding to such feeds.

All servers have a high availability option.

The key to successful deployment of a Valcom IP Mass Notification/Intercom System lies in the preparation.

Network Requirements for Managed VoIP

Hardware requirements:

10/100 Ethernet

Bandwidth requirements:

86 kbps per active One-Way Page

172 kbps per active Two-Way Call

TCP requirements:

Port 21 for FTP

Port 22 for SSH

Port 23 for Telnet

Port 53 UDP/TCP for DNS resolution

Port 80 (or 443 if using SSL) for Web based access

Port 8883 for MQTT over TLS (for use with Valcom Early Earthquake Warning System (VEEWS))

Additional ports are required when using the VE6023. These vary by telephone system.

UDP requirements:

7 Bi-directional Ports: 4097, 4098, 4099, 4120, 4121, 4122, 4197, 123 (for NTP)

The addition of Multicast-to-Unicast gateways (VEUTM) will require additional ports

Port 53 UDP/TCP used for DNS resolution

Multicast requirements:

A correctly configured multicast (IGMPv2 or IGMPv3) enabled network is essential

4+ multicast addresses:

239.1.1.2 (setup), 239.1.1.3 (audio), 239.1.1.4 (control) and 239.1.1.5 (debug) are the defaults. Add an additional address for each audio channel used by a [VE6023 Telephone Paging Server](#).

Application Servers configured for **High Availability** additionally use multicast address 224.0.0.18 for [CARP](#) protocol. No port definition is required as CARP sniffs the address.

SIP Ports:

The default SIP UDP port number is 5060. Port 20,000 is the default UDP port used for the RTP media stream.

Listed in the VIP-102B Software, however, no longer used:

The V1 Multicast address (239.1.1.1) and V1 Control Port 4096 are not required for any VIP endpoint manufactured after 2009.

See [VE602x/VE6030 Port Requirements](#) chart for additional details

Power requirements for IP speakers or VE80XX Talkback Gateways:

802.3af PoE compatible switches or equivalent inline power injector

Power requirements for IP LED signs, IP Emergency Call Towers and Interactive Console:

802.3at High Power PoE+ compatible switches or equivalent inline power injector

Power requirements for IP/SIP 20-Watt Paging Amplifiers:

802.3at High Power PoE+ compatible switches, equivalent inline power injector or 900mA 24VDC Power Supply

Power requirements for VE8006R, VE1225 and VE602X/VE6030 IP server: Supply Included

Power requirements for V-9972 Universal Paging Interface: VP-624D Power Supply

Power requirements for other Valcom managed VoIP products:

802.3af PoE compatible switches, equivalent inline power injector or VIP-324D VoIP Endpoint Power Supply

Other requirements:

A [VLAN](#) dedicated to the Valcom VoIP system or shared with IP telephony endpoints is strongly recommended. It should be a manually configured port based VLAN as Valcom endpoints do not signal the switch to select between voice and data VLANs. Failure to provide the requested VLAN will likely result in missed announcements and broken audio transmission as the Valcom endpoints will have to process numerous packets unrelated to their operation.

Note that when installing new non-Valcom network endpoints, or network maintenance, others may move Valcom endpoints from the assigned VLAN ports thus rendering them inaccessible. The use of locking RJ45s may be used to discourage this practice.

If associated Valcom IP endpoints are installed in more than one VLAN, then properly configured routing between those VLANs is required.

Make provisions for Network Time Protocol (NTP) version 4 if utilizing syslog, VoIP clock/speakers, IP LED signs or the VE602X/VE6030 Servers.

If using DHCP and PortFast or its equivalent are turned off, then spanning tree must also be turned off. DHCP operation requires that all network switches and routers involved in the Valcom endpoint communication have alternate power during facility power failures. Otherwise, static addressing should be utilized.

DHCP servers must be set to provide 2 valid DNS server addresses. If only one DNS server exists, then the 2 DNS server addresses provided may be the same address.

Default DHCP

Most Valcom Endpoints are programmed at the factory to acquire an IP address using Dynamic Host Configuration Protocol (DHCP). If DHCP is not available, the endpoint will revert to the static IP address of 192.168.6.x after 3 to 4 minutes.

In addition to the IP address, the endpoint will also try to acquire all of the information needed to synchronize time from the DHCP Scope. If the DHCP Scope Options noted below are correctly configured, the endpoint will be able to acquire the correct time without further programming.

- Option 42, NTP Server IP Address.
- Option 100, POSIX Time Zone, example: "EST5EDT4,M3.2.0/02:00,M11.1.0/2:00". This is the preferred option and works for any area of the world.
- Option 101, Time Zone Name, example: "America/New York". This option is only supported for North America time zones.

Each of these options from the DHCP scope can be overridden by manually programming the desired value using the Valcom VIP-102B IP Solutions Setup Tool. If not using DHCP for IP address assignment, after the endpoint acquires a static IP address, DHCP may be disabled and all of the network settings will be configured using the Setup Tool. Download the latest version of the free IP Solutions Setup Tool from the Valcom web site at www.valcom.com/vipsetuptool.

VIP Status Monitor

The VIP Status Monitor tool does not use multicast. It uses UDP port 4099 for control messages, just like the 102B does. In addition, it may also use UDP Port 4125 for messages between different copies of the tool, and TCP port 4126 for Remote Access. Also, depending on the type of monitoring, the VIP Status Monitor might also utilize Ping and HTTP (port 80) and port 514 if Syslog has been enabled from the monitor.

The VIP Status Monitor and the VIP-102B may not be used on the same PC simultaneously.

Network Management

Networks vary in complexity, security parameters and general configuration. It is imperative that the parties installing the IP6000 system have a working knowledge of the hosting network's design and the expertise and access rights to manage its settings, or, that they have immediate access to the individual, or individuals who do. Change management policies may require advance notice and approval for any network configuration changes required. Acquire necessary approvals in advance of the installation.

Network Security

Some networks have special security requirements, such as [DIACAP](#) certification for endpoints. If the network that will be used with the Valcom system has such requirements, then contact us to discuss the requirements.

Internet and Mail Server Access

Provide Internet access for remote factory support and/or for access to RSS/Atom Based CAP Feeds, public NTP servers, and other Internet based resources.

When posting alerts to email, the Valcom equipment will need SMTP access to the mail server.

PoE

Valcom endpoints negotiate with PoE switches using IEEE 802.3af hardware signaling (standard PoE endpoints) or 802.3at hardware signaling (PoE+ endpoints). Additionally, PoE+ endpoints use LLDP-MED protocol to advertise their extended power preference. Some LAN switches that cannot provide the extended PoE+ power may shut down or reboot the network port. On some PoE switches, the default configuration is for PoE requests to be ignored if detected through LLDP or LLDP-MED.

Power requirements vary among endpoint models and whether they are active or idle. For planning purposes, assume full Class 3 (Class 4 for PoE+ endpoints) power for each endpoint; actual power used may be less. In addition, PoE power management features may need to be set to static or high priority. This pre-allocates power to the endpoint, even when power requirement is at a minimum. This guarantees that when the endpoint requires more power, it will be available.

Remember that PoE switches typically have a power budget that limits the number of PoE endpoints that may be connected.

Multicast

Improper/incomplete configuration of multicast is one of the most common issues encountered when deploying a Valcom IP Solution.

Valcom VoIP systems require properly configured multicast:

- 1) As the primary method of discovering new endpoints via the VIP-102B IP Solutions Setup Tool.
- 2) For any audio or text sent to a group.
- 3) To locate unknown channel dial code destinations. The VECPU6, VECPU6-EXP, VENSCA, VE8006R, and any VoIP endpoints using DHCP find unknown channel dial code destinations via **multicast**. These dial code routes are dynamically added to the phone book as found. If an entry in the phone book fails, perhaps due to the DHCP assigned address changing, then a new multicast query is sent to obtain current information and the phone book is updated. *If the unknown channel dial code cannot be located via multicast, users may receive a busy tone, an incomplete call message or call button generated calls may be unsuccessful.*

Regardless of the use of DHCP or static addressing, the use of groups, such as all call, require properly configured multicast.

If multicast is not properly implemented when using the VECPU6, VECPU6-EXP, VENSCA, VE8006R, and/or any VoIP endpoints using DHCP, there may be issues with calling both individual VoIP gateway and speaker channels and/or accessing groups.

A proper installation includes maintenance of multicast forwarding tables using IGMP querying (preferred), IGMP snooping, a combination of the two, or similar functions. On a properly configured network, Valcom endpoints join the multicast group on start up. After that, whether they continue to receive multicast traffic is completely dependent upon network design. Enabling IGMP querying or equal is typically a good solution as the network routers will poll the devices to inquire as to whether they should remain in the multicast group. Valcom IP speakers and gateways will respond to these queries.

Other network methods of determining multicast group membership, such as IGMP snooping, may not be as effective since Valcom IP speakers and gateways only use multicast when required and may appear idle to IGMP snooping and subsequently be removed from the IGMP group. Note that if IGMP snooping and IGMP querying can both be implemented it is generally advisable to do so.

The specifics of your network design, [PIM dense vs. sparse mode](#) for example, is irrelevant as long as the multicast traffic is fully routable between the Valcom endpoints as required.

When using VE6023 Telephone Paging Servers, there will be additional user defined multicast addresses required (1 per simultaneous announcement to phone groups) and multicast routing will also be required to all IP phones.

Some methods for troubleshooting and verifying proper operation of multicast are described in our Best Practices & General Troubleshooting Document. This document is available [here](#).

Multicast Security Myths

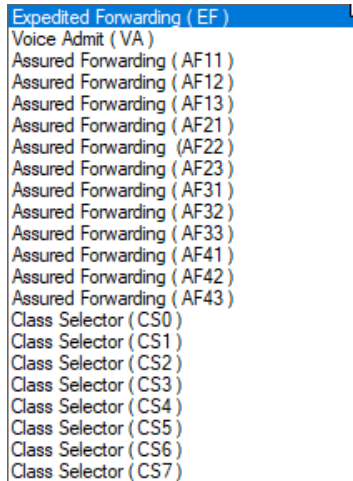
There are many myths about multicast and network security issues. Multicast is no less secure than unicast. Network endpoints that use multicast must request to join the multicast group; those that do not use multicast simply ignore the packets. In a properly configured network, with maintained multicast forwarding tables, multicast traffic is routed only where necessary. The use of multicast:

- a) Saves significant bandwidth when sending the same audio/text to multiple endpoints.
- b) Provides for audio synchronization between multiple audio endpoints.

Differentiated Services Code Point (DSCP)

Valcom endpoints default to a DSCP of Expedited Forward or Class Selector 5 (CS5).

To ensure audio good quality, advise the installer if the network DSCP setting is otherwise.



Spanning Tree¹

You will want to have [Spanning Tree Protocol](#) enabled on any network. It protects against inadvertent network loops. It is important to make the distinction between allowing a port to pass data versus disabling spanning tree protocol in general.

Configure any ports hosting Valcom devices with “spanning-tree PortFast” (for Cisco devices, command may be different for other manufacturers). This command allows the port to begin delivering packets as soon as the link is established. If the port does not have this command enabled, it will go into a listening state, then a learning state before it passes data. The default timer for these operations is 15 seconds each, so it could be 30 seconds before any data is passed. This includes DHCP, and some older devices did not handle this delay very well.

Browser Choices

Browser feature support varies by release. Occasionally, newly released versions of browsers such as Chrome®, Internet Explorer® and Firefox® will hinder Application server features such as USB microphone support and streaming audio events. Valcom works diligently to maintain features and functions as new browser versions are released.

Security

Gen 3 IP endpoints, gateways and the Application Servers can all be configured to use the [SSH](#) and [SCP](#) when intercommunicating with the VIP-102B.

Live Announcement Access

SIP (Session Initiation Protocol)

Most Valcom IP Speakers and Gateways are [SIP](#) accessible. To troubleshoot SIP, it's important to have a basic understanding of how it works. [This document](#) is a PDF that describes, in general terms, the flow of SIP between phones and Valcom endpoints/gateways.

Valcom endpoints/gateways utilizing SIP will register with the SIP server and suggest a registration expiration time of 3600 seconds. The SIP server may negotiate a different time, which the Valcom endpoints/gateways will honor. The Valcom endpoints/gateways will send re-registration at approximately 60% of the agreed upon registration expiration time.

When necessary, the default registration expiration time for Valcom endpoints/gateways can be changed to a higher or lower value. Lower values are particularly useful for hosted telephone systems. Using a value as low as 60 seconds may be necessary to keep firewall ports opened.

Non-SIP Telephone Access

If your system includes Valcom FXS Gateways (VE801X, VE801XR), then one or more dedicated POTs telephones, Valcom Admin Phones, FXO ports, Loop Start Trunk ports or C.O. Line Ports will be required. FXS Gateways provide dial tone, battery feed, and caller ID and should be treated like standard telco loop start dial tone lines (trunks).

If your system does not include Valcom FXS Gateways or SIP Paging Gateways (VE20X), then contact us to discuss telephone access.

Serverless Design

In Valcom's robust design, each Valcom IP endpoint stores information specific to its system. It stores:

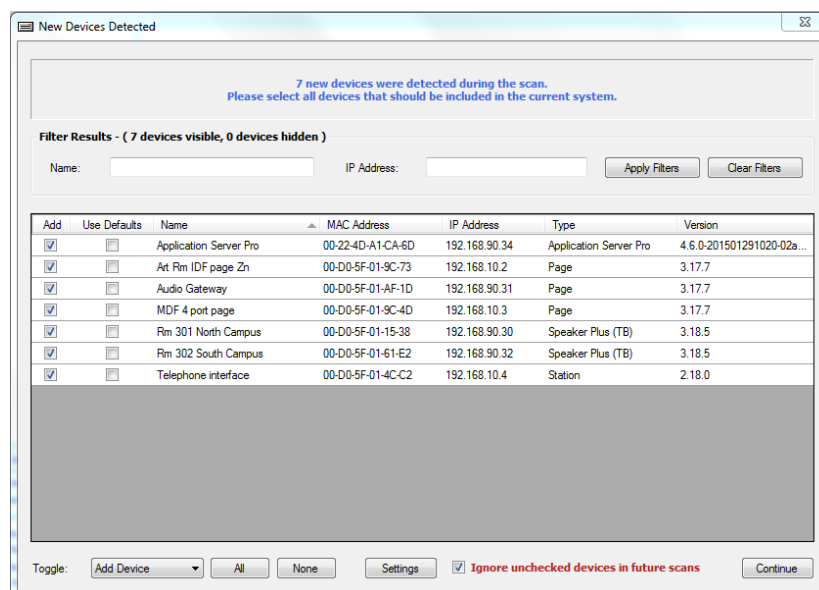
- a) a phone book of contact information for all other system endpoints.
- b) a list of all system group names, dial codes and priorities.
- c) a list of relay control groups.
- d) network port settings
- e) dial code translations

If proper network routing is maintained, Valcom IP endpoints will be able to interoperate without the need for a "control" server. Application Servers provide enhanced features and are not necessarily required for endpoint-to-endpoint interaction.

In cases where spare Valcom endpoints are put back into service at a new location, it's important to default the repurposed product so that erroneous programming is not introduced to the new site.

Multi-facility systems

When users first scan a network with the [VIP-102B](#), they are presented with a screen showing all endpoints that responded to the scan.



When working with multi-facility systems, it is critical to program the endpoints for each facility independently from the endpoints in other facilities. Failure to do so may cause unwanted migration of stored information between facilities. This can cause conflicts and take great effort to correct.

Using the screen above, the VIP-102B allows users to select which endpoints will be modified. Users may deselect all endpoints by clicking “None”, filter by the first part of the endpoint name or the first part of the IP address to find the desired endpoints, and then click “All” and “Continue”. To facilitate this feature, it is strongly suggested that each facility be on its own subnet and/or that the endpoints in each facility bear a common prefix that is unique from all other facilities. An acronym of the facility name typically works well. If intentionally adding a new or previously used endpoint, checking “Use Defaults” will clear that endpoint’s memory.

Global Announcements

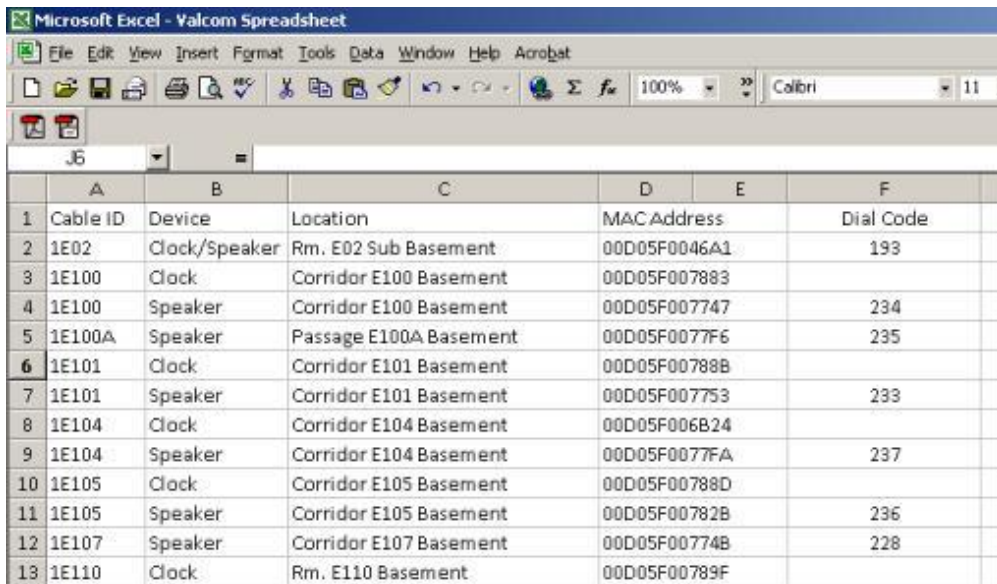
Multiple facilities on a properly configured network will all respond to common group codes that have been independently programmed into each system. In other words, if each facility has been programmed independently and includes group code 100, then any announcements to group 100 will broadcast globally throughout the enterprise.

Initial Onsite Checklist

Verify that all POE network switches are installed, labeled and configured to meet the network requirements.

Installation Checklist

As endpoints are installed, keep careful record of each endpoint's MAC address and installed location. Each endpoint is shipped with 2 identifying labels. These labels indicate the endpoint's unique MAC address and endpoint model number. Leave one of the labels affixed to the endpoint and adhere the second to a page in a spiral notebook. Write the installation location as well as the endpoint's switch and port number on or next to each label. Ultimately, this information should be transferred to a spreadsheet with an additional column for the assigned dial code(s).



The screenshot shows a Microsoft Excel spreadsheet with the following data:

	A	B	C	D	E	F
1	Cable ID	Device	Location	MAC Address		Dial Code
2	1E02	Clock/Speaker	Rm. E02 Sub Basement	00D05F0046A1		193
3	1E100	Clock	Corridor E100 Basement	00D05F007883		
4	1E100	Speaker	Corridor E100 Basement	00D05F007747		234
5	1E100A	Speaker	Passage E100A Basement	00D05F0077F6		235
6	1E101	Clock	Corridor E101 Basement	00D05F00788B		
7	1E101	Speaker	Corridor E101 Basement	00D05F007753		233
8	1E104	Clock	Corridor E104 Basement	00D05F006B24		
9	1E104	Speaker	Corridor E104 Basement	00D05F0077FA		237
10	1E105	Clock	Corridor E105 Basement	00D05F00788D		
11	1E105	Speaker	Corridor E105 Basement	00D05F00782B		236
12	1E107	Speaker	Corridor E107 Basement	00D05F00774B		228
13	1E110	Clock	Rm. E110 Basement	00D05F00789F		

As POE endpoints are attached to the network connection, verify that they are receiving power (link light activity).

Tech Tip: If you need to identify an endpoint after installation, and do not know the MAC address, open Communication/Network Diagnostics in the VIP-102B. If the VLAN and PC are properly configured, all endpoints will report in via a broadcast and multicast beacon. Unplug the Ethernet connection of the device in question and Network Diagnostics will no longer receive its beacons.

Initial System Setup Checklist

Unless using DHCP, work with the site's Network administrator to obtain a range of static IP addresses. The number of addresses available should equal the number of endpoints plus 5 to 10% spare.

Also obtain the relevant subnet mask, network class, gateway, DNS and time server information. If applicable, obtain the syslog daemon and stun server information.

It's not uncommon to have Valcom IP systems deployed in multiple facilities that:

- a) Primarily act as separate systems
- b) May be managed by one individual or group of individuals
- c) Share common groups for multi-facility or enterprise-wide announcements

A common example is a school district with Valcom IP systems deployed in each school and a desire for district wide announcements. There are important considerations related to such applications.

First, determine a logical dialing plan, noting that all dial codes in the enterprise-wide system must be unique and the same length (up to 11 digits long).

When multiple facilities have common room numbers, then one or more leading digits should be used to identify the building. For example, Room 202 in the first building would be assigned dial code **1**202, while Room 202 in the second building would be assigned dial code **2**202.

For facilities with rooms identified by a letter suffix, the dialing plan should include enough digits to allow for this letter suffix.

For example, if a facility has 3-digit room numbers that include letter suffixes such as 202A, 202B then a trailing digit indicative of the "A" or "B" will be necessary. In building **1**,

room 202 would be assigned dial code 12020, room 202A would be assigned 12021 and room 202B would be assigned 12022.

Oftentimes, multiple facilities will already share a phone system and have unique dial codes assigned to the phone in each area. Using this same code for the area speaker(s) may prove to be convenient for everyone.

Remember to reserve a range of dial codes for groups. Pick a range outside of the dial code plan used for individual areas or rooms. If your system includes an Application Server, remember to reserve group dial codes that will be used to dial select “Play lists”, that is, will be used to manually initiate audio and other server events.

For multi facility announcements (i.e., district-wide), add the desired group code(s) for such announcements to each facility *individually*. Once proper WAN routing is in place, all members of that group code will receive the global group audio.

Install the latest version of the VIP-102B Valcom IP Solutions Setup Tool on a Windows based PC that is connected to the VLAN and perform a system scan. Verify that all of the installed endpoints are discovered by the VIP-102B. A video example may be found [here](#), a reference manual may be found [here](#) and Best Practices can be found [here](#).

If endpoints are missing, then determine why they are missing, correct the problem and rescan.

Valcom endpoints and gateways are discovered by the VIP-102B in several ways:

- 1) By any IP addresses defined in the network setup
- 2) By the endpoints responding to a broadcast roll call request
- 3) By the endpoints or gateways responding to the tool's multicast roll call request
- 4) By the tool receiving a multicast beacon from the endpoint or gateway
- 5) By the tool receiving a broadcast beacon from the endpoint or gateway

If IP endpoints and gateways are not discovered by the VIP-102B IP Solutions Setup Tool, **then make certain that:**

- 1) You are using the latest version of the VIP-102B
- 2) You are not inadvertently using the "Valcom IP Tool"
- 3) The endpoints are powered
- 4) Multicast is fully implemented
- 5) The network requirements have been met
- 6) All switch ports are on a dedicated port based VLAN, or are part of a VLAN dedicated to both Valcom VoIP endpoints and VoIP telephony traffic
- 7) The PC's NIC currently utilized by the VIP-102B is connected to the VLAN
- 8) The PC is not connected through an IP phone auxiliary Ethernet port
- 9) All unused network interface cards on the PC are disabled
- 10) All port blocking protection software on the PC is disabled
- 11) Connectors/cables/switch ports are not defective
- 12) RJ45s are properly terminated
- 13) The tool Network Settings (File menu) match the endpoint or gateway network settings. Endpoint or gateway network settings are typically set to default values, however, can be changed on the System/Device Network Settings Menu and on each endpoint or gateway Network Tab
- 14) The IP endpoints and gateways are not listed in the VIP-102B's Ignore List
- 15) Any virtual machines using VMWare are disabled on the PC
- 16) If using spanning tree, that the port is defined as an Edge Port¹
- 17) The scanning PC and/or the endpoints are not plugged into network switch ports that are using MAC address filtering or some other form of MAC address security and are, therefore, denying access to the Valcom endpoints or the scanning PC.
- 18) The PC's Ethernet connection does not utilize a USB to Ethernet Adapter (dongle)
- 19) The endpoints have successfully retrieved an IP address from DHCP or have obtained a static IP address.

Keep scanning with the VIP-102B until all endpoints are discovered. Note that IP address and dial code conflicts will be reported during this scan. Note that a known working endpoint and a known working network port are your best tools for determining if issues are related to an endpoint or to the network.

A quick check of basic multicast implementation may be performed by viewing the VIP-102B's Network Diagnostics screen (Communications/Network Diagnostics). All Valcom endpoints should appear on this screen. The icon in the multicast column for each endpoint should be green. This indicates that the control multicast beacon sent by that endpoint is reaching the PC. This is not an absolute test of full multicast implementation. A more thorough test of proper multicast implementation may be performed with the Multicast Diagnostics software tool described in our Best Practices & General Troubleshooting Document. This document is available [here](#).

Once all the endpoints are discovered by the VIP-102B software:

- 1) Assign IP addresses to all endpoints*
- 2) Set the VIP-102B for the desired dial code length
- 3) Assign random channel dial codes* (to eliminate dial code conflict messages)
- 4) Program the system as required.

*These steps may be somewhat automated in the VIP-102B. If endpoints will be difficult to physically access after deployment, for example, emergency stanchions/call stations that will be distributed around a large campus, it will be beneficial to program the correct IP addresses and verify proper operation (both channel and group announcements) before installation. With this method, communication issues that occur after deployment may quickly be attributed to network issues. This is easily accomplished via a simple test setup using a small PoE switch, an FXS gateway and a POTS telephone.

System Balancing and Verification Checklist

Valcom VoIP systems have many volume adjustments. In this section we will initially discuss system volume balancing. We will be discussing individual channel output volume adjustments, offsets that may be applied to group announcements as well as offsets that may be applied to Application Server events.

First, if self-amplified or old-fashioned centrally amplified analog speakers are connected to IP endpoints, the analog volume control(s) should initially all be set to a mid-level setting.

Once system balanced is achieved, the analog volume controls on amplifiers or self-amplified speakers may be used for area specific adjustment. However, in a good design, all post install volume adjustment will be easily accomplished through the VIP-102B IP Solutions Setup Tool or user accessible wall mounted volume controls.

There are preset output volume adjustments per endpoint channel. These presets dictate the broadcast level when the channels are accessed via their individual channel dial codes.

These preset output volume adjustments may be increased or decreased (offset) when the channels receive audio as part of a group or when accessed via FXS Gateway channels.

VIP-102B Group Priorities vs. Server Group Priorities

The VIP-102B IP Solutions Setup Tool allows volume offsets to group audio based upon the group's priority. If the group is receiving audio from an Application Server event, then the group's priority and its associated volume offset is overridden by the event's priority and volume offset.

For example, an announcement to a group that has an assigned volume offset of +6 will result in the group members broadcasting the audio with an offset of 6 above their individual channel output volume presets.

An Application Server sending an audio event with an assigned volume offset of +2 to a group with an assigned volume offset of +6 will result in the group member broadcasting their audio with an offset of 2 above their individual channel output volume presets.

As previously mentioned, gateways may be providing audio to analog subsystems featuring their own volume adjustments. That's why it's important to initially have a common preset volume for analog speakers. Otherwise, balancing via the VIP-102B virtual volume controls would be impossible.

Initial Audio Level Setup

The following important process is intended to determine baseline volume levels for your VoIP speakers and audio gateways. The process will facilitate system balance by determining and setting baseline levels first and then adjusting individual area, group or event volumes up or down as necessary.

First, make a test announcement to All Call or any one-way group comprised of VoIP One Way speakers. Be certain that the group being used for testing has a priority volume offset of zero. Determine an acceptable volume level.²

Using the "Programming/Volume Adjustments" section of the VIP-102B, adjust the channel output volume of all VoIP One Way speakers to the level determined above.

Secondly, make a test announcement to a VoIP Talkback speaker that is installed in a typical area (an area representing the location of most of your talkback speakers). Determine an acceptable volume level.

Using the “Programming/Volume Adjustments” section of the VIP-102B, adjust the channel output volume of all VoIP Talkback speakers to the level determined above.

For this next adjustment, you will need for an assistant to be in an area representative of your typical VoIP Talkback speaker locations. Call into the selected area and converse in a normal level/tone of voice. Determine an acceptable receive (input) volume level.

Using the “Programming/Volume Adjustments” section of the VIP-102B, adjust the channel input volume of all VoIP Talkback speakers to the level determined above.

Set audio gateway channel output levels to -10. Make a test announcement to each individual audio gateway, office and common area. Adjust audio gateway channel output volumes as required (self-amplified speakers and amplifiers connected to each audio gateway output should all initially be set to the same level.).

Using a music source set to a level representative of a typical voice page, walk through the facility and verify that each VoIP speaker is receiving audio.

If call buttons are installed, verify the operation of each VoIP Talkback speaker by pressing its associated call button and conversing.

If call buttons are not installed, verify the operation of each VoIP Talkback speaker by calling each speaker and conversing.

Make area specific volume adjustments as necessary.

Record volume levels and the results of individual speaker tests on a spreadsheet or form. Involve the owner in the final testing in order to facilitate acceptance.

¹The spanning tree algorithm is used in switch-based networks to determine the best path for traffic to move between two network devices.

Spanning tree algorithm prevents loops and promotes efficient data delivery by discovering all possible paths between two ports on a network and ensures that only one is active at a time.

If the primary path is not available, then spanning tree protocol directs traffic to alternate paths if available.

Spanning tree protocol utilizes a primary decision-making switch called the root switch. All switches in a network utilizing spanning tree protocol branch from the root switch and all network paths are traceable back

to the root switch. The root switch is necessary as it serves as a reference point for the best route calculations.

Data messages exchanged between switches, known as bridge protocol data units (BPDUs), gather information about other switches in the same network.

Each port on a switch using spanning tree protocol may be in any of five states – blocking, listening, learning, forwarding or disabled.

With spanning tree enabled, every switch port in the network starts in the *blocking* state, then moves to the *listening* and *learning* states. If a potential loop is detected, the port will be set to the *blocking* state. If no loop is detected, the port will be set to the *forwarding* state. The ports then sustain the forwarding or blocking state unless changes are made to the network.

The bridge protocol data unit exchange is used to determine which network switch will serve as the root switch.

A switch always enters the blocking state following switch initialization and will not send or receive any data traffic across the network segment. A port in the blocking state will however listen to BPDU messages. This could create issues with the VIP-102B device discovery.

If you wish to force a port into forwarding state when connected, bypassing the blocking, listening and learning states, then program the port in Edge Port/PortFast Mode. (note: Unlike PortFast, a Cisco term, an edge port that receives a BPDU immediately loses edge port status and becomes a normal spanning tree port. There are no additional key differences between these features.) A port is considered as an edge port when it is directly connected to the user terminal or server, instead of any other switches or shared network segments. The edge port will not cause a loop upon network topology changes.

² Volume adjustment increments between the Gen 3 speakers and Gen 2 speakers may vary. If you set both for the same output volume increment in the VIP-102B, you may find that the Gen 3 speakers are significantly louder. Conversely, the input volume on Gen 3 speakers will need to be set to a higher increment than their Gen 2 counterparts to achieve the same input level. If your system contains both, volume adjustment of the 2 speaker types must be made separately.

Priority Overrides

Although the server sets the priority of audio events on a per event basis, higher priorities still prevail. For example, if group 999, assigned a priority of 50 in the VIP-102B IP Solutions Setup Tool, is currently receiving a live voice announcement, and the server sends audio to that group at a priority of 25, the audio sent from the server will not override the live voice announcement. If the audio from the server is still in progress at the conclusion of the live voice page, the group members will join the server audio stream at a new priority of 25.

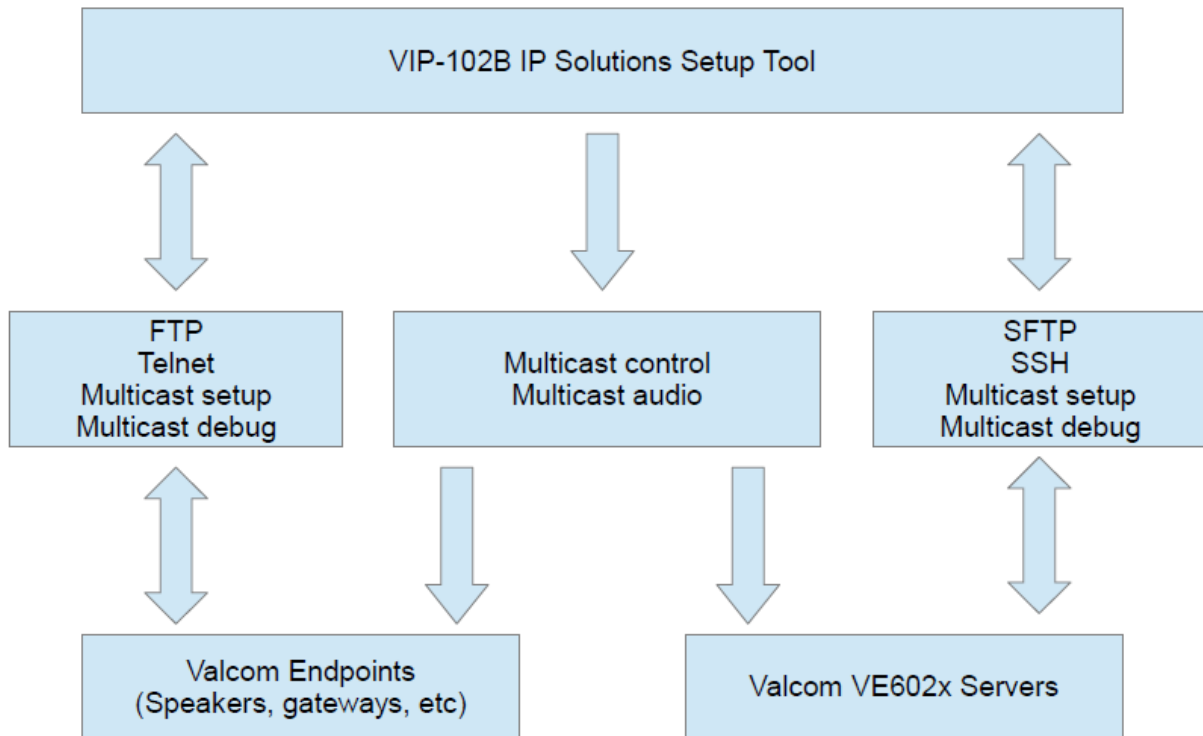
Higher priority audio overrides lower priority audio. If multiple audio streams have the same priority, then they are processed on a first come/first serve basis.

Once higher priority audio has completed, any lower priority audio still in progress will be broadcast mid-stream.

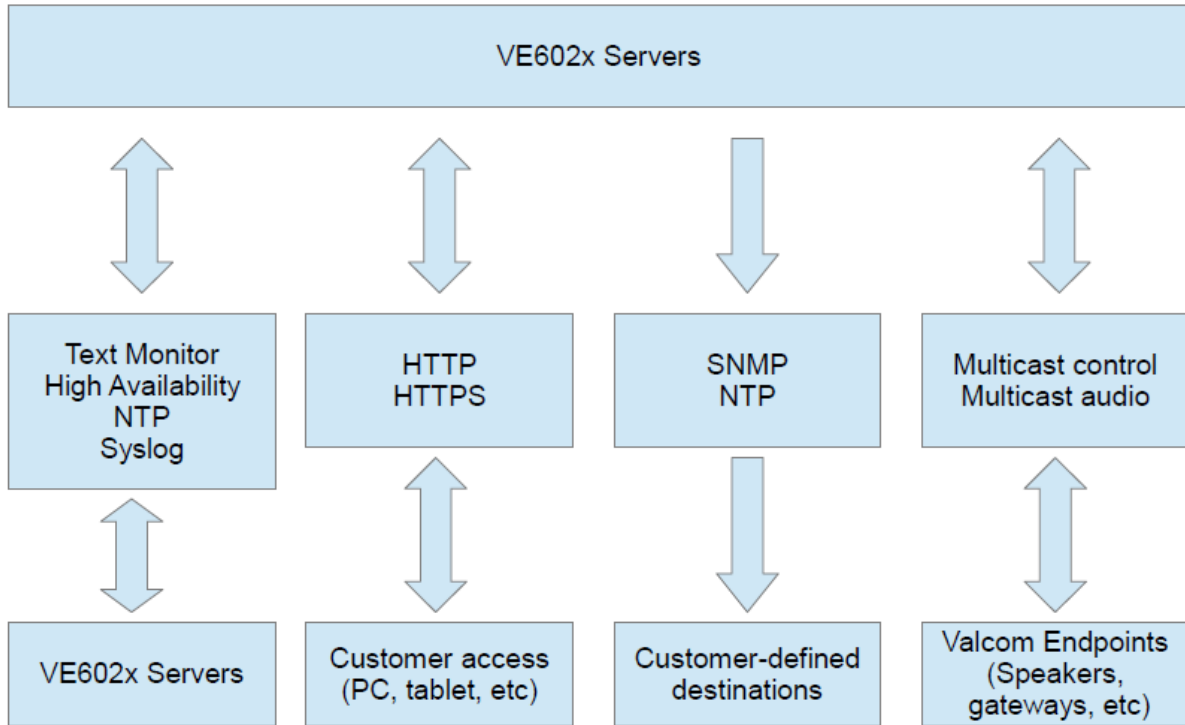
VE602x/VE6030 Port Requirements

Source	Destination	Default Destination Port	Protocol	Address (Defaults)	Service
SSH client	VE602X/VE6030 Servers	5147	tcp	Unicast	sshd
Time Server	VE602X/VE6030 Servers	123	udp/tcp	Unicast	ntpd
VE602X/VE6030 Servers	HTTP Web Access	80	tcp	Unicast	HTTP
VE602X/VE6030 Servers	HTTPS Web Access	443	tcp	Unicast	HTTPS
VE602X/VE6030 Servers	monitoring server	161	tcp	Unicast	SNMP
VE602X/VE6030 Servers	VEEWS	8883	tcp	Unicast	MQTT over TLS
VE602X/VE6030 Servers	monitoring server	161	udp	Unicast	SNMP
VE602X/VE6030 Servers	monitoring server	162	udp	Unicast	SNMP
Varies	Varies	53	Udp/tcp	Unicast	DNS Resolution
Varies	VE602X/VE6030 Servers	Varies	Varies	Varies	text monitor
VE602X/VE6030 Servers	VE602X/VE6030 Servers	7789 through 7799	tcp	Unicast	high availability
VE602X/VE6030 Servers	VE602X/VE6030 Servers or VIP 102B-Tool	514	udp	Unicast	syslogd
VIP-102B Tool	Valcom End Points	21	tcp	Unicast	FTP
VIP-102B Tool	Valcom End Points	23	tcp	Unicast	Telnet
VIP-102B Tool	VE602X/VE6030 Servers	5147	tcp	Unicast	SSH
VE602X/VE6030 Servers	VE602X/VE6030 Servers	5432/5147	tcp	Unicast	High Availability
VE602X/VE6030 Servers	VE602X/VE6030 Servers	69	tcp	Unicast	tftpd
VIP-102B Tool	VE602X/VE6030 Servers	4097	udp	Multicast (239.1.1.2)	Setup Port
VIP-102B Tool	VE602X/VE6030 Servers	4098	udp	Multicast (239.1.1.3)	Audio Port
VIP-102B Tool	VE602X/VE6030 Servers	4099	udp	Multicast (239.1.1.4)	Control Port
VIP-102B Tool	VE602X/VE6030 Servers	4120	udp	Multicast (239.1.1.2)	Secondary Setup Port
VIP-102B Tool	VE602X/VE6030 Servers	4121	udp	Multicast (239.1.1.5)	Primary Debug Port
VIP-102B Tool	VE602X/VE6030 Servers	4122	udp	Multicast (239.1.1.5)	Secondary Debug Port
VIP-102B Tool	VEUTM Routers	4197	udp	Multicast (239.1.1.2)	VEUTM Router Setup Port
VE6023 Server	Avaya Communication Manager	161	tcp	Unicast	SNMP
VE6023 Server	Avaya telephones	8989	tcp	Unicast	Avaya Push API
Avaya telephones	VE6023 Server	8989	tcp	Unicast	Avaya Subscribe API
VE6023 Server	Avaya telephones	20480+	rtp	Multicast (varies)	Streaming audio
VE6025/VE6030 Server	Avaya Application Enablement Server	4721	tcp	Unicast	Avaya API
VE6023 Server	Cisco Unified Communications Manager	2748	tcp	Unicast	Cisco API
VE6023 Server	Cisco Unified Communications Manager	443	tcp	Unicast	SSL/TLS
VE6023 Server	Cisco Unified Communications Manager	161	udp	Unicast	SNMP
VE6023 Server	Cisco Telephones	80	tcp	Unicast	Cisco Paging API
VE6023 Server	Cisco Telephones	20480+	rtp	Multicast (varies)	Streaming audio
VE6023 Server	NEC Phones	82/8282	tcp	Unicast	NEC Phone API
VE6023 Server	NEC MA4000	80	tcp	Unicast	NEC Mgmt API
NEC MA4000	VE6023 Server	9997	tcp	Unicast	NEC Mgmt API

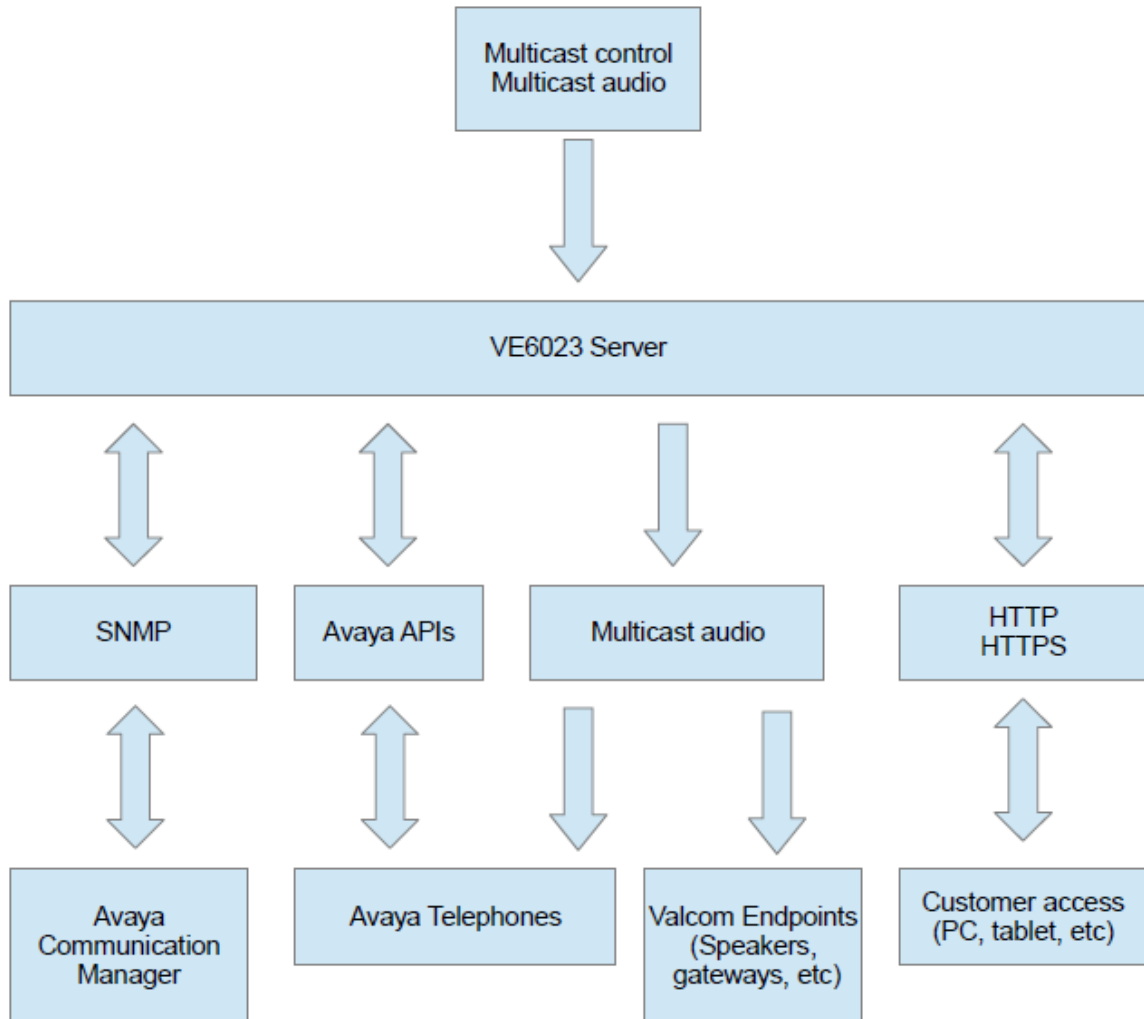
VIP-102B IP Solutions Setup Tool Network Communications



VE602x/VE6030 Server Network Communication

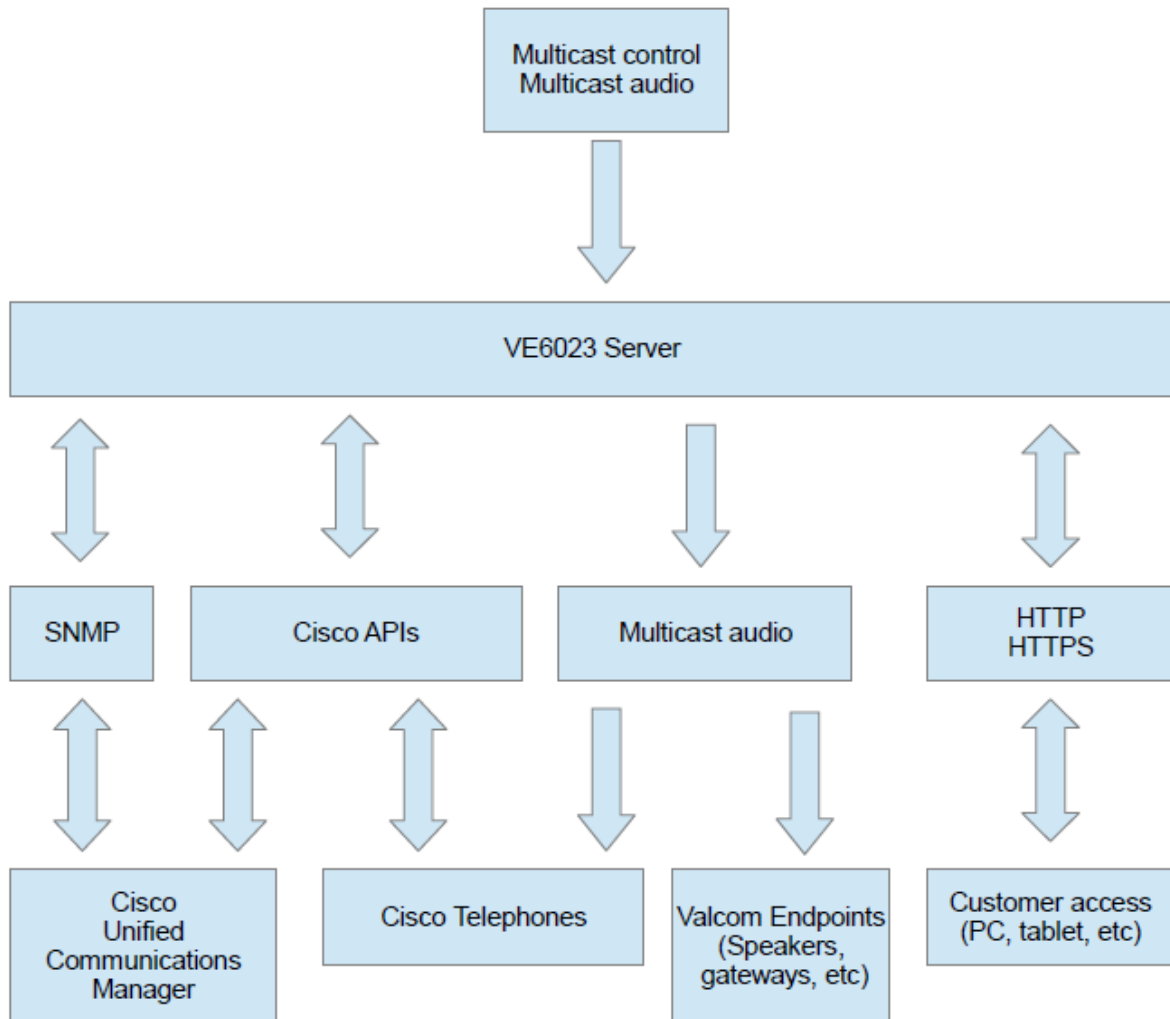


VE6023 Server Network Communication (Avaya)



Please review the [VE6023 manual](#) for set up information.

VE6023 Server Network Communication (Cisco)



Please review the [VE6023 manual](#) for set up information.

Valcom V-Alert Mobile App Network Requirements

The network requirements for Valcom's V-Alert server are very similar to the requirements for a public-facing web server.

A typical installation will require a host name to be assigned and registered with a public DNS service. The IP address assigned to the host name would likely be an outside interface of a firewall, which would then forward the traffic to the internal network (or DMZ) where the V-Alert server is connected.

TCP ports 80 and 443 will need to be forwarded through the firewall and traffic from the V-Alert server must also be allowed to exit through the firewall. Beginning with version 1.0, a customer-supplied SSL security certificate from a trusted Certificate Authority (not self-signed) is required.

In addition, if remote access by Valcom technical support is needed, then TCP port 5147 would need to be opened. This port is only required to be opened when support is required and would normally not be open.

Virtual VEXXX Server Hardware Requirements

The minimum hardware requirements for a virtualized version of the Valcom Application Server and Telephone Paging Server are located [here](#).

Proper shutdown during power failures is critical.

The hardware utilized for the virtual machines (VMWare) must include a smart UPS.

During a power failure, the smart UPS must signal the VMWare server to shut down.

The VMWare server will then send ACPI Shutdown commands to the Virtual Machines running on the server.