INNOVATIVE IED electronic designs

9701 Taylorsville Road
Louisville, KY 40299, USA
phone (502) 267-7436
fax (502) 267-9070
www.iedaudio.com

IED GLOBALCOM / 500ACS NETWORK PROTOCOL / PORT UTILIZATION

Destination Ports

The ports used depend on what features are implemented in a system. For a given system, the following network messages may occur which use the ports indicated:

- IEDnet Messages – These are TCP/UDP packets always sent to UDP port 3048. On GLOBALCOM systems the source port is port 3049. On legacy systems, the source port is 1026.
- SQL Server Messages – In Enterprise systems, the clients communicate to the Microsoft SQL Server database on the server computer. These are TCP/IP connections to server TCP port 1433.
- MSMQ Messages – In Enterprise systems, clients also communicate with IED-provided Windows services on the server computer via Microsoft Message Queuing (MSMQ). The ports used for this are: TCP: 1801, RPC 135 and UDP: 3527 & 1801. If firewall or other network configuration needs to be done to accommodate MSMQ, one should refer to Microsoft's online articles such as: http://support.microsoft.com/kb/178517
- ICMP (Ping) – Used to monitor some devices on the network. This uses TCP/UDP Port 7.
- FTP – Used to pass configuration files to Lifeline ACS's and new message files between ACS's, Lifelines and MSG boxes. This uses UDP/TCP Ports 20 and 21.
- SNMP – Used control some peripherals like DNA7800's, 15xxNA's or 1100DAB's. If a Lifeline controller is employed, this is used to ensure the other controller's bundles are cleared. In some systems, SNMP Traps are used to report fault information. The ports used for this are UDP/TCP Ports 161 and 162.
- HTTP – Used to access GLOBALCOM System Management Center (SMC) and to view Logs on the server or to access T-CAS via TCP port 80.
- WCF (Windows Communication Foundation) – This is between services/devices, such as between the 1100ACS and the 1100MSG units. These use TCP ports 8088 and 8089.
- SIP (Session Initiation Protocol) – This is used for VoIP phone connections. These use a range of UDP ports 5065 – 5105, although there are configuration options in GLOBALCOM which may be changed by the installer.
- RTP (Real-Time Protocol) – This is used for VoIP phone data exchange. These use a range of UDP ports 40006 – 40086, although these are configuration options in GLOBALCOM which may be changed by the installer.
- SMC (System Management Center) Live Feeds – These are Silverlight feeds to drive such things as meters and announcement/zone activity on the web pages using TCP ports in the range of 4502 – 4534.

In addition, there are optional protocols and ports used depending on what kinds of remote access are implemented on site:

- LogMeIn – If this remote access is installed for IED Technical Support, TCP port 443.
- Windows Remote Desktop (RDP) – For accessing one client computer on site from another, TCP port 3389
- VNC – Alternate to RDP for computer-to-computer access, TCP ports 5500, 5800 & 5900

Source Ports

Sources ports can be any free port. This is managed by underlying drivers and network stacks. For example, an SNMP request may go to port 161, but the source port can be any free port. Some software uses only free ports above 49152. Other software uses any free port. For example, HTTP requests often use lower valued free ports in the 1000's range. IED recommends that any network/firewall configuration should not block or filter on source port.

IED005041 RevA 10/14

INNOVATIVE IED electronic designs

9701 Taylorsville Road
Louisville, KY 40299, USA
phone (502) 267-7436
fax (502) 267-9070
www.iedaudio.com

IED GLOBALCOM / 500ACS NETWORK PROTOCOL / PORT UTILIZATION

Other Network Traffic/Notes

Underlying Ethernet management protocols such as ARP must be enabled across the network connecting IED devices. It is standard for network stacks to time-out dynamic ARP entries in their tables every few minutes (ranging from 2 to 10 minutes by default in most versions of Windows, for example). This protocol must be enabled across all layer 2 and layer 3 network connections to IED devices and computers that talk to them.

In addition, the network should support CobraNet traffic within each system's LAN or VLAN. CobraNet is layer 2 and does involve broadcasting (technically MAC multicasting). All traffic is identified as Ethernet type 0x8819. The exact requirements on network equipment and configuration can be found on the cobranet.info website, in particular the page on network performance is:

http://www.cobranet.info/support/design/performance

Communications between LANs/VLANs can/should block CobraNet traffic, but should include all other TCP/UDP and ARP traffic described above. Not doing this will risk breaking certain features of the system.

1100DAB Specifics

The two sides of an IED1100DAB (Digital Audio Bridge) are connected to two different networks (LANs or VLANs) and provide a mechanism for bridging CobraNet audio across those two networks. To allow for the dynamic configuration of CobraNet bundles during real-time operation, the GLOBALCOM 1100/1200ACS must be able to communicate with both sides of the 1100DAB at all times. This means it must be able to communicate using the SNMP protocol, which uses the fixed destination port of 161, but any available source port above 49152. In addition, basic network communication protocols must be enabled such as ARP, and PING. (PING is not absolutely required, but is highly recommended for technician diagnostic purposes.)

The block diagram below shows how 1100DAB's are connected to networks. The Local Net will be implemented as a set of network switches. The Global Net may be implemented via separate switches and/or routers, or just by a bridge between VLANs on a master/core switch.