AtlasIED Network Protocols & Ports

Ver 3.0 14 May 2020

GLOBALCOM Controllers (IP100-series)

Protocols and ports that will or may be used for network communications to/from GCK (vACS) controllers such as IP100-series. If the system is Dante-enabled, see Audinate's listing of ports and multicast addresses employed as part of this protocol. If the system is CobraNet enabled, the network will also see packets employing the CobraNet layer 2 protocol (0x8819).

Protocol	Destination Ports	Notes
Ping (ICMP)	n/a (not TCP or UDP)	Used for some device supervision
FTP	UDP/TCP:20, 21	Used for sending configuration/recording files to lifeline controllers
SMTP	TCP:25 *(default)*	Fault and event notification via e-mail *if this feature is employed in the system*. Default value is 25, but depending on mail server, can be changed in SMC.
DHCP	UDP:67	If the DHCP server function is enabled on the controller.
HTTP	TCP:80, 8080	Earlier GLOBALCOM/GCK systems used for System Management Center. Recent GCK SMC is via HTTPS. Uses of HTTP in GCK are some diagnostic feeds from select services.
HTTPS	TCP:443	GCK System Management Center (SMC) web pages.
SNMP	UDP/TCP:161, 162	For some device control & supervision
IEDnet	UDP:3048	For device control & supervision. Sometimes broadcast.
Silverlight Data	UDP:4502 – 4534	Live feeds from SMC such as audio meter data.
SIP	*Typical* UDP:5060 – 5105	For VoIP telephony integration, *if used*. Exact ports are user-definable and may differ from those shown as typical.
RTP	UDP:40006 – 40086	For VoIP telephony audio, *if used*.

Protocol	Destination Ports	Notes
IEDnet+ RTP	UDP:5002 – 36016	For controller-to-controller audio, *if IEDnet+ used for multi-controller audio.* Exact ports are user-definable but default to 4000 + (1000*System_Number) + (IEDnet+_Transmitter_index*2), i.e., 5002, 5004, 5006. . . for GCK system #1.
WCF	TCP:8088 and 8089	(Windows Communication Foundation). For some device supervision/discovery
Signalr	TCP:8082	For SAFE comms to desktop clients.
HTTP	TCP:17436	Comms with Dante service on controller.
proprietary	TCP:7436	Control commands to T112 and IPX
proprietary	TCP:1764	Firmware updates to IPX.
proprietary	TCP:3000	RTP Audio Service controls
proprietary	TCP:3047	vACS debug/diagnostic port
proprietary	UDP:3030, 12301, 12302	Barix device control and subscription reporting ports – *if Annunicom100 or Barionet devices used in a system.*
proprietary	TCP:4052	System Management Center notifications such as announcement reports.
proprietary	TCP:9000	Audio Service communications
MDNS	UDP:5353	For Dante device discovery
proprietary	TCP:6347	Device Configuration Service comms
SNPP	TCP:444	For Simple Network Paging Protocol (RFC 1861) *if this module is used in a system* (e.g., nurse call interfacing)

Director Workstations

Computers that host AtlasIED Director may use any of the control protocols mentioned above for GLOBALCOM Controllers in their interactions with the system. In addition, they use the following protocols/ports.

Protocol	Destination Ports	Notes
Director peer-to-peer messaging	TCP/UDP:35000	For communication between Director workstations.

Enterprise Computers

Protocols and ports that occur between Enterprise computers, servers or clients.

Protocol	Destination Ports	Notes
HTTP	TCP:80	For web pages hosted in Enterprise such as announcement log viewer
IEDnet	UDP:3048	For device control & supervision. Sometimes broadcast.
SQL Server	TCP:1433	
MSMQ	TCP:1801 RPC 135 UDP:3527,1801	Microsoft Message Queuing. 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

Any Kind of Computer

In addition to the above, depending on how the controllers/computers are configured for remote access, the following protocols and ports may be enabled and used.

Protocol	Destination Ports	Notes
Remote Desktop	TCP: 3389	For accessing the computer from another on-site.
TeamViewer	TCP:80, 443, 5938	For off-site remote access

A Note on Simple TCP/IP Services

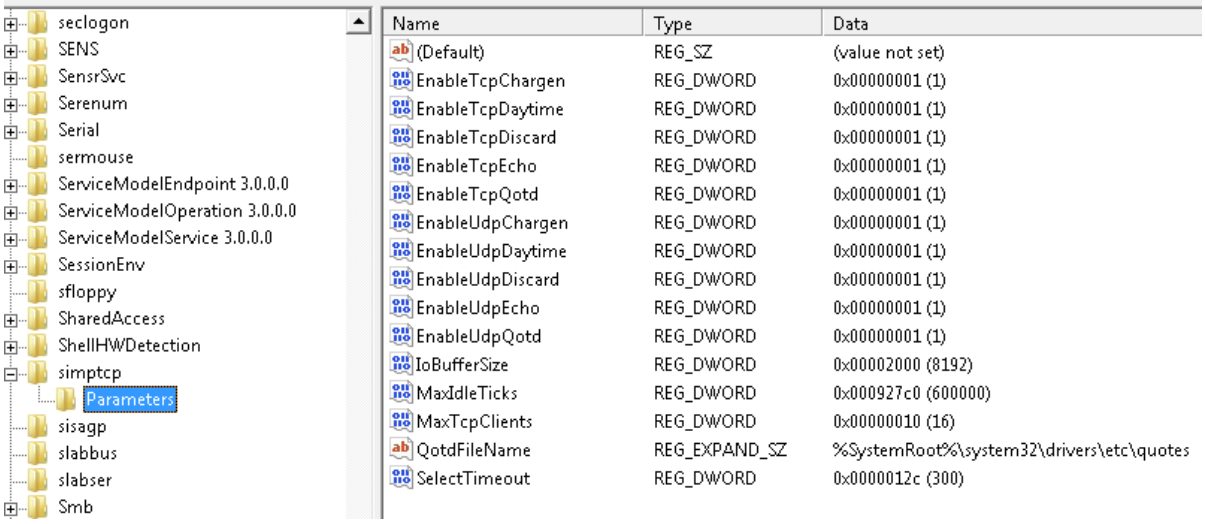
Windows has available something called the **Simple TCP/IP Services** (simptcp) that implements support for the following protocols and ports:

- Echo, port 7, RFC 862.
- Discard, port 9, RFC 863.
- Character Generator, port 19, RFC 864.
- Daytime, port 13, RFC 867.
- Quote of the Day, port 17, RFC 865.

AtlasIED controllers based on the Windows Embedded Standard 7 operating system have this service and all protocols enabled by default, while the newer controllers based on Windows 10 IoT (Internet of Things) has this service disabled. If an installation has concerns about these ports being active and possibly used for denial of service type attacks on the controller, they can be disabled without impacting the normal operation of the AtlasIED software.

One way to disable some or all of these services is to go into RegEdit and find the enable protocol keys under: **HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters** and set the Enable___ values for protocols not wanted to zero (0). See the list of parameters in RegEdit below. Then, one either restarts Windows completely, or just stops and restarts the SimpTCP service via the following commands in a Command window (CMD.exe):

```
net stop simptcp
net start simptcp
```



Alternately, one can go into Windows Services and disable the Simple TCPIP service entirely to disable all of the protocols it supports.