Andover Continuum Communications Network Ports Matrix

There have been many questions on which network ports the Continuum system uses for communication. Below is a matrix of the network ports along with what the port is being used for.

The destination UDP port from the controller will always be one of the port numbers below. The source UDP port that the controller uses is completely arbitrary and will be anywhere from 32768 to 65534 (0x8000 to 0xFFFE).

Controller/CyberStation	Application	Packet type	Decimal Port Number	Hex Port Number
BACnet b4 controller	Point Configuration	UDP	33487	0x82CF
BACnet b4 controller	Alarm Configuration, Alarms, and COV	UDP	47808	0xBAC0
BACnet b4 controller	Controller flash	TCP	33456	0x82B0
BACnet b4 controller	Web Server	TCP	80	
NetController	Point Configuration, Alarms, and Events	UDP	33487	0x82CF
NetController	Save from Controller	TCP	33440	0x82A0
NetController	Controller flash	TCP	33456	0x82B0
NetController	WebServer	TCP	80 (but configurable)	
CX9702*	Point Configuration, Alarms, and Events	See Note	33487	0x82CF
CX9702*	Save from Controller	See Note	33440	0x82A0
CX9702*	Controller flash	See Note	33456	0x82B0
CX9702*	WebServer	See Note	80 (but configurable)	
Remote View	Remote View Video	TCP	18772	0x4954
CyberStation	Controller Alarms and Events	UDP	33487	0x82CF
CyberStation	Peer CyberStation communication	UDP	44224 (1.4x and 1.5x), 47808 (all other revisions)	0xACC0 (1.4x and 1.5x), 0xBAC0 (all other revisions)
CyberStation	Workstation to SQL Database	TCP	Determined by Microsoft, 1433 by default	
CyberStation	BACnet Communication	UDP	47808	0xBAC0
CyberStation	MSMQ	TCP	1801	0x0709
CyberStation	MSMQ	UDP	3527	0x0DC7
CyberStation	MSMQ	UDP	1801	0x0709
CyberStation	MSMQ	RPC	135	0x0087
CyberStation	MSMQ	RPC	2101**, 2103**, 2105**	0x0835, 0x0837, 0x0839

*   UDP or TCP port (user configurable via the TransportType attribute)

**   Message Queuing message traffic and internal session management traffic between Queue Managers is delivered over Winsock through reserved TCP port 1801.

The Message Queuing Independent Client multicasts a server discovery broadcast over reserved UDP port 1801.

Message Queuing Servers listen on TCP port 2101* for RPC-based MQIS and Active Directory lookups. Message Queuing 3.0 independent clients and Message Queuing servers make MQIS requests directly to Active Directory by using LDAP on TCP port 389.

Message Queuing Independent Clients and Servers listen on fixed TCP port 2103* and 2105* for RPC-based remote reads of their public queues and private queues. Also, the Dependent Client uses these two ports to communicate with its server for send and for receive.

There is a dynamic RPC port that is assigned by the RPC layer for handshaking with an Independent Client or with an RPC server for the Message Queuing Server to determine the fixed ports. This is typically port 135.

The internal "ping" mechanism for Message Queuing operates over reserved UDP port 3527.

When you use HTTP messaging in Message Queuing 3.0, Message Queuing message traffic and internal session management traffic between Queue Managers is delivered over Winsock through reserved TCP port 1801.

* These port numbers may be incremented by 11 if the initial choice of RPC port is being used when Message Queuing initializes. A connecting QM queries port 135 to discover the 2xxx ports.

For more information on MSMQ ports check with Microsoft, http://support.microsoft.com/kb/178517

Network Security Notes:

If Network Security is enabled on the NetController II or ACX Series (models 5720 and 5740) controllers, the IKE (Internet Key Exchange Protocol) will operate on UDP Port 500.

Additionally, when Network Security is enabled on either of these two products, the Infinity Protocol will operate on UDP port 33792 (0x8400) and the Save to Database protocol will operate on UDP TCP Port 33952 (0x84B4).

Last, if the user decides to secure the Web Interface, the suggested port is TCP 33920 (0x8480), but may be changed by the user.

Note, that these port numbers (33792, 33952, and 33920) are not visible via a network capture when Network Security is enabled due to the fact that all of the UDP/TCP header data is encrypted in an ESP (Encapsulated Security Payload) packet.

If there are any questions on this, please contact TAC Product Support Services at +1 (978) 975-9508.