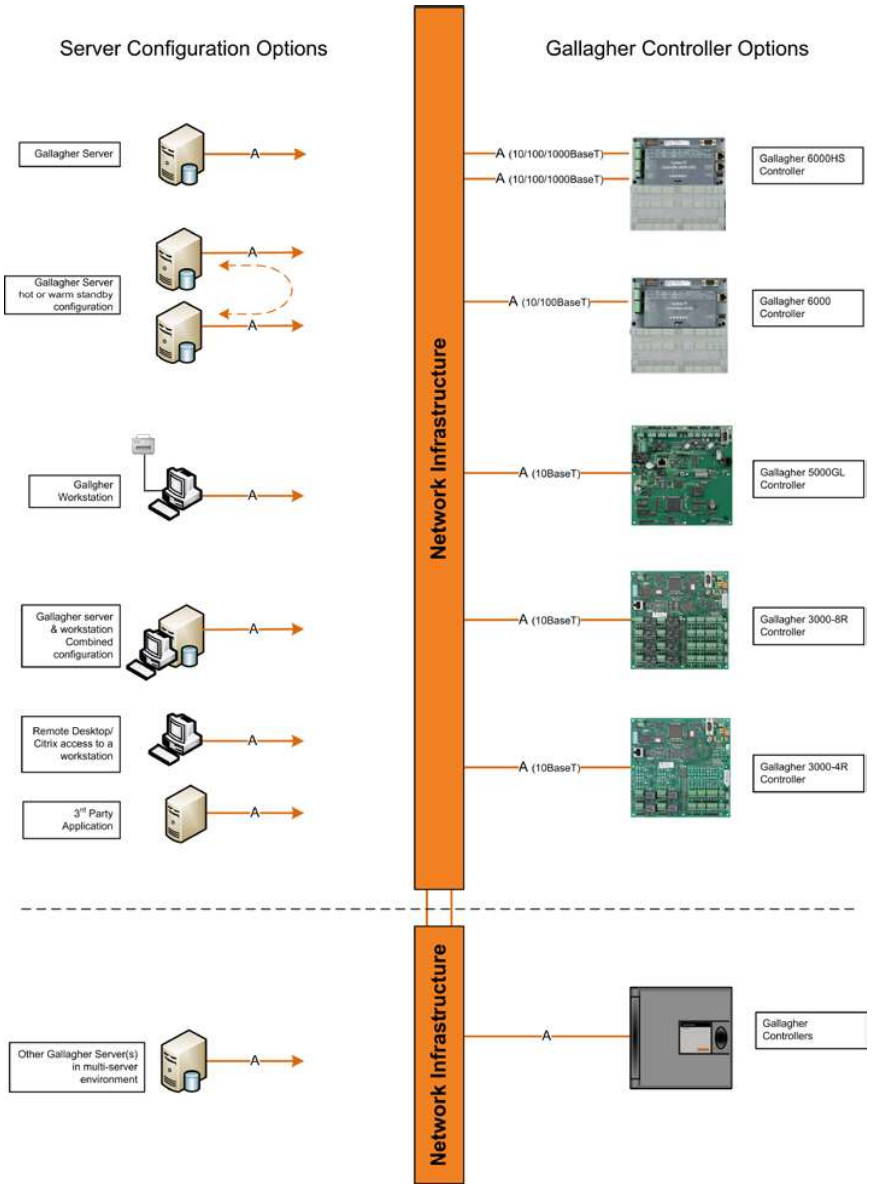


Network Data Rates

Controller	Connectivity
3000	10BaseT
5000GL	10BaseT
6000	10/100BaseT
6000HS	10/100/1000BaseT (2 ports)

Port Assignment - Gallagher Controller to Gallagher Command Centre Server

Keyword	Decimal	Description	Function
Bootps	67/tcp[2]	Bootstrap protocol server	BootP

Bootpc	68/tcp[2]	Bootstrap protocol client	BootP
www	80/tcp[3]	HTTP	Internet Explorer to Gallagher Controller connection
Cardax	1072/tcp[1]	Gallagher	Gallagher Controller connection (enable both ways)
Sagem	11010/tcp[4]	Morpho	Command Centre to Morpho reader communications [6]

Notes:

1. CARDAX port 1072 is required for Gallagher Controller to Gallagher Server communications
2. BootP ports 67/68 are only required if BootP/BootStrap protocol required for assigning Gallagher Controller IP addresses
3. WWW port 80 is only required if web browsing to a Gallagher Controller required
4. Applicable to Morpho biometric reader operation only

If a gateway is defined for the Gallagher Controller, ICMP must be enabled between the Controller and its gateway as the Controller will first ping the gateway if it needs to send a message to an address outside of its subnet.

Port Assignment - Gallagher Command Centre Server to Client Workstation

Keyword	Decimal	Description	Function
epmap	135/tcp	DCE endpoint resolution	Client Connection [1]
various	dynamic/tcp	DCOM (5 x dynamic ports)	License Verification, Alarms and Events, CCNTSAD
Microsoft-ds	445/tcp	Microsoft-ds Service	ClickOnce [2]
Configurable	4840/tcp	Gallagher	Premier Client [2]

Notes:

1. Port 135 is required for initiating Client/Server connection
2. Required for Premier Client (vEL7.00 or later)

Controllers acquire IP addresses after they issue a BootP broadcast request.

Gallagher Command Centre incorporates a service called FT Bootstrap Protocol Service (BootP). If a controller is isolated from Gallagher Command Centre by a router, BootP broadcasts are likely to be blocked. In this case, either the Gallagher BootP Protocol Service or a third party BootP server needs to be installed in the same network segment as the controller.

Workstation to Server Communications

Classic Workstation Client

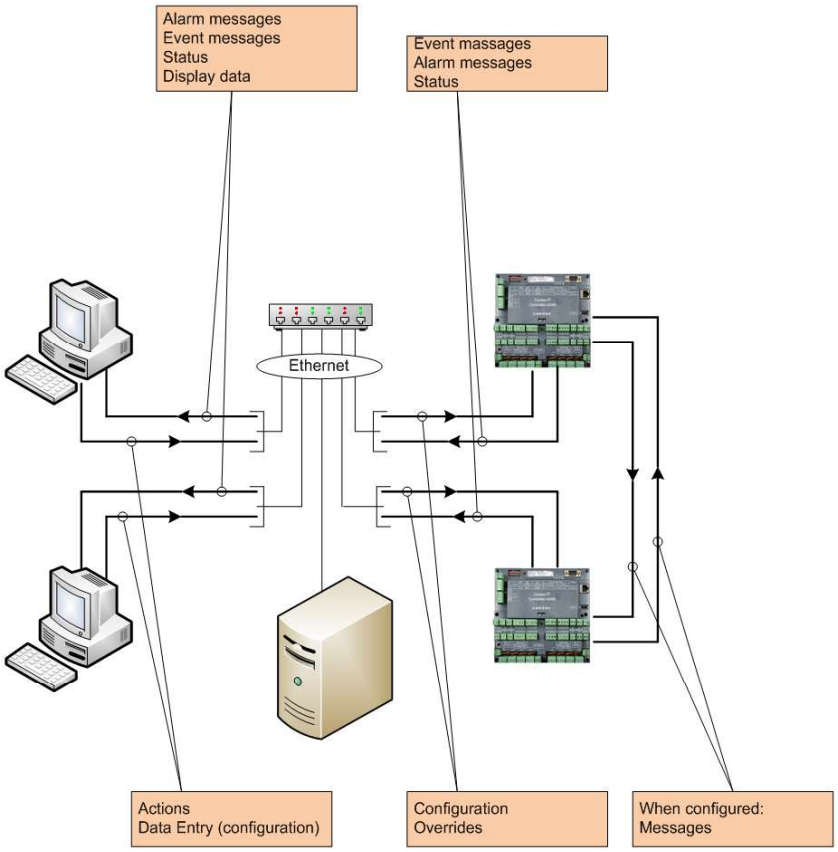
Gallagher Command Centre Server communicates with Gallagher Command Centre Classic workstations using the Distributed Component Object Model (DCOM) over TCP/IP. Because the amount of data transferred between the workstation and server is both substantial and time critical, any TCP/IP infrastructure used by the communications must meet the following minimum standards.

Ping Times < 20 ms Effective data rate > 4 M bit/s

Premier Workstation Client

Gallagher Command Centre Premier Client workstations use OPC (UA) and not DCOM over TCP/IP. As the data transfer time is not critical, a ping test is not relevant to Premier Client.

Network Dataflow



Workstation to Server, Server to Controller and Controller to Controller use Ethernet 10/100/1000BaseT[1] connectivity. The network communication protocol conforms to IEE802.3 specifications.

Multi-Server

Gallagher supports inter-connection of servers for enterprise-wide solutions. Servers connect to each other via TCP/IP, using OPC (UA) data protocol.

Each Gallagher Server enabled with a Multi-Server license, can be configured to establish a secure peer-to-peer relationship with any other similarly licensed Gallagher Server within an organisation. These connections are created in a peer-to-peer matrix structure, where operators on each Server have the ability to operationally view and/or manage items on all other Gallagher Servers on the network. These views can additionally be restricted by Operator divisional view restrictions, allowing an organisation to manage a Multi-Server network in a hierarchical manner, with a head office able to monitor and control subsidiary servers, as the need arises.

Secure server authentication and communications are conducted under the OPC UA (Unified Architecture) security framework. This framework implements strong open encryption algorithms, secure authentication techniques and long key lengths, such as RSA 2048 bit keys and AES 256 bit symmetric encryption.

[1] 1000BaseT is supported in the Gallagher 6000HS controller only.

Port Assignment - Gallagher Command Centre Multi-Server (vEL6.00 and later)

Keyword	Decimal	Description	Function
configurable	4840/tcp	Gallagher	Multi-Server OPC (UA) connection

Cross-site Operational Cover

Each Gallagher Server connecting to an Operator's home server appears as a 'Remote Server' in its own specific Division. A suitably privileged Operator will be able to view certain information from the Remote Server, and override items as if the Operator was connected directly to the Remote Server. This allows organizations to provide cross-site operational cover, where operators from one site can temporarily manage security on a remote site when a remote site Operator may be unavailable. This also allows a head office to maintain control of the security at any time on a remote site should the need arise.

Multi-Server operation should not be considered as a redundant server solution. In the Gallagher environment, each server stores configuration, alarm and event data for the local system only. Alarms and events are received at remote workstations, not the remote server. The exception to this rule is the Cardholder database. This database is replicated to all servers on the system.

Global Access - Cardholders

In a Multi-Server environment, Cardholders are treated as 'Global Items', with their Cardholder details known to all servers on a Multi-Server network. This allows Cardholders to use their same cards/fingerprints/PINs across all sites within a Multi-Server network (eg. a manager with appropriate access rights can travel between sites controlled by separate Gallagher servers, using the one card for entry).