Galil EPICS driver networking guide

Document no: 1

Revision no: 1

Date: 22 April 2015

REVISION HISTORY

Revision	Date	Prepared by	Description
1.0	22/04/2015	Mark Clift	Original

TABLE OF CONTENTS

LIST OF FIGURES

1 Network topology

The network between the IOC and the Galil controllers that it communicates with should be a private network. A private network is strongly recommended for the following reasons:

1. Reduces the probability of IP address conflict
2. Reduces the probability that a broadcast packet will contain a valid Galil command
3. Reduces the probability that a broadcast packet will contain text that causes Galil controller lockup
4. Reduces Ethernet load on the Galil controller

Two recommended private network topologies are shown below, in no particular order.

1.1 Half duplex mode

The older Econo range of Galil controllers only support ½ duplex communication mode (MC8000). Some newer corporate switches are beginning to drop support for ½ duplex communications. In this case the "separate private network" topology is recommended and the local switch is needed to provide the required ½ duplex capability.

1.2 Separate private network

The separate private network topology requires an IOC with two network interface cards (NIC). The first IOC network card faces the main beamline network, and is used for EPICS database access. The second NIC on the IOC connects to an additional layer 2/3 switch, and uses a private subnet. All Galil controllers should be connected on the additional switch, and therefore placed on the private network.
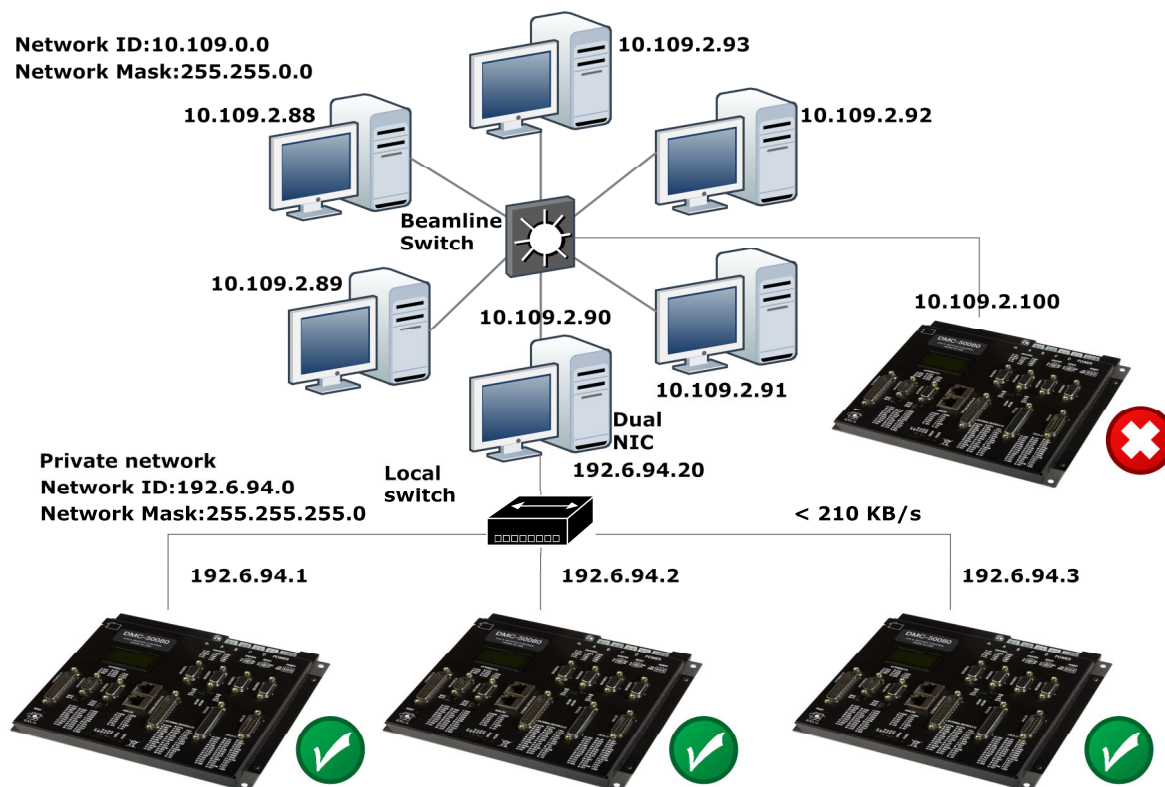

Figure 1 Separate private network

1.3   Configured private network

The configured private network topology requires an IOC with two network interface cards (NIC). The first IOC network card faces the main beamline network, and is used for EPICS database access. A group of ports on the main beamline switch should then be configured to be on a separate private VLAN. The IOC second NIC, and all Galil controllers should then be connected to the main beamline switch using the ports configured to be on the private VLAN.
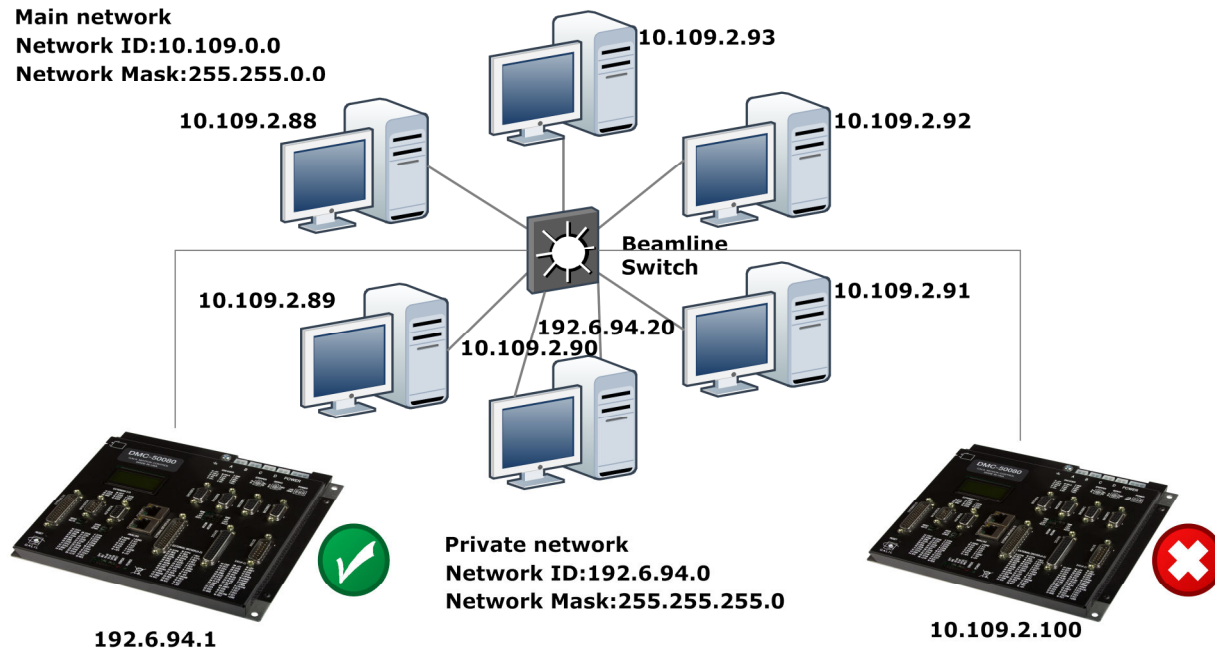

Figure 2 Configured private network

1.4   Open network

When the open network absolutely cannot be avoided, then the network should be configured as shown in figure 3.

Figure 3 Open network

Printed copy of this document is uncontrolled. It is the responsibility of the user to ensure that the correct version of the document is used.
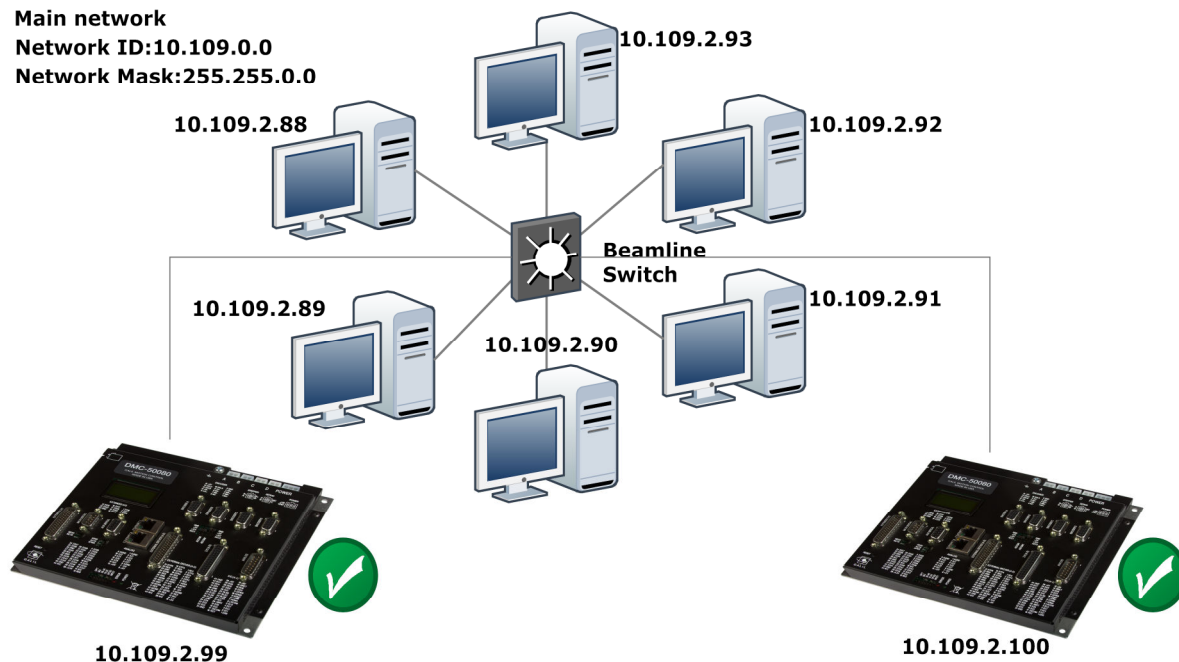
2 Controller configuration

2.1 Disable DHCP

The Galil controller should use a static IP address. Newer Galil controllers have DHCP enabled at the factory, and DHCP is also enabled after a master reset. To disable DHCP complete the following steps.

1. Ensure no firewalls running
2. Connect to the controller using GalilTools, or GalilSuite
3. DH0 – Issue DH0 command to disable DHCP. Connection will drop

2.2 Assigning a static IP address

To assign a static IP address, complete the following steps.

1. Ensure no firewalls running
2. Load GalilTools, or GalilSuite
3. Search for controllers with no IP address
4. Assign static IP address
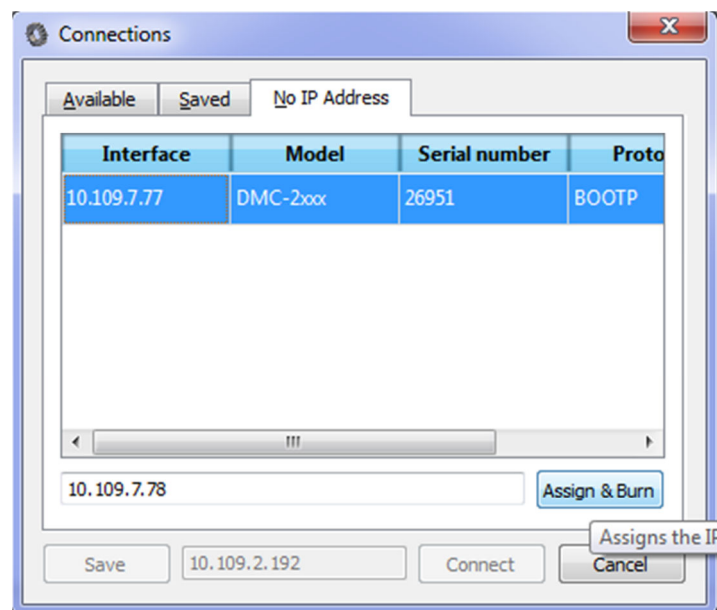
IP address is burnt to controller EEPROM automatically.

Figure 4 Assign IP address

2.3 Broadcast traffic

If the open network installation cannot be avoided, and the controller displays connection dropouts, then it is strongly recommended to configure the Galil controller to block network broadcasts. The main problem with blocking broadcasts is the controller will no longer respond to arp requests, so assigning an IP address will no longer function. In other words, after configuring the controller to block broadcast traffic, the only way to assign a different IP address is by issuing a master reset.

The steps to configure the controller are shown

1. Ensure no firewalls running
2. Connect to controller using GalilTools or GalilSuite
3. IB1 – Block all broadcast packets

Printed copy of this document is uncontrolled. It is the responsibility of the user to ensure that the correct version of the document is used.

4. BN – Burn settings
5. Add static arp entry on IOC host using: Arp –s <ip address> <mac>

After completing this procedure, only the operating system with the static arp rule will be able connect with the controller.

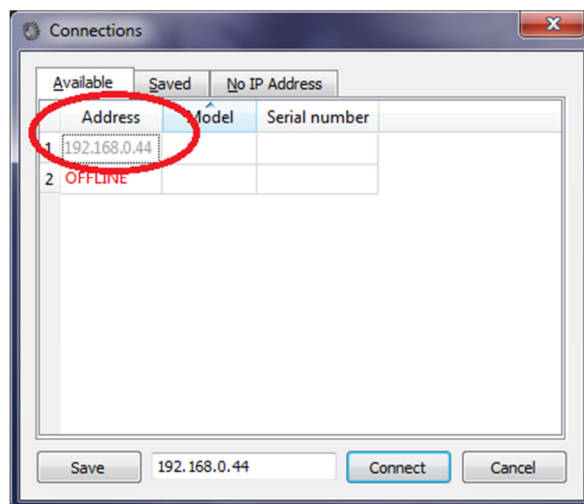Use IB0 to stop blocking broadcast packets if needed.

Figure 5 Controller blocking broadcast traffic

2.4   Block ports

If the controller displays network connection dropouts, then configuring the controller to block most ports below 1000 may help. To block ports below 1000, complete the following steps:

1. Ensure no firewalls running
2. Connect to controller using GalilTools or GalilSuite
3. IK1 – Block most ports below 1000
4. BN – Burn settings

Use IK0 to stop blocking ports below 1000.