

N-TRON Corp.

820 S.University Blvd. Suite 4E

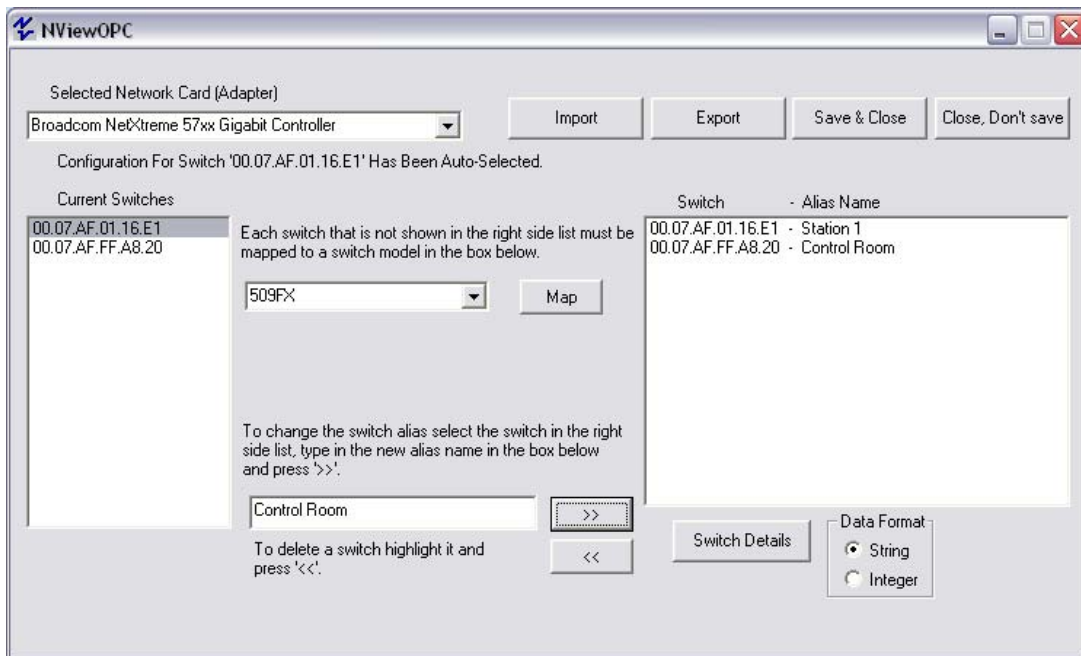
Mobile, Al. 36609

phone: 251-342-2164 fax: 251-342-6353 or 251-342-6436

N-VIEW & Routing

The N-TRON N-View OLE for Process Control (OPC) Server Software will work with industrial standard OPC Client software and most popular Human Machine Interface (HMI) packages to provide complete remote network traffic and status monitoring for N-TRON 200, 300, 400, 500, 700, 900, 7000, and 9000 Series Industrial Switches with the N-View Firmware. N-TRON Industrial Ethernet Switches offer outstanding performance, and ease of use. They are ideally suited for connecting Ethernet enabled industrial and/or security equipment requiring mission critical reliability. The N-View OPC Server in combination with one or more of our industrial switches will add complete network visibility to an HMI Control and Monitoring application.

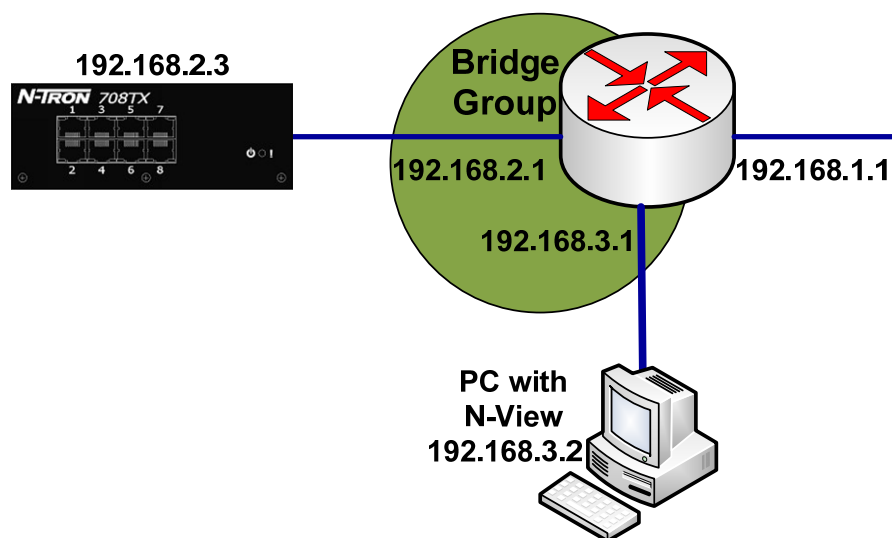
N-TRON Switches with the N-View firmware upgrade (part numbers ending in –N), switches with advanced management features (part numbers ending in –A), and fully managed switches will autocast a small Ethernet frame periodically containing a port-by-port status of the switch. This information includes 5 switch level data points and 41 data points per port. This data is captured by the N-View OPC Server Software and can be displayed by application software running in the same Windows environment with OPC Client capability.



The frames produced by N-View capable switches have a multicast destination MAC address. However, the frames do not map to a multicast IP address having no IP header. This will make the frames unroutable. If a router is used to segment a network, under normal circumstances the N-View frames will be dropped by the router. This will occur even if a multicast routing protocol such as Protocol Independent Multicast is implemented because these frames do not have an IP header.

There are two options in order to view N-View data when there is a router between the network segment with N-Tron switches and the network on which the user is currently located. The first is to install a remote access application on a PC that is on the same network segment as the switches that are to be monitored. The remote user could take control of the device and launch the N-View application to monitor switch information. Applications such as LogMeIn[®], GoToMyPC[®], or Windows Remote Assistance have this capability and frequently have free versions.

The second option is to configure transparent bridging. With transparent bridging chosen interfaces are connected together in a bridge group and will functionally operate like a Layer 2 switch. Frames destined to a multicast address will forward out any interface in the bridge group. This is the simplest form of transparent bridging.



To configure bridging in this fashion, the following commands would be used on a Cisco router. The particular model used was a Cisco 3640 running IOS version 12.4(5a). Differences in configuration may exist between models and certainly between vendors. If a different vendor is in use, the concepts will remain the same but the configuration will differ.

```
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#bridge 1 protocol ieee  
Router(config)#interface ethernet0/0
```

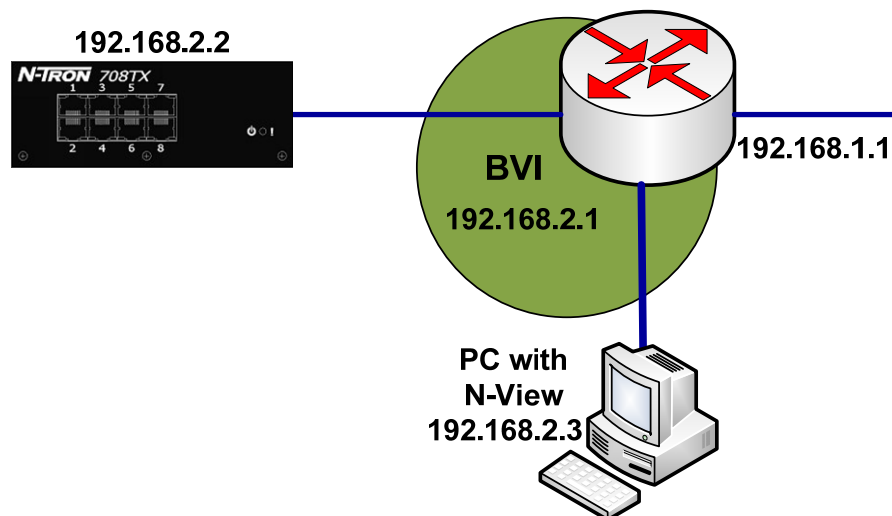
```

Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#bridge-group 1
Router(config-if)#bridge-group 1 spanning-disabled
Router(config-if)#exit
Router(config)#interface ethernet0/1
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#bridge-group 1
Router(config-if)#bridge-group 1 spanning-disabled
Router(config-if)#exit

```

The command *bridge-group 1 spanning-disabled* is optional. Enabling bridging will cause 802.1D Spanning Tree frames to be originated by the router to prevent bridging loops. In a topology, shown, this is unnecessary so the spanning tree protocol is disabled.

In order to route data off the network segment, Integrated Routing and Bridging should be used. This calls for the removal of IP addresses from the interfaces being bridged and the creation of a virtual interface called a Bridged Virtual Interface (BVI). The BVI will be configured with an IP address in the same subnet as the devices being bridged. The BVI will allow bridging of traffic that should be bridged, and anything destined to the BVI that needs to be routed off the network segment will be routed accordingly.



```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#bridge 1 protocol ieee
Router(config)bridge irb
Router(config)bridge 1 route ip
Router(config)interface BVI1
Router(config-if)ip address 192.168.2.2
Router(config-if)exit

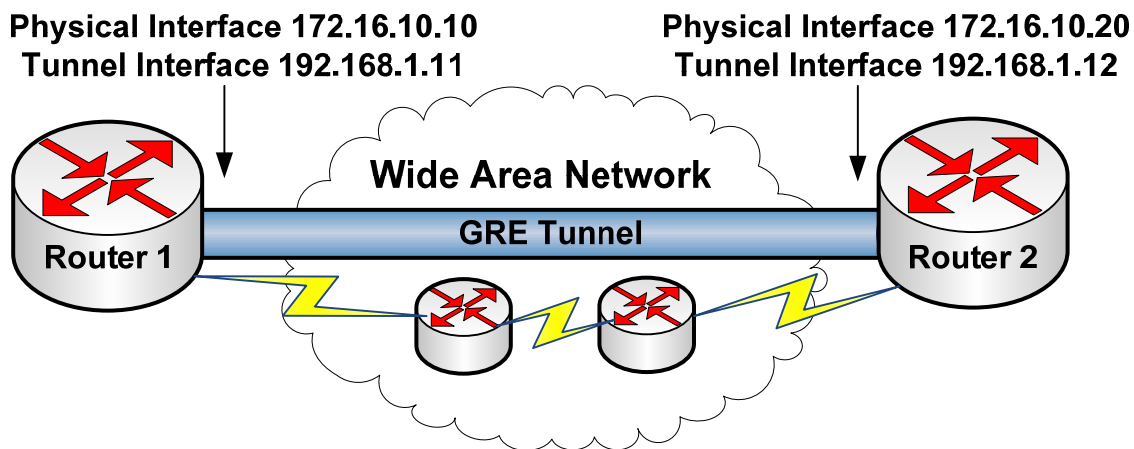
```

```

Router(config)#interface ethernet0/0
Router(config-if)#bridge-group 1
Router(config-if)#bridge-group 1 spanning-disabled
Router(config-if)#exit
Router(config)#interface ethernet0/1
Router(config-if)#bridge-group 1
Router(config-if)#bridge-group 1 spanning-disabled
Router(config-if)#exit

```

If there is a need to have the frames traverse a Wide Area Network, a General Routing Encapsulation (GRE) tunnel can be used. GRE will add an additional header to the frame. This in turn will have an IP header added containing the IP address of the tunnel endpoint making the entire datagram routable.



Once the GRE frame is received at the tunnel endpoint the encapsulation will be removed. The two devices on the end points of the tunnel will appear to be directly connected.

```

Router1(config)#interface Tunnel1
Router1(config)#keepalive
Router1(config-if)#ip address 192.168.1.11 255.255.255.252
Router1(config-if)#tunnel source 172.16.10.10
Router1(config-if)#tunnel destination 172.16.10.20
Router1(config-if)#exit
Router1(config)#end

```

```

Router2(config)#interface Tunnel2
Router2(config)#keepalive
Router2(config-if)#ip address 192.168.1.12 255.255.255.252
Router2(config-if)#tunnel source 172.16.10.20
Router2(config-if)#tunnel destination 172.16.10.10

```

```
Router2(config-if)#exit  
Router2(config)#end
```

The command *keepalive* is optional. GRE tunnels are stateless by default. If one side goes down the other side will remain up unless keepalives are implemented. It is also important to note that the addresses used as the tunnel destination must be reachable by the router itself either through the use of static routes or through a dynamic routing protocol. A complete discussion of GRE tunnels is outside the scope of this document. Careful consideration to their use should be considered as they can complicate network design.