WorkstationST* Network Monitor Instruction Guide

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

Public Information – This document contains non-sensitive information approved for public disclosure.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

GE provides the following document and the information included therein as is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Revised: Dec 2019
Issued: March 2003


* Indicates a trademark of General Electric Company and/or its subsidiaries. All other trademarks are the property of their respective owners.

We would appreciate your feedback about our documentation. Please send comments or suggestions to controls.doc@ge.com
## Document Updates

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Custom Network Switch Layout Configuration</td>
<td>Added Monitoring properties to the Network Switch Layout Configuration Properties table</td>
</tr>
<tr>
<td></td>
<td>Switch Stacking and Hardware Monitoring</td>
<td>New section</td>
</tr>
<tr>
<td>M</td>
<td>Network Switches</td>
<td>Updates to the table Network Switch Port Configuration Properties include updates to Trunk Port property and adding the following new properties for new port connection types:</td>
</tr>
<tr>
<td></td>
<td>Redundant HMI Example without HMI Trunk Ports</td>
<td>These sections have been removed; configuration is no longer supported at the device level</td>
</tr>
<tr>
<td></td>
<td>Redundant HMI Example with HMI Trunk Ports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller Example</td>
<td>Updated to provide overview, configuration details for new sites, upgrade instructions for existing sites, support for newly qualified NetworkST standard switch types, and custom configuration</td>
</tr>
<tr>
<td></td>
<td>Network Switch Layout Overview and Configuration</td>
<td>Updated ControlST version and provided the table Network Switch Layout Version Compatibility</td>
</tr>
<tr>
<td>L</td>
<td>Network Switches</td>
<td>Updated the table Network Switch Configuration Properties with the Switch Layout Type property</td>
</tr>
<tr>
<td></td>
<td>Configure Network Switch Configurations to Use Management Network</td>
<td>Update screenshot to include the Switch Layout Type property</td>
</tr>
<tr>
<td></td>
<td>Network Switch Layout Configuration</td>
<td>New section</td>
</tr>
<tr>
<td></td>
<td>Thin Client HMI Support</td>
<td>Chapter moved from this document to the WorkstationST Control System Health Instruction Guide (GEI-100834) as the Thin Client can only be configured from the CSH</td>
</tr>
<tr>
<td>K</td>
<td>Introduction</td>
<td>Updates for clarification purposes</td>
</tr>
<tr>
<td></td>
<td>Network Switches</td>
<td>Updated with additional port connection properties</td>
</tr>
<tr>
<td></td>
<td>Assigning Ports</td>
<td>Removed this section and incorporated content in section Network Switches; switch port connection is modified in the network switch Component Editor instead of at each component's network adapter.</td>
</tr>
<tr>
<td>J</td>
<td>Network Switch SNMP Configuration</td>
<td>New chapter added to distinguish SNMP V1 and SNMP V3 protocol configuration</td>
</tr>
<tr>
<td></td>
<td>Troubleshoot Network Switch SNMP Issues</td>
<td>Renamed this chapter and updated the first paragraph and related figure for SNMP V1 and SNMP V3 protocol clarification</td>
</tr>
<tr>
<td>H</td>
<td>Configuration</td>
<td>Replaced the screenshot of Network Monitor Configuration properties, removed unnecessary procedures, and added the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network Monitor Alarm Configuration Parameters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network Monitor Data Acquisition Configuration, including a Note to further explain the Network Monitor rate settings and how to tune the parameters to avoid an HMI freezing up</td>
</tr>
</tbody>
</table>

## Related Documents

<table>
<thead>
<tr>
<th>Doc #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6700 or GEH-6703</td>
<td>ToolboxST User Guide for Mark Controls Platform</td>
</tr>
<tr>
<td>GEI-100834</td>
<td>WorkstationST Control System Health</td>
</tr>
<tr>
<td>GEI-100828</td>
<td>WorkstationST OPC UA Server</td>
</tr>
</tbody>
</table>
# Contents

1 Introduction ............................................................................................................................................. 4

2 Configuration ........................................................................................................................................... 5
   2.1 Network Monitor Alarm Configuration Parameters ........................................................................ 5
   2.2 Network Monitor Data Acquisition Configuration ...................................................................... 6
   2.3 System Information ......................................................................................................................... 7
   2.4 Networks ......................................................................................................................................... 9
   2.5 Network Switches .......................................................................................................................... 10
   2.6 Network Status and Troubleshooting ........................................................................................... 15

3 Alarms .................................................................................................................................................... 23

4 Switch Management Network Support ............................................................................................... 25
   4.1 Add Management Network to System Topology ........................................................................... 26
   4.2 Configure Network Switch Configurations to Use Management Network ....................................... 28
   4.3 Network Switch Layout Overview and Configuration ................................................................... 30
   4.4 Switch Stacking and Hardware Monitoring .................................................................................... 40
   4.5 Configure Local HMI Management Address .................................................................................. 52
   4.6 Add Local HMI Management Address to PDH Adapter in Workstation ....................................... 53

5 Configure Local HMI Management Address for Systems without Switch Management Network ........ 54
   5.1 Configure Local HMI Management Address .................................................................................. 54
   5.2 Add Local HMI Management Address to PDH Adapter in Workstation ....................................... 55

6 Network Switch SNMP Configuration .................................................................................................. 56
   6.1 New System Configuration .............................................................................................................. 56
   6.2 ControlST Upgrade ......................................................................................................................... 66
   6.3 Network Switch Replacement (Upgrade) ........................................................................................ 67

7 Troubleshoot Network Switch SNMP Issues ....................................................................................... 68
1 Introduction

The WorkstationST* Network Monitor provides the status of all devices (such as controllers, computers, and network switches) that are defined in the system and connected to at least one of the Ethernet-based networks. The Network Monitor also provides information about the health of each network switch and network switch ports. The Network Monitor uses the Windows® Simple Network Management Protocol (SNMP) component to communicate with the network switch components.

The Network Monitor also allows proactive network maintenance by providing visual indications and alarms of abnormal conditions. These include devices not connected in their configured location, unknown devices being connected to a switch, or attempts to gain unauthorized access to switch SNMP data. During system startup, the Network Monitor determines where the devices are physically connected. During normal system operation, changes in network topology should not occur; therefore, any changes would indicate an abnormal condition. For example, devices may be incorrectly reconnected after a network switch is replaced or new network cables are run. This feature can be very useful as a debugging tool because it allows network issues to be identified or ruled out very quickly.

The Network Monitor also enhances network stability and security by providing alarms in the event of an unauthorized connection to the network.

Beginning with ControlST* Software Suite V04.07, the ToolboxST* application allows switch port connection information modification within the network switch Component Editor, rather than at each component’s network adapter. During upgrade, ToolboxST imports the component network adapter information into each network switch’s configuration when the switch is first modified in the new version. Computers running WorkstationST V04.06 and earlier use the component network adapter modified information. Although it is no longer be possible to view or edit the component network adapter switch connection information at each Component Editor, any information that was configured prior to the upgrade will remain available for any WorkstationST computer that has not been upgraded. All upgraded WorkstationST computers will use the new switch-centric information. After the upgrade, any change to the network switch connection information from the switch Component Editor will not be available for computers in a control system running WorkstationST V04.06 and earlier. These computers will need to be upgraded in order to use the network switch connection information changes.
# 2 Configuration

The Network Monitor is configured from the WorkstationST Network Monitor tab using the configuration properties (parameters).

![WorkstationST Network Monitor Tab Properties](image)

## 2.1 Network Monitor Alarm Configuration Parameters

The parameters associated with the Network Monitor alarms are as follows:

**Network Monitor Alarms**

*Enable Alarm On Intrusion Detection Threshold Exceeded* when enabled generates an alarm when the intrusion detection counter delta threshold is exceeded.

*Enable Alarm On Loss of Device Communication* when enabled generates an alarm whenever network communications are lost with a device.

*Enable Alarm On Topology Error* when enabled generates an alarm when a device is not connected to its configured port.

*Enable Alarm On Unknown Device Connected* when enabled generates an alarm when an unknown device is connected to any of the defined networks.

*Enable Event On Intrusion Detection Threshold Exceeded* when enabled generates an event when the intrusion detection counter delta threshold is exceeded.

*Enable Event On Loss of Device Communication* when enabled generates an event whenever network communications are lost with a device.

*Enable Event On Topology Error* when enabled generates an event when a device is not connected to its configured port.

*Enable Event On Unknown Device Connected* when enabled generates an event when an unknown device is connected to any of the defined networks.
2.2 Network Monitor Data Acquisition Configuration

The parameters associated with the Network Monitor data acquisition are as follows:

**Network Monitor Data Acquisition**

**Device Network Communication Status Request Rate (seconds)** is the number of seconds between device network communication status requests. Decreasing the rate makes detection of device communication status changes faster at the cost of using additional network bandwidth. Increasing the rate reduces the amount of network bandwidth used at the cost of slowing down the speed of detection of device communication status changes.

**Intrusion Detection Delta Threshold** is the delta of intrusion detection counter values over the device SNMP request period that will trigger an intrusion alarm or event.

**Switch SNMP Data Request Rate** is the number of seconds between SNMP queries of the network switches. Decreasing the rate makes detection of switch port status changes and connected device changes faster at the cost of using additional network bandwidth and increased CPU usage on the host computer. Increasing the rate reduces the amount of network bandwidth used at the cost of slowing down the speed of detection of switch port status and connected device status.

**Local HMI Management Address** is the address configured in the switch access list (ACL) for SNMP requests.

---

**Note** The Network Monitor Data Acquisition request rate settings are used to tune the performance of the Network Health monitoring based on the size of the system and the capabilities of the hardware hosting the Control System Health feature. Lower Request Rates (polling periods) increase the frequency of the data requests and provides faster detection of issues at the expense of consuming higher network bandwidth and CPU resources on the host computer. Higher values for the Request Rates results in a lower frequency of requests, which ultimately results in slower updates while consuming less network and host computer resources. The default rates provide very fast updates in small systems, but can easily overwhelm the host computer in a large system. The Request Rate settings are used to tune the Network Health monitoring to achieve the best compromise of performance and resource usage based on the priorities of the site. If a site wants to minimize detection delays and is willing to accept higher network bandwidth usage and CPU usage on the host computer, they can increase the polling frequency by decreasing the Request Rate setting. If the site is sensitive to network bandwidth usage and needs good performance for other applications on the host computer, they can reduce the polling frequency by increasing the Request Rate setting.

Many factors come in to play and each site is different so there is no simple calculation for performance versus resource usage. The best way to determine actual system behavior is to adjust the rate settings until an acceptable balance of performance and hosting computer resource usage is achieved at the site.
2.3 System Information

The system network drawing displays all physical networks, as well as network switches and devices, their physical locations, and their interconnection. The host name and IP address of each device network connection on a per network basis, as well as the switch and port where the physical connection is made is also provided. This information is entered for the network switches and devices as they are added to the system in the ToolboxST application. Samples of information contained in the system network drawing are as follows.
2.4 Networks

Information from the system network drawings must be entered into the ToolboxST System Editor, as well as the ToolboxST devices. When a new system is created in the ToolboxST application, it automatically includes a Unit Data Highway (UDH) network. This is the default controller-level network to which all controllers are connected. The Network Monitor only attempts to monitor devices connected to networks configured with media type Ethernet and Transport type IP. Additional networks are added as needed.

The UDH network has a default Media value of Ethernet and a default Transport value of IP.
2.5 Network Switches

After the networks have been added, add and configure the network switches to define device network connections for the devices as they are added to the system. This allows the device network connections to be defined as the devices are added to the system.

➢➢ To add a network switch to the system

From the System Editor Tree View, right-click the system and select Insert New and Network Switch.

The Network Switch Device Creation Wizard displays.

Select Name and enter a name for the switch (such as NS1).

Select Number Of Ports and enter the number (such as 48).

Click Finish.

The new switch displays in the Tree View and Summary View.
➢ To configure a network switch

1. From the System Editor Tree view, double-click a Network Switch to display the Component Editor.

2. From the Component Editor Tree view, select General (top-level node) to display the Property Editor containing the network switch configuration properties.

3. Modify the properties to configure the network switch.

---

### Network Switch Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Holds the user entered description for the switch. This text is displayed in the switch ToolTips in the Network Status Viewer and should include the physical location of the switch in order to help maintenance personnel locate and identify the switch in the event of a failure.</td>
</tr>
<tr>
<td>GE Part Number</td>
<td>Optional setting</td>
</tr>
<tr>
<td>Host Name</td>
<td>Part of the communication path</td>
</tr>
<tr>
<td>Management IP Address</td>
<td>Configured management IP address of the switch</td>
</tr>
<tr>
<td>Management Network</td>
<td>Network associated with the management interface of the switch</td>
</tr>
<tr>
<td>Number of Ports</td>
<td>Specifies the number of switch ports. Note that for a stacked switch arrangement, the total number of ports for both switches should be specified.</td>
</tr>
<tr>
<td>Protection</td>
<td>Shows access rights for the device</td>
</tr>
<tr>
<td>Switch Layout Type</td>
<td>Specifies the type of switch. If a switch type cannot be found that matches the actual switch, one of the generic switch types can be used. Unknown switch types may require trial and error in order to find a switch type that matches the behavior of the actual switch. switch layout type.</td>
</tr>
<tr>
<td><strong>SNMP Overrides</strong></td>
<td></td>
</tr>
<tr>
<td>SNMP Local Parameter Override</td>
<td>When True, these local switch SNMP settings are used. When False, the SNMP settings from the Network Monitor are used.</td>
</tr>
<tr>
<td>SNMP Mode</td>
<td>Sets SNMP mode used to read SNMP data from the network switches</td>
</tr>
</tbody>
</table>

---

For instructions to configure the SNMP, refer to the section Network Switch SNMP Configuration.
Network Switch Configuration Properties (continued)

<table>
<thead>
<tr>
<th>SNMP V1 Community</th>
<th>SNMP V1 Community name configured in the network switches. This value must match the SNMP Community value configured in the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch SNMP Data Request Rate</td>
<td>Number of seconds between SNMP queries of the network switches</td>
</tr>
</tbody>
</table>

➢ To configure the network switch port properties

1. From the **Tree View**, select a Port # to display the Property Editor containing the network switch port configuration properties.

2. Modify the properties to configure the network switch port.

![Property Editor Screenshot](image-url)
### Network Switch Port Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>Defines the type of connection made to the port. The available options are as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default_NativeDeviceConnectionOrNotUsed</strong>: used in the typical case when there is a single native device (a device represented in the system configuration) connected to the port, or the port is unused. Most ports will use this setting, except for the special cases below.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Trunk Port</strong>: selected when the port is used to connect to another switch. Trunk ports are critical to network communications and alarms will be generated in the event that a configured trunk port is down or disabled. The description field for Trunk Ports is included in the Network Status Viewer ToolTip for the port and also in the alarm text for trunk port alarms. The description should include the name and port of the switch that this port is connected to in order to facilitate troubleshooting network issues.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Server</strong>: selected when the port is connected to a server device that is hosting a hypervisor and Virtual Machines (VM). When this port type is selected, only the port status is monitored and an alarm is generated if the port is down. The Server connection type is used for connections to Control Servers, Security Servers, and any third-party hypervised equipment connected to the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Thin Client</strong>: selected when the port is connected to a Thin Client terminal. When this connection type is selected, only the port status is monitored and an alarm is generated if the port is down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Gateway</strong>: selected when the port is connected to a router or third-party network. This connection type is also used for ports connected to multiple devices via a hub. When this connection type is selected, only the port status is monitored and an alarm is generated if the port is down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Temporary Gateway</strong>: selected when the port is connected to a hub, router, or non-critical third-party network. When this connection type is selected, the port status is monitored but no alarms are generated when the port is down. An example of this type of connection is a connection to a remote access network that is enabled only during remote troubleshooting.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ThirdPartyCriticalDeviceConnection</strong>: used to specify a port that is connected to a third-party device (a device not represented in the system configuration) that is critical to the operation of the plant and is expected to be online at all times. Alarms will be generated in the event that the port is down or disabled. The description field for critical third-party connection ports is included in the Network Status Viewer ToolTip for the port and also in the alarm text for any alarms generated for the port. The description should include information about the device the port is connected to so that the Network Status Viewer display and the alarms associated with the port provide information about the connected device to the user. This designation also serves the purpose of suppressing Unknown Device alarms associated with the port. If a third-party device is connected to a port using the default selection, the MAC Address of the connected device will not match any of the native devices and an Unknown Device alarm will be generated for the port.</td>
</tr>
<tr>
<td></td>
<td>- <strong>PeripheralDeviceConnection</strong>: used to specify a port that is connected to a third-party device (a device not represented in the system configuration) that is not critical to the plant operation and may not always be online, such as a printer. Alarms are only generated for the port in the event that the port is disabled. This designation also serves the purpose of suppressing Unknown Device alarms associated with the port.</td>
</tr>
<tr>
<td><strong>Port Connection</strong></td>
<td>Holds the user entered description for the port. This text is displayed in the Network Status Viewer ToolTip for the port, and the text is included in alarms generated for the special case Port Connection settings described below.</td>
</tr>
<tr>
<td><strong>Port Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Port Number</strong></td>
<td>Port number</td>
</tr>
</tbody>
</table>

**Note** Systems with Control Servers will use the Control System Health (CSH) feature instead of Network Monitor. Network Monitor is a legacy feature that does not support monitoring Control Server elements and network connections.
### Network Switch Port Configuration Properties (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>Speed and specifies whether the port is copper or fiber-based. Available options are:</td>
</tr>
<tr>
<td></td>
<td>• 10Base-T</td>
</tr>
<tr>
<td></td>
<td>• 100Base-T</td>
</tr>
<tr>
<td></td>
<td>• 100Base-FX</td>
</tr>
<tr>
<td></td>
<td>• 1000Base-T</td>
</tr>
<tr>
<td>Port Connection</td>
<td>Network Component Component or controller within a controller set</td>
</tr>
<tr>
<td></td>
<td>Network_1 Name of the connected network</td>
</tr>
<tr>
<td></td>
<td>Network_1 IP Address IP address of the Network Adapter connected to this port</td>
</tr>
<tr>
<td></td>
<td>Network_2 Second network name. Only available for WorkstationST components.</td>
</tr>
<tr>
<td></td>
<td>Network_2 IP Address second IP address of the Network Adapter connected to this port. Only available for WorkstationST components.</td>
</tr>
<tr>
<td></td>
<td>Primary Network WorkstationST components can be configured with an arrangement where a single network port can service two networks on a workstation, one Primary and one Backup. When set to True, this is designated as the Primary network. Available on WorkstationST component types only.</td>
</tr>
</tbody>
</table>

Some components (such as the WorkstationST component) can support redundant network interface connections (NICs). Switch connection allows the Backup switch and port number to be specified on a switch port from the Network Component property.

With redundant NICs, the active NIC displays as the active connection for the device and the redundant port link status will be up but no actual device connection is recognized by the switch. The Network Status Viewer shows that the redundant connection for the device is functioning correctly as long as the redundant port link status is up. The Network Monitor generates an alarm if either the configured Primary or Backup port is down, which gives an immediate indication of a failure in the redundant communications path for the device.
2.6 **Network Status and Troubleshooting**

The system network status can be used to troubleshoot issues with the network. The system network status can be viewed in several ways: from the System Editor Summary View, the Network Status Viewer, or from the Network View tab.

### 2.6.1 System Editor Summary View

The Summary View in the ToolboxST System Editor displays all system components and their simplified connections to the defined networks. It also displays the composite health of the connection of each device to each network by displaying healthy connections with a green line and unhealthy connections with a red or orange line.
2.6.2 Network Status Viewer

The Network Status Viewer allows you to troubleshoot network issues down to the device level. This utility retrieves status data from the Network Monitor.

➢ To open the Network Status Viewer: From the System Editor View menu, click Network Status Viewer to display the Network Status Viewer.
2.6.3 Network View Tab

The Network View tab displays the network hierarchy; the networks are the top-level items. The switches are at the next level, followed by the devices.
2.6.4 Device View as Configured Tab

The Device View As Configured tab displays the devices in their configured locations, as well as deviations of the device connections from their configured locations. This is used to find occurrences of a device connected to the wrong port that is masking the location of an offline device configured to be connected to that port.
The following screen displays the configured and connected device views with the switch connections expanded.
2.6.5 **Device View by Connection Tab**

The Device View By Connection tab displays the actual location of each device by the network switch and port.
2.6.6 Network Troubleshooting Example

The following is an example of the Network Status Viewer being used to determine any network issues, the devices affected, and the cause.

This sample screen displays no issues with the **LegacyUDH**, one error on the **UDH**, and a topology error on the **PDH** networks.
To display the UDH network issues, expand the UDH item.

Expand Switch2 to display all issues related to that switch. This example displays that multiple devices configured to be connected to this switch are offline, and several others are online but not connected in their configured locations.
3 Alarms

The Network Monitor generates alarms and maintains them in an internal queue. The WorkstationST Alarm Server feature can be configured to connect to the Network Monitor, which allows you to receive and display Network Monitor alarms.

From the WorkstationST Component Editor, Alarms tab, under Network Monitor Interface, select Connect To Network Monitor and set to True.

Select Network Monitor Hostname and enter the appropriate IP address.
Network Monitor-generated Alarms Example

<table>
<thead>
<tr>
<th>Device Time (UTC)</th>
<th>Recorded Time (UTC)</th>
<th>Type</th>
<th>Status</th>
<th>Class</th>
<th>Device</th>
<th>OPC Severity</th>
<th>Ack.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>2009-06-25 22:30:01.315</td>
<td>2009-06-26 22:30:01.315</td>
<td>Alarm</td>
<td>ALARMED</td>
<td>Alarm</td>
<td>Ethernet</td>
<td>1</td>
<td>N</td>
</tr>
</tbody>
</table>

Network Monitor-generated Alarms Example
4 Switch Management Network Support

Switch management and periodic data collection from the switches through SNMP has traditionally been done over the PDH (plant scope) network. The switches have traditionally been given PDH IP addresses and the management interface has been associated with the PDH VLAN in the switches. This approach exposes the network switch management interface to any device on the PDH network.

A more secure architecture uses an isolated Switch Management network for switch configuration management and data gathering. Further security can be achieved by limiting access to this network to a single PC in the system. Sites configured to use a separate Switch Management network implement this arrangement with enhanced switch and router configurations. The ToolboxST application and the WorkstationST features have been modified to support this new network topology.

A series of steps must be performed to configure the WorkstationST Network Monitor feature to support systems with an isolated Switch Management network. As an example, we start with this simple system containing a PDH (plant scope) and UDH (unit scope) network, two network switches, a single Workstation PC and two controllers.

![Initial System Topology](image-url)
4.1 Add Management Network to System Topology

➢ To add a new network to the system

From the Tree View, right-click the system icon, select Insert New and Network.

From the New Network dialog box, enter a Name (the convention is to use MGH) and Description (such as Switch Management).

Click OK.

From the Property Editor, select Scope and select Management from the drop-down list.

Select Media and select Ethernet from the drop-down menu.

Select Transport and select IP from the drop-down list.
System Topology with new Network
4.2 Configure Network Switch Configurations to Use Management Network

Specify the management network and the management address for all of the switches in the system.

➢ To configure a network switch

1. From the System Editor Tree view, double-click a Network Switch to display the Component Editor.
2. From the Component Editor Tree view, select General (top-level node) to display the Property Editor containing the network switch configuration properties.
3. Select Management IP Address and enter the appropriate IP address.
4. Select Management Network and select MGH from the drop-down list.
5. Repeat this procedure for each network switch in the system.

The Summary View displays all of the switches connected to the management network, as displayed in the following figure.
4.3 Network Switch Layout Overview and Configuration

Beginning with ControlST V07.06.00C, Network Switch Layouts provide enhanced network switch management features. Network Switch Layouts provide the mapping between the internal switch interfaces and the physical switch ports, which enables the Network Monitor feature to read the switch data over SNMP and display the data with the correct physical port location.

**Note** This feature was also added to some previous versions of ControlST and single-product releases. Refer to the table Network Switch Layout Version Compatibility for a complete version compatibility list.

Two types of Network Switch layouts are supported:

- **GE standard switch layout definitions**: standard switch layout definitions that are provided as part of the ControlST product. The standard switch layout files correspond to the standard switch types qualified for NetworkST. GE standard layouts cannot be modified.
- **Custom switch layout definitions**: custom switch layouts can be created to support non-standard switch types.

The use of switch layouts has been designed to provide the following improvements:

- **Support for newly qualified switch types independent of ControlST releases**: in previous ControlST versions, the network switch layouts were hard coded in the release. Support for newly qualified switches was only available as part of the next ControlST release and required, at a minimum, an update of ToolBoxST and WorkstationST. ControlST V07.06.00C and later (or previous versions specified in the table Network Switch Layout Version Compatibility) moved the switch-specific code to a switch layout file. The switch layout file is updated as new switches are qualified, and this file can be sent to existing sites that need to support the new switch type independently of the ControlST release cycle and without the need to upgrade to a newer version of ControlST.

- **Minimize the impact of switch operating system changes**: network switch vendors periodically update the switch operating systems, and in some cases these changes have required ControlST updates to support new behaviors that were introduced as part of the operating system update. The switch layout files have been designed to minimize the impact of internal switch layout changes. In the event that internal switch changes cannot be supported by an existing switch layout, a new switch layout will be included in the next ControlST release. A new layout file can be requested to provide the ability to import the new switch layout into the site’s existing ControlST version. Refer to the table Network Switch Layout Version Compatibility for a complete version compatibility list.

- **Support for unqualified (custom) switch types**: GE standard switch layouts are provided for all NetworkST standard switch configurations. Support for non-standard switch types can be added by creating custom layout files.

### Network Switch Layout Version Compatibility

<table>
<thead>
<tr>
<th>ControlST Version</th>
<th>Single-product Release Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>V07.04.05C SP04 (and higher within V07.04 branch)</td>
<td>ToolBoxST V07.04.09C and higher</td>
</tr>
<tr>
<td></td>
<td>WorkstationST V07.04.09C and higher</td>
</tr>
<tr>
<td>V07.05.00C SP01 (and higher within V07.05 branch)</td>
<td>ToolBoxST V07.05.01C and higher</td>
</tr>
<tr>
<td></td>
<td>WorkstationST V07.05.01C and higher</td>
</tr>
<tr>
<td>V07.06.00C and higher</td>
<td>ToolBoxST V07.06.00C and higher</td>
</tr>
<tr>
<td></td>
<td>WorkstationST V07.06.00C and higher</td>
</tr>
</tbody>
</table>
4.3.1 Configure Switch Layouts for New Sites

When configuring a new system with a ControlST version that supports the Network switch Layout feature (refer to the table Network Switch Layout Version Compatibility), only the GE standard switch layouts are available by default. The GE standard switch layouts correspond to the standard switch types supported by NetworkST. The following figure displays the switch device Switch Layout Type property with the list of available switch layout types.

**Note** Layouts for GE standard NetworkST switch types always begin with GE, followed by the switch manufacturer, model number, and any model-specific options (GE_<Manufacturer>_<Model>_<Options>).

The GE standard switch layouts support any NetworkST qualified Cisco® switch. Switches from other manufacturers have been supported on a legacy basis but it is not anticipated that these switches will be used often in new systems. If support for a legacy switch type is required on a new system, legacy switch support can be enabled using the following procedure.
➢ To enable legacy switch support on a new system

1. From the System Information Editor Tree View, select Network Switch Layouts to display the supported switch layouts.

2. From the Property Editor, set the Enable Legacy Switch Support property to True to display the legacy switch layouts.
Enable Legacy Switch Support

When true, legacy switch layout types are included in this display.

Is a legacy layout

Legacy layouts cannot be edited.
When this setting is enabled (True), the legacy switch types are available for selection when modifying the network switch configuration, as shown in the following figure.

Note Always use the GE standard switch layouts when available. For example, always use the GE_CISCO_2960_24Port layout but never use the legacy Cisco_Catalyst_2960 layout. In the case where a supported legacy switch such as the Enterasys_N1 is required, the legacy layout must be used because there are no GE standard layouts defined for Enterasys switches.

Refer to section Custom Network Switch Layout Configuration for the procedure to create custom switch layouts. For example, the GE standard switch layouts only support 24 port versions of the Cisco 2960 switch. Support for a 48 port Cisco 2960 switch is not available with the GE standard layouts, but a custom switch layout can be created to allow monitoring of this non-standard switch type.

Note The custom layout is used for qualifying new switch types and cannot be used for normal operation. The switch is not monitored when the custom layout is selected.
4.3.2 Manage Switch Layouts when Upgrading Existing Sites

When a system that was created by an older version of ControlST is opened in ToolboxST V07.05.01C or later, the legacy switch support is enabled by default, and the existing switch configurations remain valid without opening or building the existing switch configurations. Although it is not necessary to upgrade the switch configurations, the best practice is to upgrade any Cisco switches to the GE qualified layout if one is available. For example, a switch configured for the legacy Cisco_Catalyst_2960 layout should be updated to use the GE_CISCO_2960_24Port layout. Updating the switches to the GE qualified switch layouts will insulate the site against future switch operating system changes that are most likely to occur if a switch fails and is replaced with a newer version.

Whenever a GE standard switch layout is selected for a switch type that supports stacking, stacking is enabled by default and the number of switches in the stack is initialized to the maximum stack size defined by the switch layout type. Do not forget to modify these properties to match the actual layout of the switch being configured.
4.3.3 Add Support for Newly Qualified NetworkST Standard Switch Types

New GE standard switch layouts are created as new switch types are qualified for NetworkST. The new standard switch layouts are added to the GeSwitchLayouts.xml file, which is then used to update older versions of ControlST with the latest standard switch layouts. Any ControlST version that supports the GE standard switch layouts (V07.05.01C and later) can be updated to support the latest GE standard switch layouts by updating the GeSwitchLayouts.xml file. Simply copy the latest GeSwitchLayouts.xml file to the top level of the ToolboxST project directory (the directory where the .tcw file is located), then close ToolboxST and re-open the project to make the new GE standard switch layouts available.

**Note** For systems under CMS source control, first check out the system configuration (check out from the root tree node of the system overview), then copy the new GeSwitchLayouts.xml file in place of the existing one. Open the System Information Editor by double clicking on the system overview root tree node. Make some change to something in the editor and change it back so the document requires saving. Save the editor and close it. Check the system back into CMS.

4.3.4 Custom Network Switch Layout Configuration

The Network Switch Layouts in ToolboxST provide the mapping between the internal switch interfaces and the physical switch ports, which enables the Network Monitor feature to read the switch data over SNMP and display the data with the correct physical port location.

ToolboxST provides GE standard switch layouts that correspond to all supported NetworkST standard switch types. Support for non-standard switch types can be configured by creating custom Network Switch Layouts, which are used to enable the Network Monitor to monitor non-standard switch types.

**Note** The use of a non-standard switch implies that the user assumes responsibility for all aspects of the switch configuration and its interaction with and impact on the network. Switch configuration is beyond the scope of this document. SNMP V1 or SNMP V3 must be enabled and properly configured in the switch to enable monitoring of the switch values.

Network Switch Layouts allow users to enter unique physical port-to-port faceplate and interface name mapping. The Network Switch Layouts include a set of legacy switch layout types that were supported before the ability to add custom switch layouts existed. These legacy switch layout types cannot be edited, but are presented for completeness and to allow easy version upgrade. There is also a set of GE standard switch layout definitions that cannot be modified but are included as validated switch layouts.
➢ To add a custom Network Switch Layout

1. From the **System Information Editor**, expand the Network Switch Layouts.

2. From the **Tree View** of layouts, right click a port, select **Add Switch Layout**, and enter a unique name for the layout. (As an alternative, you may copy an existing one.)

3. From the **Property Editor**, modify the properties to configure the switch layout.
### Network Switch Layout Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Is a legacy layout</td>
<td>Legacy layouts; cannot be modified (False)</td>
</tr>
<tr>
<td>Is Stackable</td>
<td>Switch is a stackable switch (default is True)</td>
</tr>
<tr>
<td>Maximum Stack Size</td>
<td>Maximum number of stacked switches allowed. This setting limits the Stacked Switch Group Size setting in the Network Switch component editor.</td>
</tr>
<tr>
<td>Number of ports on each switch</td>
<td>Sets the number of ports on each switch. For a stacked switch this number controls how many ports are defined as the Stacked Switch Group Size is set. For a non-stacked switch this controls the total number of ports. For the switch layout, all ports are shown per the Maximum Stack Size and Ports Per Switch setting.</td>
</tr>
<tr>
<td>Standard Layout</td>
<td>Standard GE switch configurations are part of the product. This switch layout is a standard configuration; cannot be modified (False).</td>
</tr>
<tr>
<td>Switch Layout Type</td>
<td>Name of the type of switch. There are some pre-defined legacy switch types that were used by previous ToolboxST / WorkstationST versions, which are included but cannot be modified.</td>
</tr>
<tr>
<td>Switch Manufacturer</td>
<td>Manufacturer of the network switch. There are some manufacturers that require special SNMP behavior by the WorkstationST Network Monitor.</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td></td>
</tr>
<tr>
<td>Supports Dual Power Supplies</td>
<td>True if the switch type provides standard redundant power supply connections that can be optionally connected to a power source for Simplex or redundant power supply operation.</td>
</tr>
<tr>
<td>Supports Fan Monitoring</td>
<td>True if the switch type has internal fans and provides the ability to monitor them via SNMP.</td>
</tr>
<tr>
<td>Supports Power Supply Monitoring</td>
<td>True if the switch type provides the ability to monitor the switch power supplies via SNMP.</td>
</tr>
<tr>
<td>Supports Temperature Monitoring</td>
<td>True if the switch type has internal temperature sensors and provides the ability to monitor them via SNMP.</td>
</tr>
</tbody>
</table>

In the Data Grid View, each non-legacy switch allows modification to port information.

<table>
<thead>
<tr>
<th>Port Location</th>
<th>Faceplate Port Number</th>
<th>Faceplate Port Name</th>
<th>Port Number</th>
<th>Faceplate Port Port Text</th>
<th>Interface Name</th>
<th>Stack Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 001 X</td>
<td>1</td>
<td>Port</td>
<td>1</td>
<td>X</td>
<td>FastEthernet1/1</td>
<td>1</td>
</tr>
<tr>
<td>Port 002 X</td>
<td>2</td>
<td>Port</td>
<td>2</td>
<td>X</td>
<td>FastEthernet1/2</td>
<td>1</td>
</tr>
<tr>
<td>Port 003 X</td>
<td>3</td>
<td>Port</td>
<td>3</td>
<td>X</td>
<td>FastEthernet1/3</td>
<td>1</td>
</tr>
<tr>
<td>Port 004 X</td>
<td>4</td>
<td>Port</td>
<td>4</td>
<td>X</td>
<td>FastEthernet1/4</td>
<td>1</td>
</tr>
<tr>
<td>Port 005 X</td>
<td>5</td>
<td>Port</td>
<td>5</td>
<td>X</td>
<td>FastEthernet1/5</td>
<td>1</td>
</tr>
<tr>
<td>Port 006 X</td>
<td>6</td>
<td>Port</td>
<td>6</td>
<td>X</td>
<td>FastEthernet1/6</td>
<td>1</td>
</tr>
<tr>
<td>Port 007 X</td>
<td>7</td>
<td>Port</td>
<td>7</td>
<td>X</td>
<td>FastEthernet1/7</td>
<td>1</td>
</tr>
<tr>
<td>Port 008 X</td>
<td>8</td>
<td>Port</td>
<td>8</td>
<td>X</td>
<td>FastEthernet1/8</td>
<td>1</td>
</tr>
<tr>
<td>Port 001</td>
<td>1</td>
<td>Port</td>
<td>9</td>
<td></td>
<td>GigabitEthernet1/1</td>
<td>1</td>
</tr>
<tr>
<td>Port 002</td>
<td>2</td>
<td>Port</td>
<td>10</td>
<td></td>
<td>GigabitEthernet1/2</td>
<td>1</td>
</tr>
</tbody>
</table>
## Switch Layout Data Grid Column Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Location</td>
<td>Read only indication of the stack and face plate port number</td>
</tr>
<tr>
<td>Faceplate Port Number</td>
<td>Port number on the switch nameplate. This number is the same on all individual switch ports for a stacked switch, but the Stack Number will be different.</td>
</tr>
<tr>
<td>Faceplate Port Name</td>
<td>Faceplate port name. This is used in the port location which is displayed in the network status viewer.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number returned from SNMP queries and shown using the switch command line interface</td>
</tr>
<tr>
<td>Faceplate Port Text</td>
<td>Text is appended after the port number into the Port Location field</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Interface name that can be viewed through the switch command line interface (for example, FastEthernet1/4)</td>
</tr>
<tr>
<td>Stack Number</td>
<td>Stack number for a stackable switch (1 for a switch that does not support stacking)</td>
</tr>
</tbody>
</table>
4.4 **Switch Stacking and Hardware Monitoring**

Beginning with ControlST V07.07.00C, Network Monitor monitors the health of the stack members for stacked switch configurations, as well as the hardware status for stand-alone switches and individual switch stack members.

4.4.1 **Switch Stack Monitoring**

Switch stacking is used to make multiple switches behave as a single switch. Switch types that support stacking can normally be configured for either stand-alone or stacked mode. Network Monitor monitors the stack health of any switch of a type that supports stacking and is configured for stacking mode.

**Stack Provisioning Health Monitoring**

Stack provisioning reflects the number of switches a stack is configured to support. Network Monitor monitors the configured stack size and the switch stack provisioned capacity in order to provide an indication if the switch configuration in ToolboxST exceeds the capacity of the actual switch stack. Network Monitor requests the stack configuration from the switch and compares the number of provisioned switches with the stack size configured for the switch in ToolboxST. Network Monitor reports errors if the stack size configured in ToolboxST exceeds the provisioned capabilities of the switch. Provisioning errors are addressed by either modifying the switch configuration in ToolboxST to a stack size supported by the switch stack, or by increasing the provisioned size of the switch stack.

Network Monitor also monitors the status of each stack member and reports errors if a stack member is not actively participating in the stack.

In the example displayed in the following figure, the switch is configured as a stack with two stack members, each with 12 ports per switch.

![Example Switch Stack ToolboxST Configuration](image)
The switch stack provision status is also displayed as part of the tooltip information for the switch in the Network Status Viewer.

![Example Switch Stack Provision Status in Network Status Viewer](image1)

In the example displayed in the following figure, the stack size configured in ToolboxST exceeds the provisioning of the switch.

![Example Switch Stack Exceeds Switch Provisioning ToolboxST Configuration](image2)
The switch stack provision error is also displayed as part of the switch status text and as part of the tooltip information for the switch in the Network Status Viewer.

Example Switch Stack Provision Error in Network Status Viewer

Network Monitor also generates provisioning alarms that can be viewed in the WorkstationST Alarm Viewer, as shown in the following figure.

Example Provision Alarm in WorkstationST Alarm Viewer
Stack Member Health Monitoring

Network Monitor monitors the status of each stack member and reports errors if a stack member is not actively participating in the stack.

In the example displayed in the following figure, the switch is configured with a stack size of four.

![Example Switch Stack Member ToolboxST Configuration](image)

The actual switch is provisioned for four stack members, but in this example there are only two physical switches currently in the stack, and the switch reports these missing switches with a Provisioned/Not Ready status. Any status other than Ready indicates that the switch is not participating in the stack. The Network Monitor Status Viewer reports the error condition and shows status of each stack member.

The switch stack member status is displayed as part of the tooltip information for the switch in the Network Status Viewer.

![Switch Stack Member Status in Network Status Viewer](image)
Network Monitor also generates Stack Member alarms that can be viewed in the WorkstationST Alarm Viewer, as shown in the following figure.

Example Switch Stack Member Status Alarms in WorkstationST Alarm Viewer
4.4.2 Hardware Monitoring: Power Supplies

Network Monitor can be configured to monitor the status of the switch power supplies. The Monitor Power Supplies property is available in the switch configuration for switch types that support this capability. In the following figure, power supply monitoring has been enabled (Monitor Power Supplies property is set to True).

![Power Supply Monitoring ToolboxST Configuration](image1)

The status of the switch power supplies is displayed as part of the tooltip information for the switch in the Network Status Viewer.

![Example Switch Internal Power Supply Status in Network Status Viewer](image2)
Unplugging the AC power cord from one of the power supplies generates a power supply error that is reported in the tooltip information in the Network Status View as shown in the following figure, and an alarm is generated.

Network Monitor also generates power supply alarms that can be viewed in the WorkstationST Alarm Viewer, as shown in the following figure.

**Note** Network Monitor automatically monitors all power supplies in the switch. Some switch chassis have slots that accept power supply modules and therefore allow the capability for single or redundant power supplies. Any power supply modules that are installed but do not have AC power connected to them will be reported as a failed power supply because it is assumed that there is no good reason to add the expense of a redundant power supply module but not provide power to it. If power redundancy is not desired, unplug the redundant power supply modules from the switch to avoid redundant power supply errors.
Dual Power Supply Example

Some switch types (primarily the Cisco IE2000 switches) come with internal dual power supplies, and power can optionally be connected to either one of them for non-redundant power or to both of them for redundant power.

![Cisco IE2000 Switch Dual Power Supplies](image)

The switch device configuration in ToolboxST provides the properties to support any combination of power connections to the switch, as displayed in the following figure.

Configure the Monitoring properties, Power Supply 1 Connected and Power Supply 2 Connected, to report errors or alarms only for the connected (used) power supplies as follows:

- **To configure dual power supplies to report errors or alarms for connected power supplies only**
  - If only DC-A is connected to a power source, set **Power Supply 1 Connected** to True and set **Power Supply 2 Connected** to False.
  - If only DC-B is connected to a power source, set **Power Supply 1 Connected** to False and set **Power Supply 2 Connected** to True.
  - If both DC-A and DC-B power connections are connected to a power source, set both **Power Supply 1 Connected** and **Power Supply 2 Connected** to True.
4.4.3 Hardware Monitoring: Fans

Network Monitor can be configured to monitor the status of the internal switch fans. The Monitor Fans property is available in the switch configuration for switch types that support this capability. In the example displayed in the following figure, Fan Monitoring has been enabled (Monitor Fans property is set to True).

![Switch Internal Fan Monitoring ToolboxST Configuration](image1)

Network Monitor automatically monitors the status of all of the internal switch fans. In the example displayed in the following figure, the selected stack member has two internal fans and they are both operating without any errors. The switch fan status is displayed in the switch tooltip information in the Network Status Viewer.

![Example Switch Fan Status in Network Status Viewer](image2)
Internal fan failures are reported as an error and an alarm will be generated. The switch fan error is displayed in the switch tooltip information in the Network Status Viewer.

Example Switch Fan Status in Network Status Viewer

Network Monitor also generates switch fan alarms that can be viewed in the WorkstationST Alarm Viewer, as shown in the following figure.

Example Switch Fan Alarms in WorkstationST Alarm Viewer
4.4.4 **Hardware Monitoring: Temperature Sensors**

Network Monitor can be configured to monitor the status of the internal switch temperature sensors. The Monitor Temperature property is available in the switch configuration for switch types that support this capability. In the example displayed in the following figure, temperature sensor monitoring has been enabled (Monitor Temperature property is set to True).

![Switch Internal Temperature Monitoring ToolboxST Configuration](image)

Network Monitor automatically monitors the status of all of the internal switch temperature sensors. In the example displayed in the following figure, all temperature sensors in the selected switch are reporting temperatures in the normal range. The switch temperature sensor status is displayed in the switch tooltip information in the Network Status Viewer.
Switches with Temperature Sensor readings that exceed normal values will indicate an error in the tooltip information in the Network Status Viewer, and an alarm will be generated.
4.5 Configure Local HMI Management Address

As the system overview shows, the workstations do not have direct access to the management network, and communications with the network switches can only occur through network routing between the PDH network and the management network (MGH). The network router is typically configured to allow only PDH traffic from a single IP address. The Network Monitor feature must be configured to send all requests to the network switches over the PDH network using this established PDH address as the source address of the request. The Local HMI Management Address property of the Network Monitor feature is used to specify this predefined management network routable PDH address. Typically this address will be configured as 172.16.201.60.

➢ To configure the Network Monitor feature: From the Tree View, double-click the WorkstationST item to display the Component Editor.

![Network Monitor Configuration]

From the Network Monitor tab, select Local HMI Management Address and enter the appropriate IP address.
4.6 Add Local HMI Management Address to PDH Adapter in Workstation

The Local HMI Management Address must be added to the PDH (plant scope) network adapter of the computer running the Network Monitor.
5 Configure Local HMI Management Address for Systems without Switch Management Network

To increase the security of the network infrastructure, the network switches are being configured with restricted access to the switch SNMP data. The Network Monitor feature must be configured correctly to gain access to the switch SNMP data. Without this SNMP data, the switch information such as port status and connected devices will be unknown. This causes the Network Monitor to generate Topology Error alarms for all of the devices in the system, and preventing the Network Monitor from detecting network issues.

5.1 Configure Local HMI Management Address

Updated switch configurations include an Access Control List (ACL) that blocks all SNMP data requests except for those from a single, predefined IP address, which is referred to as the Local HMI Management Address. In order to get SNMP data from the network switches, the Network Monitor must send all SNMP requests with the Local HMI Management Address as the source address in the TCP/IP message header. The Local HMI Management Address property of the Network Monitor feature is used to specify this address, which is typically configured as 172.16.201.60 in the network switches.

➢ To configure the Local HMI Management Address: From the Tree View, double-click the WorkstationST item to display the Component Editor.
5.2 Add Local HMI Management Address to PDH Adapter in Workstation

The Local HMI Management Address must be added to the PDH (plant scope) network adapter of the PC running the Network Monitor feature.
6 Network Switch SNMP Configuration

Network Monitor uses Simple Network Management Protocol (SNMP) to read data from the network switches to determine the state of the switch ports, which devices are connected to them, and so forth. In previous releases, Network Monitor and the network switches only implemented the SNMP V1 protocol. As a security enhancement, ControlST and the network switches have been expanded to use the SNMP V3 protocol, which introduces strong authentication and data encryption to securely read data from the network switches. ControlST V07.02.00C SP01 and earlier versions use the SNMP V1 protocol to read SNMP data from the network switches. ControlST V07.02.00C SP02 and later versions can use either the SNMP V1 or SNMP V3 protocol to read data from the network switches.

<table>
<thead>
<tr>
<th>Application</th>
<th>SNMP V1 Protocol</th>
<th>SNMP V3 Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlST</td>
<td>ControlST V07.02.00C SP01 and earlier</td>
<td>ControlST V07.02.00C SP02 and later</td>
</tr>
<tr>
<td>NetworkST</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

6.1 New System Configuration

The SNMP Mode and security information is configured and displayed from the WorkstationST Network Monitor configuration tab, located under the Network Monitor Data Acquisition property group.

The following figure displays the properties that are listed when SNMP Mode V1 is selected.

The following figure displays the properties that are listed when SNMP Mode V3 is selected.
6.1.1 SNMP V1 Configuration

➢➢➢ To configure SNMP V1 Mode

1. Open the appropriate .tcw system file and double-click the WorkstationST device to open the WorkstationST Component Editor.

2. Select the Network Monitor tab to display the SNMP Mode and security information located under the Network Monitor Data Acquisition property group.

3. From the SNMP Mode drop-down menu, select V1.

4. Click the SNMP V1 Community property Edit button to display the Change Password dialog box.

5. Enter the SNMP V1 Community name in the New Password field, re-enter it in the Verify Password field, and click OK to save it.

6. Perform a Build, Download to the WorkstationST device to save the configuration, and restart the Network Monitor feature to display the new configuration values.

Tip You can verify the configured SNMP Mode and the SNMP V1 Community Name used by the Network Monitor feature from the Network Status Viewer. With your cursor, hover over each network switch to display the SNMP Mode and security information in the tool tip. The Community Name is hidden for security.
Configured SNMP V1 Mode and Community Name Displayed in Network Status Viewer

Note Refer to the chapter *Troubleshoot Network Switch SNMP Issues* for assistance with resolving SNMP configuration issues.
6.1.2 SNMP V3 Configuration

➢➢

To configure SNMP V3 Mode

1. Open the appropriate .tcw system file and double-click the WorkstationST device to open the WorkstationST Component Editor.

2. Select the Network Monitor tab to display the SNMP Mode and security information located under the Network Monitor Data Acquisition property group.

3. From the SNMP Mode drop-down menu, select V3.

4. Click the SNMP V3 Authentication Password property Edit button to display the Change Password dialog box.

5. Enter the SNMP V3 Authentication password in the New Password field, re-enter it in the Verify Password field, and click OK to save it.

6. Click the SNMP V3 Encryption Password property Edit button to display the Change Password dialog box.
7. Enter the SNMP V3 Encryption password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

8. Enter the SNMP V3 user name for the **SNMP V3 User Name** property.

9. Perform a **Build, Download** to the WorkstationST device to save the configuration, and restart the Network Monitor feature to display the new configuration values.

---

**Tip** You can verify the configured SNMP Mode and security settings used by the Network Monitor feature from the Network Status Viewer. With your cursor, hover over each network switch to display the SNMP Mode and security settings in the tool tip. The Authentication and Encryption Password values are hidden for security.
Configured SNMP V3 Mode and Security Settings Displayed in Network Status Viewer

Note Refer to the chapter Troubleshoot Network Switch SNMP Issues for assistance with resolving SNMP configuration issues.

6.1.3 Network Switch SNMP Override Settings

The SNMP configuration settings are typically configured the same for all of the network switches at the site. When this is the case, the SNMP settings on the configuration tab specify the SNMP settings for all of the network switches in the system. Situations may arise where different SNMP configurations are needed between network switches. For example, a site may replace an failed switch that only supports SNMP V1 (ControlST V07.02.00C SP01 and earlier versions) with a new switch with SNMP V3 support (ControlST V07.02.00C SP02 and later). In this case, the site may choose to enable SNMP V3 protocol to collect data from the new switch while leaving the existing switches at SNMP V1 protocol. ToolboxST provides network switch device override settings to override the Network Monitor feature-level settings.

➢➢ To enable the local SNMP Parameter Override property

1. Open the appropriate .tcw system file and double-click the Network Switch device to open the Network Switch Component Editor.

The SNMP Parameter Override settings are located under the SNMP Overrides property group.
2. From the **SNMP Local Parameter Override** drop-down menu, select **True**. When set to True, the locally configured SNMP settings are used instead of the SNMP settings configured at the Network Monitor feature level.

3. From the **SNMP Mode** drop-down menu, select the appropriate value as V1 or V3.
   a. If SNMP Mode **V1** is selected, perform the following steps:
      i. Click the **SNMP V1 Community Name** property **Edit** button to display the *Change Password* dialog box.
ii. Enter the SNMP V1 Community name in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

![Change Password dialog box]

b. If SNMP Mode **V3** is selected, perform the following steps:

i. Enter the SNMP V3 user name for the **SNMP V3 User Name** property.

![SNMP Overrides]

ii. Click the **SNMP V3 Authentication Password** property **Edit** button to display the **Change Password** dialog box.

![SNMP Overrides with password]

iii. Enter the SNMP V3 Authentication password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

![Change Password dialog box with password]
iv. Click the **SNMP V3 Encryption Password** property **Edit** button to display the **Change Password** dialog box.

![Change Password Dialog Box](image)

v. Enter the SNMP V3 Encryption password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

![Change Password Dialog Box](image)

4. Perform a **Build** to build the switch device, save the configuration, and automatically restart the Network Monitor feature to display the new configuration values.

---

**Tip** You can verify the configured SNMP Mode and security settings used by the Network Monitor feature from the Network Status Viewer. With your cursor, hover over each network switch to display the SNMP Mode and security settings in the tool tip. The SNMP V1 Community Name and the SNMP V3 Authentication and Encryption Password values are hidden for security.

![Network Status Viewer](image)

**Configured SNMP V3 Mode and Security Settings Displayed in Network Status Viewer**
➢ To disable the local SNMP Parameter Override property

1. Open the appropriate .tcw system file and double-click the Network Switch device to open the **Network Switch Component Editor**.

2. From the **SNMP Local Parameter Override** drop-down menu, select **False**.

3. Perform a **Build** to build the switch device, save the configuration, and automatically restart the Network Monitor feature to display the new configuration values.
6.2 ControlST Upgrade

ControlST V07.02.00C SP01 and earlier versions only support the SNMP V1 protocol to read data from the network switches. The only required SNMP setting was the SNMP Community name, which was configured at the switch level as shown in the following figure.

![SNMP Community Property Setting Prior to Upgrade](image1)

When upgrading from ControlST V07.02.00C SP01 or earlier versions to a newer version that supports SNMP V3 settings (ControlST V07.02.00C SP02 and later), the network switch device in ToolboxST automatically captures the SNMP V1 switch configuration settings and updates them with the new settings: the SNMP Local Parameter Override property is set to True, the SNMP Mode is set to V1, and the SNMP Community is copied to the SNMP V1 Community Name property of the switch device. The changes are saved and permanently stored when the switch device is built after upgrade. This allows the SNMP V1 settings to continue to be managed at the switch level after a ControlST upgrade without the user having to make any changes to the network switch configuration. The following figure displays the switch SNMP settings after a ControlST upgrade has been performed.

![SNMP Community Property Setting After Upgrade](image2)
6.3 Network Switch Replacement (Upgrade)

The default network switch configuration from the factory supports both SNMP V1 and SNMP V3 protocols. The following options are available when replacing a network switch that only supports the SNMP V1 protocol with a network switch that supports the SNMP V3 protocol:

- Continue using SNMP V1: configure the replacement network switch in the same way as the replaced switch. This is the only option in a system using ControlST V07.02.00C SP01 or earlier versions that only support the SNMP V1 protocol. The default switch configuration supports both SNMP V1 and SNMP V3 protocols. Modify the ToolboxST network switch device’s Management IP Address to match the IP address of the replacement switch, and configure the switch’s SNMP Community to match the replaced switch’s Community Name. Build the switch device to update the configuration and restart the Network Monitor feature with the new values.

- Configure the ToolboxST network switch device for SNMP V3: update the ToolboxST switch device configuration to benefit from the SNMP V3 capability of the replacement switch. This option is only available if the system in which the switch is being implemented has ControlST V07.02.00C SP02 or later with SNMP V3 support. Set the ToolboxST switch device SNMP Local Parameter Override to True, set the SNMP Mode to V3, and set the SNMP V3 User Name, SNMP V3 Authentication and Encryption passwords to match the network switch configuration. Build the switch device to update the configuration and restart the Network Monitor feature with the new values.

---

**Note** After the upgrade is complete, promote management of the switch SNMP parameters to the Network Monitor feature level by configuring the feature-level SNMP settings and clearing the SNMP Local Parameter Override setting, then perform a build of each network switch.
7 Troubleshoot Network Switch SNMP Issues

The most common issue associated with the Network Monitor is the inability to get SNMP data from one or more network switches. This results in topology errors due to the Network Monitor’s inability to determine which ports the devices are connected to, as well as a lack of port level data. Failure to read SNMP data from a network switch is typically the result of SNMP settings in ToolboxST that do not match the network switch SNMP configuration. For the SNMP V1 protocol, this results from an incorrect SNMP V1 Community setting. For the SNMP V3 protocol, this may be the result of an incorrect setting for the SNMP V3 User Name, and/or invalid SNMP V3 Authentication and Encryption passwords. Telnet into the switch to determine the SNMP settings and verify that the SNMP settings in ToolboxST are correct.

**Note** SNMP is a simple network management protocol for managing devices on internet protocol networks.

The recommended way to determine if Network Monitor is receiving SNMP data from the switch is to hover over the switch in the Network Status Viewer to display the system information (System Info), which provides the SNMP value read from the switch. If System Info is blank, Network Monitor is not able to read SNMP data from the switch.

Another method to determine if the Network Monitor is receiving SNMP data from the switch is to expand one or more ports to see if the data has been updated. If the values are all zero and port description (first field) is blank, SNMP data has not been read for that port. This would normally coincide with failure to read SNMP data for the entire switch.
The following figure shows the expected Network Status Viewer display, including a legitimate topology error:
**Note** Some Allied Telesis switch models do not accept special characters such as the @ symbol, so these switches cannot use the standard GeS@lem9ro SNMP community name. This is a common configuration error where all of the switches are configured with the default community name, while certain switches are using a different community name.