



Designing a Reliable Industrial Ethernet Network

Facts

- Most factories average 5-20% downtime yearly.
- Experts estimate that manufacturers undervalue the true cost of factory downtime by up to 300%.
- N-TRON® helps companies combat downtime. The company is recognized around the world for developing and manufacturing highly reliable, quality ruggedized products for Industrial Ethernet automation. Our network solutions are the benchmark for quality and reliability, providing exceptional performance for mission-critical data acquisition and control applications.
- N-TRON offers a complete line of affordable unmanaged and managed Ethernet switches, media converters, Power over Ethernet (PoE), and wireless access devices for rugged industrial environments .

Most of the major manufacturing automation end users and suppliers are using or considering Ethernet as an industrial control option for field devices, drives, power management equipment, and special purpose controllers. Engineers and others who design Ethernet networks for these applications must follow correct installation procedures and must select network equipment that will function in plant environments with little or no downtime.

Power supply configuration, proper network grounding, selection of network topology, and configuration of network switches are critical when Ethernet is used in industrial applications. Design techniques such as port-by-port addressing can significantly reduce the time required to replace field devices by eliminating the need for maintenance personnel to manually input IP addresses.

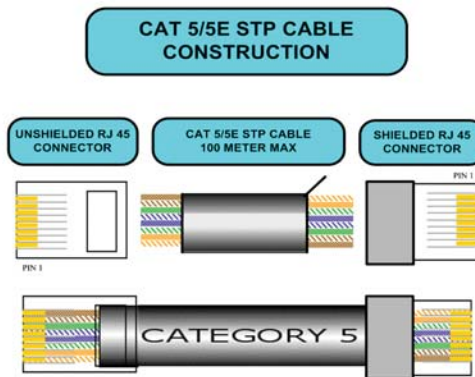
This white paper explores these issues and shows how to design a reliable industrial Ethernet network for manufacturing applications.



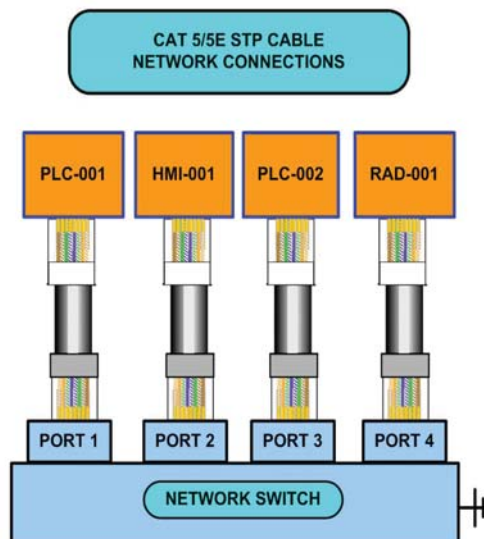
Media Selection

The selection and proper installation of network media insures that the network will function at expected data rates and will not be vulnerable to electrostatic, induction and radio frequency interference. Proper selection and installation also helps avoid the loss of network devices due to the introduction of a high voltage pulse event such as a lightning strike. Downtime through equipment malfunction can be minimized by utilizing proper grounding techniques.

Copper cable installations should use four twisted pair CAT5, CAT5e, or CAT6 for 10/100/1000 Mbs Ethernet Networks. The use of copper twisted pair cable should be limited to indoor use in low noise areas, and the maximum cable run should be 100 meters. In most industrial installations or in known high noise areas such as AC drive, welding, and robotics applications - shielded CAT 5e cable should be employed.



Shielded twisted pair cables should be installed with the shield connected to the network switch and not connected to the field device. The network switch should be connected to a good earth ground. By following this termination protocol, the network will be protected from electrical noise through the grounded shield and ground potential differences will not cause a ground loop current in the shield.



White Paper Series

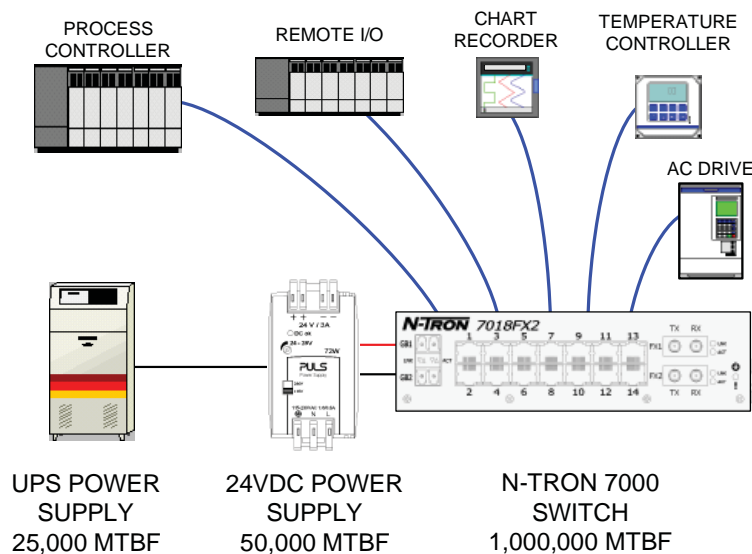
Twisted Pair cables should be deployed in separate IT wiring trays and should not be run parallel to high voltage lines. These cables can be degraded by excess pulling force that tends to untwist the twisted pairs, and also by the use of tie wraps applied too often or too tightly. Cable performance should be tested after installation.

Fiber optic media should be used in installations requiring runs over 100 meters, areas of high electrical noise, and any time electric isolation is required. Multimode fiber optic cable can be used in cable runs up to 2km at 10/100Mbps; at 1000Mbps the maximum cable length will be between 330 meters and 500 meters depending on the cable specification (50/125 micron cable = 500 meters, 65/125 micron cable= 330 meters). Single mode fiber optic cable can be used for Ethernet networks with communication rates of 10/100/1000Mbps which require cable runs up to 80km.

Optical isolation using fiber optic cable should be used in larger networks. This will prevent voltage pulses generated by lightning and other electrical disturbances from damaging the entire network by providing optical breaks in the copper network topology. Fiber optic installation should be performed by trained installation personnel to avoid costly mistakes and to insure performance and long term reliability.

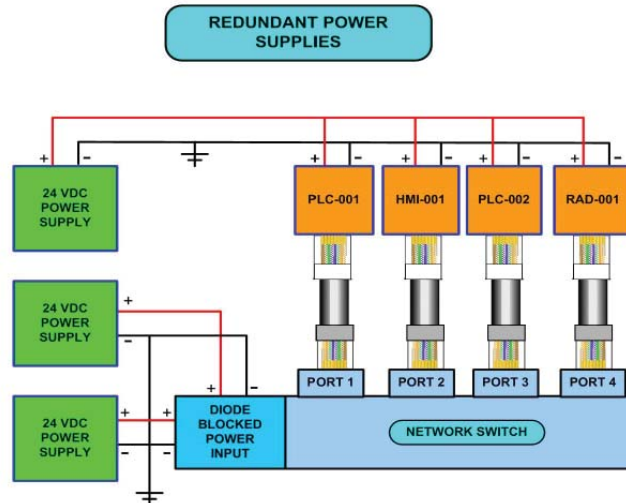
Power Supply Configuration

Industrial network switches are normally powered through diode blocked redundant power inputs by two redundant power supplies. This is necessary because most power supplies have very low mean time between failure (MTBF) performance when compared to the MTBF of an industrial Ethernet switch.



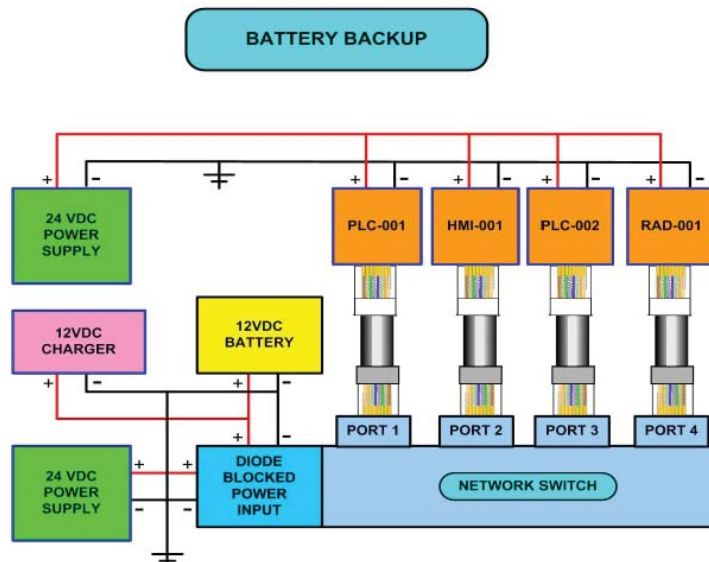
White Paper Series

There are generally two scenarios when configuring switch power. When the network is not required during a utility power outage, two 24VDC power supplies are used in a redundant configuration.



In some applications the network must operate during utility outages. These applications require a battery backup configuration using one 24VDC power supply and one 12VDC battery with battery charger connected. The power supply will provide current through the blocking diodes during normal operation. The battery will supply current to the switch whenever the voltage from the power supply drops below 12VDC.

Most industrial Ethernet switches accept input power in a range from 10-30VDC, and automatically use the higher power input. So in this scenario, the switch will normally use the primary 24VDC power input and automatically switch to the secondary lower voltage 12VDC input in the event of 24VDC power interruption.



Network Switch Selection

If an industrial Ethernet switch malfunctions in any way, then the control system is compromised. For this reason the network switch should have the highest MTBF possible. The MTBF of the network switch should be higher than that of the connected field devices and should have environmental specifications that exceed those of the field devices connected to it.

MTBF ratings are often a key difference between commercial switches and industrial switches. Relatively low MTBF components such as cooling fans are commonly used in commercial switches, but should be avoided in industrial applications.

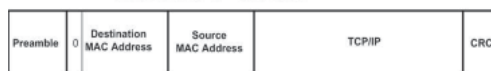
Specifications	Typical Commercial Switch with Fan Cooling	Typical Industrial Switch and Field Devices	Critical Control Switch
MTBF Hours	25K	200K	1-2M
Vibration	0G to 1G	5G	30G
ESD Protection	2KV	4KV to 6KV	16KV
RF Rejection	3 Volts/Meter	3 Volts/Meter	10Volts/Meter
Operation Temp	0° to 45°	-20° to 60°	-40° to 80°

The choice of an Ethernet switch requires knowledge of the switch software functions required for the plant control schemes. There are two types of switches generally available, unmanaged and managed switches.

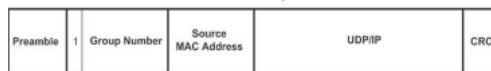
Unmanaged switches provide basic network switching functionality by learning the Media Access Control (MAC) address of each device connected to each port of the switch. This is accomplished by reading the Source Address of the Ethernet packets being received from each device connected to the switch.

A database of each port on the network is created and used by the network switch to direct Unicast Ethernet packets to the correct port based on the MAC address found in their destination MAC address area. Multicasts and broadcasts are sent to all the ports of an unmanaged switch.

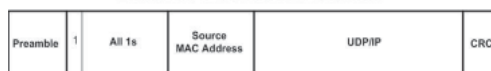
Ethernet / IP Unicast



Ethernet / IP Group Multicast

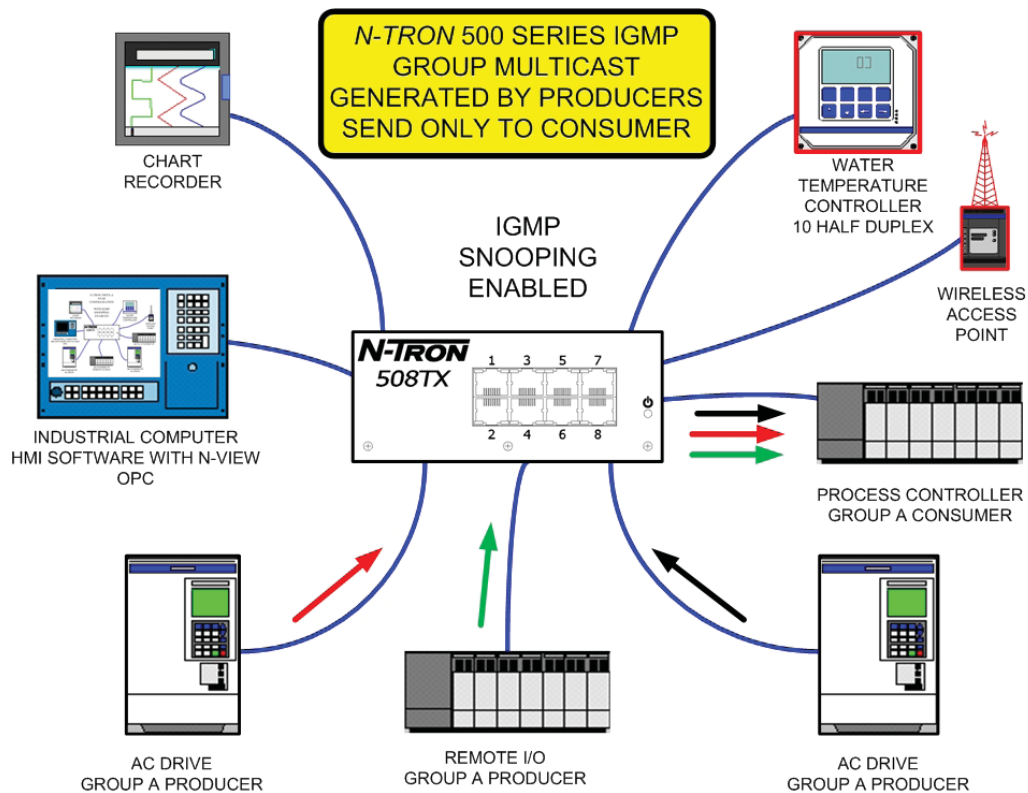


Ethernet Broadcast Multicast



Managed switches are available with a variety of software protocols used to add functionality to the basic switch capability. The list of protocols or functions on a managed switch is not defined and varies widely from one manufacturer to another. A full discussion of the many functions available on managed switches is beyond the scope of this white paper, but the list below includes some of the management features required in many critical control applications:

1. **Internet Group Management Protocol (IGMP Snooping).** This protocol is used to control the routing of Ethernet multicast packets to the ports on the switch with connected devices that have requested this information. Without IGMP Snooping the switch will send multicasts out all ports. This can cause certain devices like radios, RS232/485 to Ethernet Converters, certain routers, certain firewalls, and any older half duplex devices to have communication failures.



If the switches used do not have IGMP Auto Configuration capability, the following procedure must be followed:

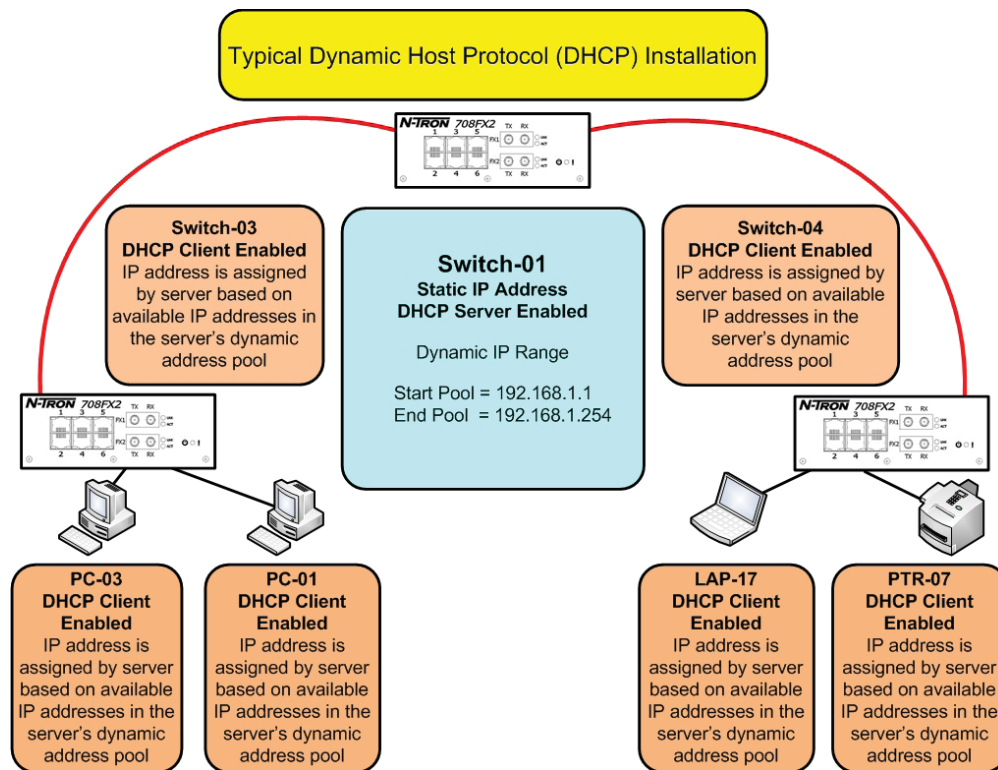
- a. IGMP Snooping must be enabled
- b. Router ports must be identified and configured
- c. Routers and wireless routers connected to the switch must have port filtering setup to pass IGMP control data but block all other multicast traffic not required by these devices.

- d. One IGMP Query Switch should be configured to poll the field devices connected to the network periodically. This query will cause all connected devices to send an IGMP Multicast Group Join message to the network switch or switches. The IGMP Join message will be used by the switches to update their network address database in order to insure that only the devices requiring the Multicast packets receive them.
2. **Quality of Service (QoS).** This protocol is used to read the priority code included in Ethernet packets used by some IP phones, IP cameras and by many control devices to prioritize traffic through the network switch. There are two types of QoS:
 - a. Tagged QoS will prioritize packets generated by field devices that can create and add QoS priority codes to their packets. QoS must be enabled during setup of the switch.
 - b. Port QoS will add a priority to incoming packets on a specific port. The priority level is programmed into the network switch on a port-by-port basis during setup of the switch.
3. **Virtual Local Area Network (VLAN).** VLAN allows the switch to be split into many virtual network switches or local area networks. Each Ethernet packet has a VLAN ID number—the default is VLAN ID 1—and devices on one VLAN are only able to communicate with devices on the same virtual LAN. There are two ways to implement VLAN:
 - a. Tagged VLAN will receive Ethernet packets, check the VLAN ID, and only allow communication between devices with the same VLAN id number.
 - b. Port VLAN will receive Ethernet packets and load a VLAN ID configured into the switch at setup for each port.

**N-TRON 508FX2
Industrial Ethernet Switch**



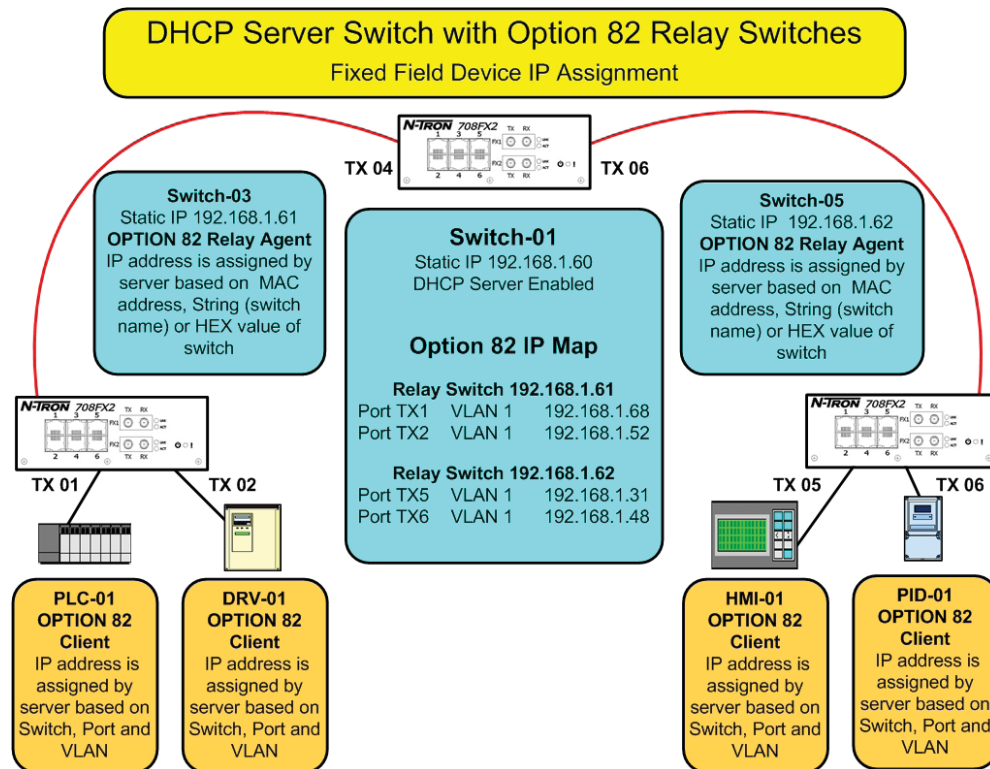
4. **Dynamic Host Configuration Protocol (DHCP).** DHCP provides a way to automate and manage the assignment of Internet Protocol (IP) addresses to field devices in a network. Critical control networks use both MAC and IP addressing. The MAC address of each device on the network is a unique address assigned by the manufacturer of the device. The IP address is assigned by the user and each device must have a unique IP address to prevent address conflicts.



Many devices in a critical control network must use an address that is registered with its associated controller. The controller is sending and receiving data to and from field devices and has been given the IP location (address) of each device it is controlling as part of its software setup. The IP relationship between a controller and an I/O rack connected in the network must remain constant. If an I/O rack is replaced the new rack must be assigned the same IP address as the one it is replacing or the controller will not be able to communicate with it.

All DHCP Client devices connected to a network will receive a unique IP address from the network's DHCP Server. The IP address will be within a range of addresses assigned to the DHCP Server. This will work well for most IT networks but will cause problems with most process control networks because basic DHCP will not maintain the IP address for a device on a specific port when the device is replaced.

This problem can be solved through the use of DHCP Option 82 Relay. With DHCP Option 82 Relay the server will be assigned a list of switch ports, which require specific IP Addresses. If an I/O Rack is replaced on a specified Option 82 Relay Switch port the replacement I/O Rack will receive the same IP address previously programmed in the DHCP Server for that port.



In this manner control devices can be replaced by maintenance personnel without the need to program an IP address in the unit. As long as the replacement unit is connected to the correct switch port it will receive the proper IP Address. This function can simplify field maintenance and reduce the recovery time caused by a failed field device.

Some unmanaged switches and most managed switches allow network monitoring through the switch using one or more of the following methods:

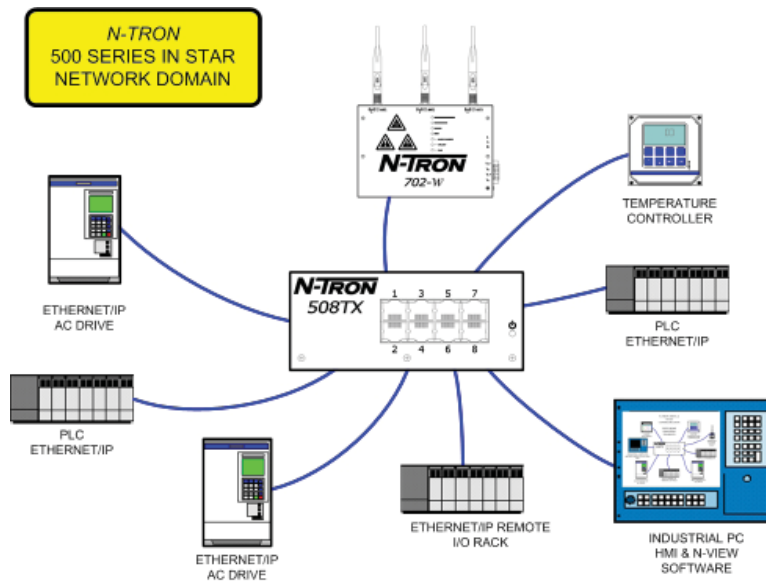
1. **OPC.** OPC is a Microsoft-based standard widely understood and utilized in the process control industry. It is used to import data points from switches and other field devices used in process control applications, and to provide this information to Human Machine Interface (HMI) software packages. This allows the user to view data points produced by the network switches on an HMI, alarm those points and historically trend data. OPC capability allows the HMI to display both process operations and network operations simultaneously.
2. **Simple Network Management Protocol (SNMP).** SNMP is used to monitor and control switches using one of many commercially available network management tools. These tools can be relatively complex to use and are normally used by IT personnel to manage large enterprise level networks.
3. **WEB Browser Management Tools.** Many fully managed switches employ web page monitoring and control. This is used in most cases for setup and field monitoring of network switches.

Proper network monitoring and alarming can often indicate problems with the network and provide information that will prevent future downtime. In the case of a device failure, monitoring protocols can indicate where network faults are located to facilitate quick repair.

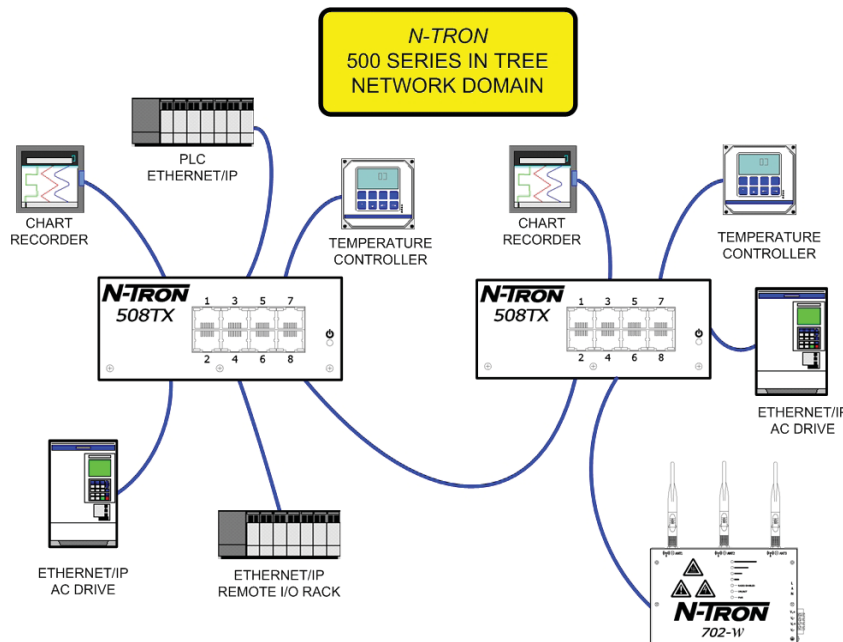
Network Topology

Unmanaged and managed switches may be configured in several topology configurations.

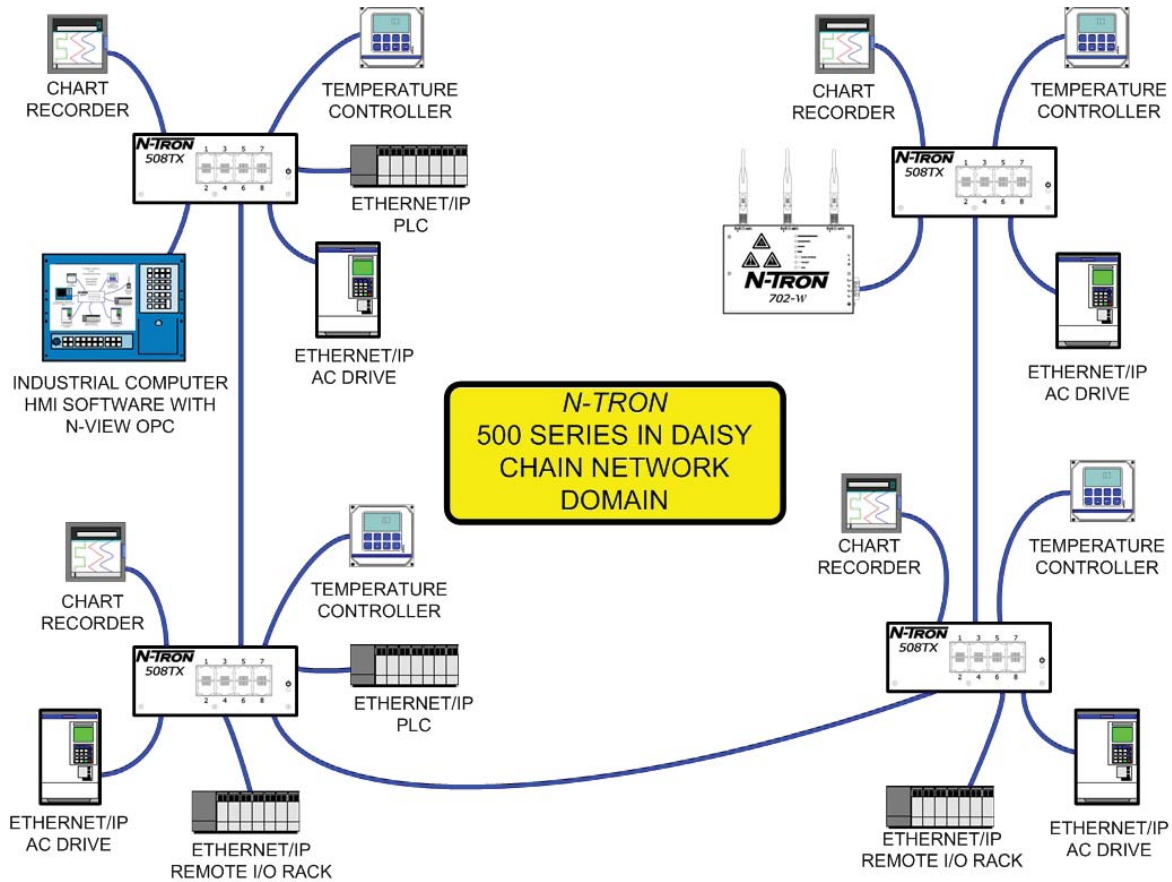
1. The star topology is always the most efficient way to interconnect switches and field devices.



2. The tree topology is a combination of two or more star configurations. The tree configuration is less efficient than a star because the data must pass through more switches in the process of traversing the network.

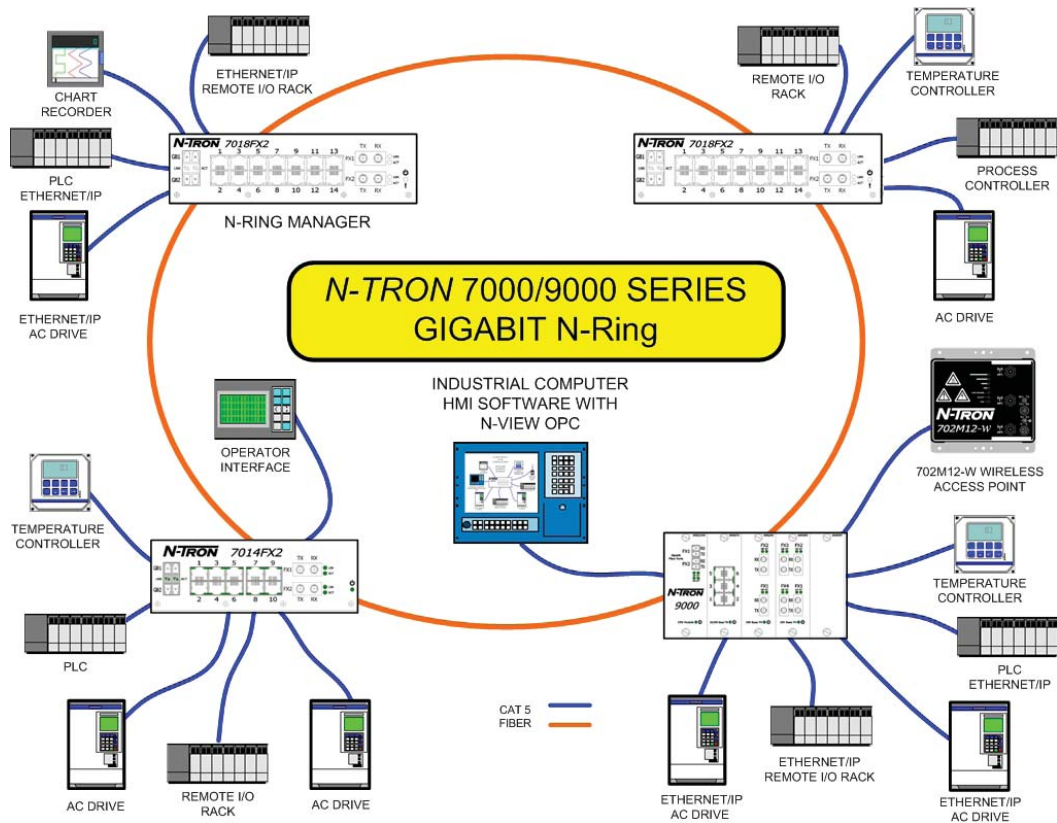


3. The least efficient network topology is the daisy chain. Daisy chain networks requires that the data travel through many intermediate switches to traverse the network.



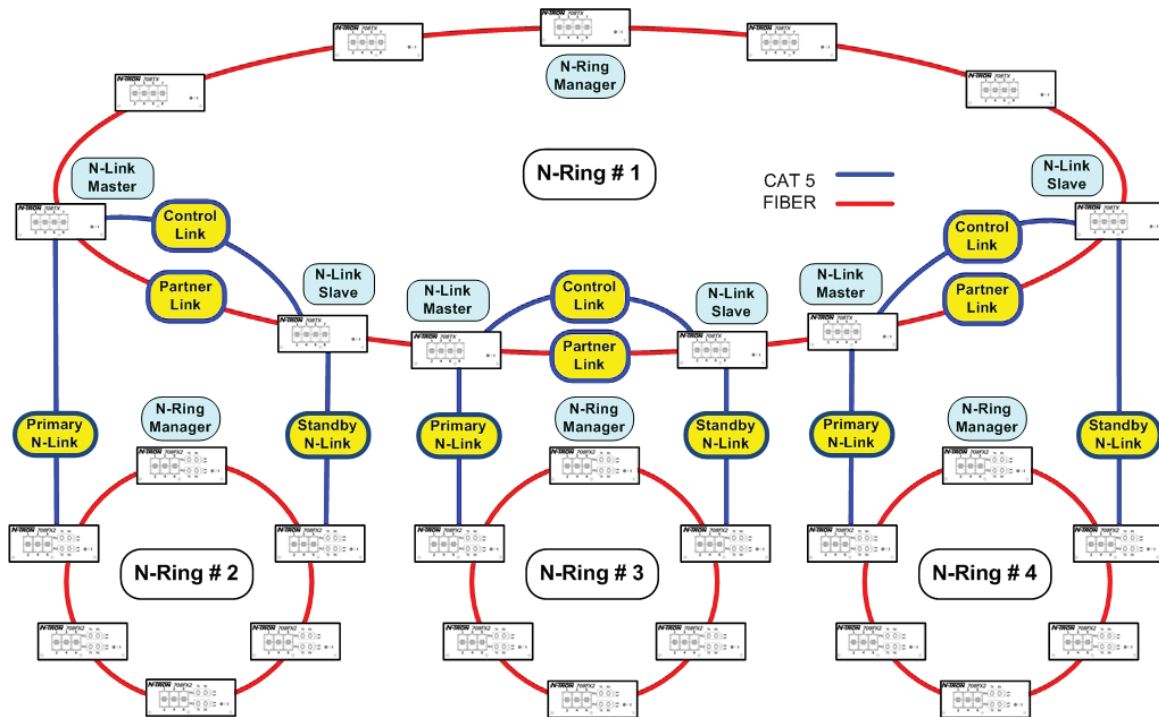
Managed switches may be configured in ring and mesh configurations if they are equipped with either Spanning Tree Protocol (STP) or one of the Rapid Spanning Tree Protocols (RSTP). Some switches may also provide an option to support proprietary high-speed ring topology. Ring and Mesh (multiple rings) is a topology normally used in critical control networks to provide redundant media paths around the network.

RSTP and proprietary ring management requires a switch that can detect the formation of a ring and block one of the ring ports in order to form a daisy chain configuration. Without a ring manager, the formation of a ring would cause replication of broadcast packets and cause what is known as a broadcast storm. This would stop or severely impact communication between devices on the ring. Blocking one port in a ring topology prevents this from happening.



The ring manager will also send packets around the ring in both directions to check the integrity of the ring. If the media is broken or damaged, the break in the ring topology will be detected by the loss of these packets. The ring manager will then unblock the ring port that was previously blocked. This allows packet communications to flow around the break in order to maintain network functionality. When the break is repaired the ring manager will again detect that the ring has been restored and block one of the ring ports.

N-Tron 700 Series Multiple N-Rings with N-Link Topology



The type of Spanning Tree or proprietary ring management used is very dependent on the switch product used in the network. The choice of a specific ring, multi-ring or mesh management switch is based on control requirements and selected topology.

Industrial networks have many demands beyond those of traditional business networks. With careful design, planning, and the use of industrial rated components, Industrial Ethernet provides harsh environments with a cost effective, high performance and highly reliable network solution.

N-TRON USA & Corporate Headquarters
 820 S. University Blvd • Suite 4E
 Mobile, AL 36609 • USA
 Phone 251-342-2164
 Fax 251-342-6353

www.n-tron.com

N-TRON ASIA

CHINA
 Phone +86-021-6194-6777
 Fax +86-021-6194-6699

INDIA
 Phone +91-9844-876540

SINGAPORE
 Phone +65-8118-6821

N-TRON EMEA

Phone +41-41-740-6636
 Fax +41-41-740-6637

N-TRON UK/Ireland/Nordic/Benelux

Phone +44 (0)1928 577257
 Fax +44 (0)870 7051506