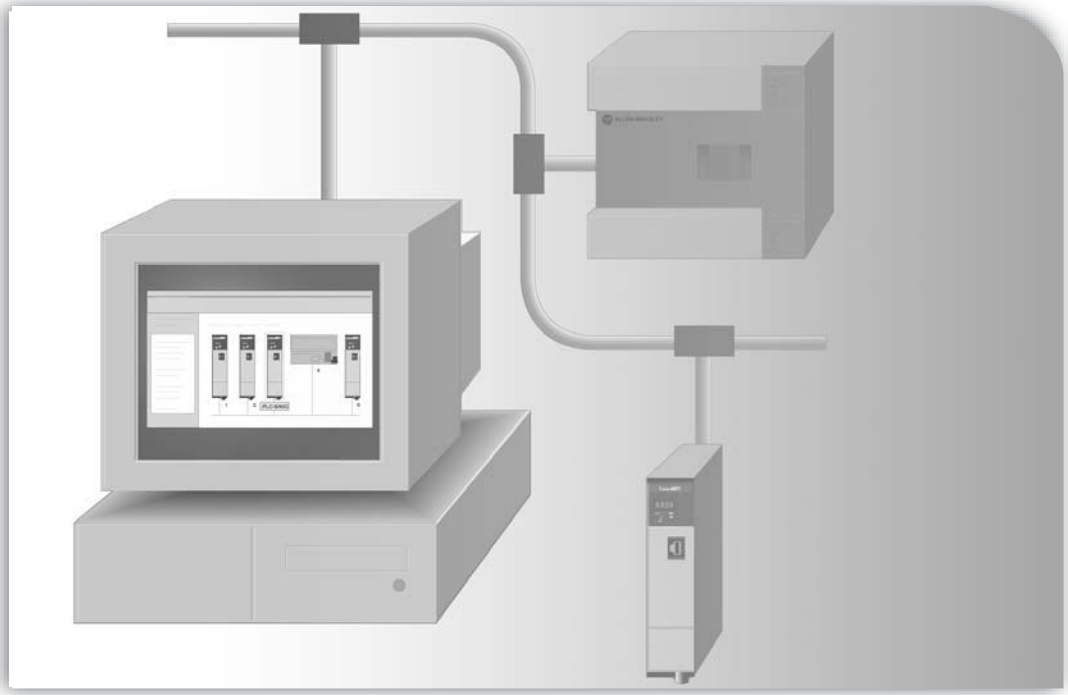
LISTEN.
THINK.
SOLVE.®



Ethernet Design Considerations for Control System Networks

AN INTRODUCTION

PUBLICATION ENET-SO001A-EN-E–November 2007

ALLEN-BRADLEY • ROCKWELL SOFTWARE

Rockwell Automation

Contact Rockwell

Customer Support Telephone — 1.440.646.3434
Online Support — http://www.rockwellautomation.com/support/

Copyright Notice

Trademark Notices

Allen-Bradley, ControlLogix, FactoryTalk, Rockwell Automation, Rockwell Software, RSLinx, RSView, and the Rockwell Software logo, are registered trademarks of Rockwell Automation, Inc.

The following logos and products are trademarks of Rockwell Automation, Inc.:

FactoryTalk Batch, FactoryTalk Historian Classic, FactoryTalk Directory, FactoryTalk Security, FactoryTalk View.

Any Rockwell software or hardware not mentioned here are also trademarks, registered or otherwise, of Rockwell Automation Technologies, Inc.

Other Trademarks

ActiveX, Microsoft, Microsoft Access, SQL Server, Visual Basic, Visual C++, Visual SourceSafe, Windows, Windows ME, Windows NT, Windows 2000, Windows Server 2003, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

ControlNet is a registered trademark of ControlNet International.

DeviceNet is a trademark of the Open DeviceNet Vendor Association, Inc. (ODVA).

Ethernet is a registered trademark of Digital Equipment Corporation, Intel, and Xerox Corporation.

OLE for Process Control (OPC) is a registered trademark of the OPC Foundation.

Oracle, SQL*Net, and SQL*Plus are registered trademarks of Oracle Corporation.

All other trademarks are the property of their respective holders and are hereby acknowledged.

Warranty

This product is warranted in accordance with the product license. The product's performance may be affected by system configuration, the application being performed, operator control, maintenance, and other related factors. Rockwell Automation is not responsible for these intervening factors. The instructions in this document do not cover all the details or variations in the equipment, procedure, or process described, nor do they provide directions for meeting every possible contingency during installation, operation, or maintenance. This product's implementation may vary among users.

This document is current as of the time of release of the product; however, the accompanying software may have changed since the release. Rockwell Automation, Inc. reserves the right to change any information contained in this document or the software at anytime without prior notice. It is your responsibility to obtain the most current information available from Rockwell when installing or using this product.

Publication Number: ENET-SO001A-EN-E November, 2007

Contents

Supervisory and Manufacturing Network Architecture Guidelines

This guide provides fundamental best-practice guidelines for designing the Ethernet infrastructure for your Supervisory Controls and Data Acquisition (SCADA) and MES (Manufacturing Execution Systems) systems with Rockwell Automation software and hardware products.

The recommendations presented in this guide are Rockwell Automation standards for Ethernet configuration. They are intended to help you build the foundation for improving network performance and securing your control system network from cyber attacks and internal malicious or unintentional mishaps. The recommendations in this guide are also based on ISA (Instrumentation Society of America) SP-99 standards for industrial automation and control system security.

The guide is intended for the following audience:

- plant control engineers
- IT managers
- system integrators
- business managers

Terminology Used in This Guide

Term	Definition
control system network	All of the devices, computers, network infrastructure, and software that are involved in manufacturing product in a plant-floor network or industrial control environment. In other industry organizations the control system network is also commonly referred to as the ‘process control network’ or the ‘automation and control system network’.
enterprise network	All of the computers, network infrastructure, and software that are involved in running office functions such as email and web services, finance systems, HR systems, and phone systems. In other industry organizations the enterprise network is also commonly referred to as the ‘business system network’.
level	Refers to levels of operations in a production facility, as defined by the Purdue Model for Control Hierarchy. This model segments industrial control devices and equipment into hierarchical functions. In this guide, levels generally refer to this concept of levels of operations. See “Overview of Network Levels” on page 5.
layer	Refers to network communication functions as defined by the OSI 7-layer model. The OSI model is also commonly referred to when discussing network architectures. In this guide, layers refer to layers of the OSI model. See “Designing the Supervisory and Manufacturing Ethernet” on page 7.

Additional Resources

While this guide is intended to provide a basic network reference architecture and design guidelines for the Ethernet network connecting the computers in your control system, see the following publications for more detailed information:

Resource	Description
Ethernet-to-the-Factory Design and Implementation Guide	http://www.cisco.com/web/strategy/manufacturing/ettf_overview.html A collaborative development guide from Cisco and Rockwell Automation that provides more detailed information and technical guidance on implementing standard networking technologies in an industrial automation and control environment.
Network Infrastructure for EtherNet/IP: Introduction and Considerations	http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf This whitepaper is published by the Open DeviceNet Vendors Association (ODVA).

Rockwell Automation TechNotes

You can access the following Technote at http://www.rockwellautomation.com/knowledgebase/.

Resource	Description
FactoryTalk View SE Distributed System Design Considerations, Answer ID 32549	Variables to consider when designing a FactoryTalk View SE distributed application.

Rockwell Automation Publications

You can view or download publications at http://www.literature.rockwellautomation.com. To order paper copies of technical documentation, contact your local Rockwell Automation distributor or sales representative.

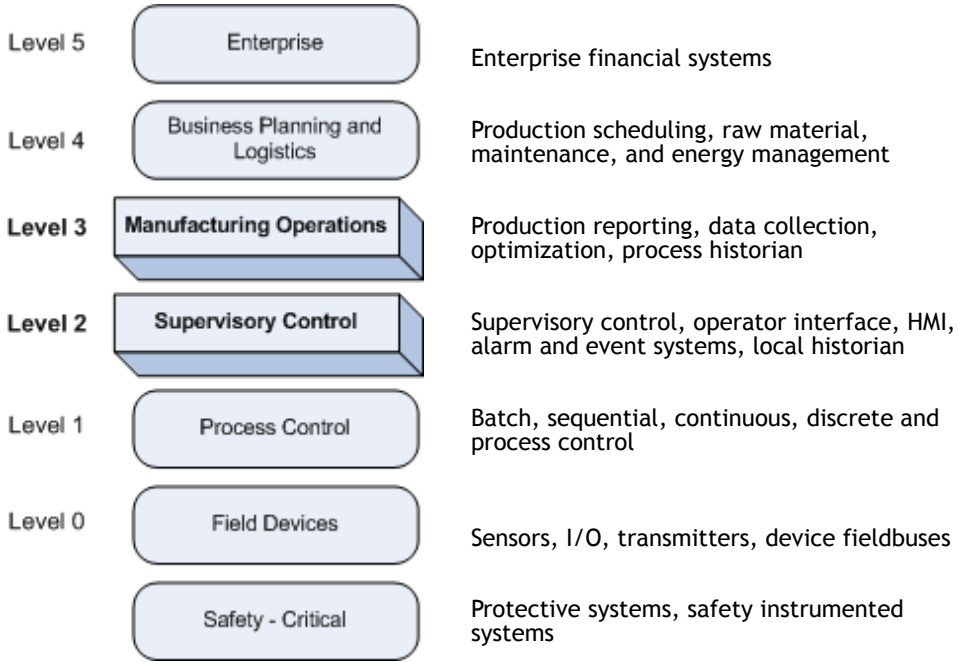
Resource	Description
EtherNet/IP Performance, ENET-AP001D-EN-P	Planning, installing, and implementing an EtherNet/IP network.
EtherNet/IP Media Planning and Installation Guide, ENET-IN001	
EtherNet/IP Modules in Logix5000 Control Systems User Manual, ENET-UM001	

Resource	Description
Integrated Architecture for Process Control System Reference Manual, PROCES-RM001A-EN-P	Process system architecture guidelines.
Logix5000 Controllers Design Considerations, 1756-RM094C-EN-P	Designing and optimizing Logix5000 controller applications.

CHAPTER 1

Overview of Network Levels

This guide refers to the S95 Hierarchy model, or Purdue Model, to describe the various environments within an industrial manufacturing organization.



Network levels in the S95 Hierarchy model, also known as the Purdue Model

This guide describes network architecture recommendations for the supervisory control (level 2) and manufacturing operations (level 3) networks.

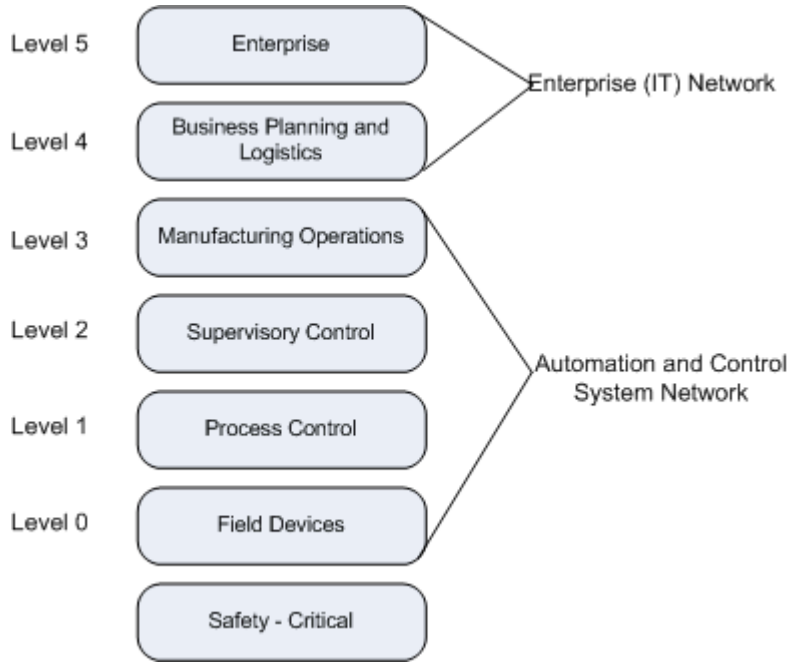
Differences in Control System Networks and Enterprise Networks

It is important to distinguish between the control system network, and enterprise, or IT networks with regard to security requirements. Separation of the control system network from the enterprise network, while allowing key data to be shared between the two networks, is critical for the success of both the plant engineering and IT organizations. It is acceptable to treat the control system network differently from the enterprise network because traffic patterns are vastly different on each type of network. Greater consideration of traffic flow and initial engineering when setting up the control system network is required to ensure a sufficient level of network performance.

Both types of networks are comprised of networks, servers, infrastructures, and hardware/software assets. The purpose for which these assets are used defines which network they reside within. Managing the control system network differently from the enterprise network is an acceptable practice. This means you may have different rules and policies to govern the control system network versus the enterprise network.

Control system network assets should be used for the sole purpose of creating, manufacturing, and shipping product. Examples of control system network elements include PACs (Process Automation Controllers), FactoryTalk View servers, automation firewalls, and RSLogix 5000 software. The control system network resides in levels 0-3.

Enterprise network elements are used for all other business purposes, such as email and web services, finance systems, HR systems, and phone systems. The enterprise network resides in levels 4 and 5.



The security goals for control system networks are different than those for enterprise networks. Control system networks must be designed to maintain availability and safety of all system components while ensuring a rapid response time. In contrast, the IT security strategy for business systems typically focuses on confidentiality as its priority, with much lower requirements for availability. For example, achieving 98 percent uptime is great for a typical business IT network, but for a manufacturing environment, 98% uptime is unacceptable.

This guide suggests best practices related to security and network design specific to automation and control systems.

Designing the Supervisory and Manufacturing Ethernet

This chapter contains guidelines for configuring the supervisory control network. In our network reference model, this is Level 2.

Rockwell Automation recommends using an Ethernet network to connect the PC clients in your control system network to the controllers and to the servers running supervisory software.

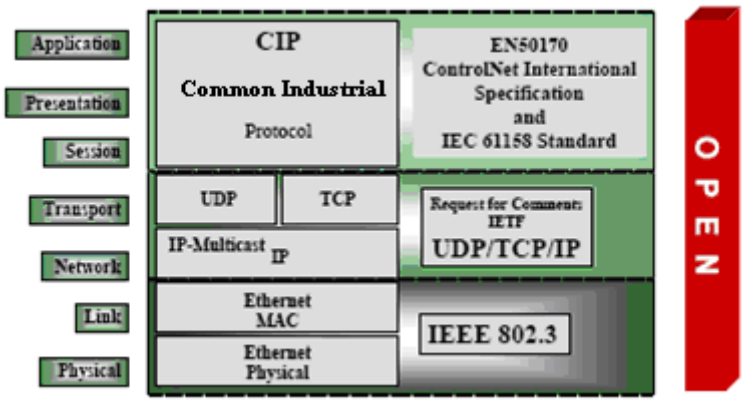
Adopting standard Ethernet and IP technologies throughout the production environment allows manufacturers to better share real-time plant-floor data with their enterprise applications. Moving to standard Ethernet and IP technologies can also result in significant cost savings, better maintenance, enhanced flexibility, and increased efficiency by easing the integration of plant-floor systems with business systems.

This guide provides best practices and recommendations for successfully integrating Ethernet and IP technologies into an industrial automation environment that uses Rockwell Automation products.

OSI Seven Layer Model

The Open Systems Interconnection Basic Reference Model, also referred to as the OSI seven layer model, is a layered, abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnection (OSI) initiative.

The terms 'level' and 'layer' are used in this guide when discussing the network reference architecture. Note that the term 'layer' refers to a layer in the OSI seven layer model. The term 'level' refers to a level of operation in a production facility as defined by the Purdue Model. (*See "Overview of Network Levels" on page 5.*)



OSI seven layer model for network communications with protocol examples

The OSI model is commonly referred to when discussing network architectures. This guide discusses best practices and recommendations regarding these layers of the OSI model within an industrial automation network:

Layer	See
1 - Physical	“Cabling” on page 21
2 - Link	“Where to Use Layer 2 Switches and Layer 3 Switches” on page 20
3 - Network	“Limiting Multicast Traffic from I/O Modules” on page 13
4 - Transport	“TCP Ports” on page 12

Rockwell Automation software products provide the Layer 7- Application communications, and the software code includes Layer 5 - Session and Layer 6 - Presentation.

For more information on the OSI seven layer model, see the following ODVA whitepaper:

- *Network Infrastructure for EtherNet/IP: Introduction and Considerations*

  http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf

Security Zones

To satisfy the various security goals of both your industrial control system and the office functions of your business, the network levels in your facility should be divided and grouped into the following security zones:

- **Enterprise Zone**

  Includes level 4, the business network of your local site, and level 5, the business network of your entire enterprise which may connect locations distributed around the world.

- **Demilitarized Zone (DMZ)**

  The Demilitarized Zone (DMZ) is a buffer zone with limited activity which separates the automation and control system network from the business network, but still allows data and services to be shared. The DMZ prevents any direct traffic between the business network and the automation and control system networks.

  A firewall blocks traffic between the Enterprise Zone and the Manufacturing Zone. Servers that provide data from the control system to the enterprise network should be placed on a DMZ created by the firewall between the factory network and the enterprise network. These computers, networks, and systems must be appropriately locked-down and hardened to prevent inappropriate access to the plant-floor network.

  The DMZ should also prevent CIP traffic from the control system from entering the enterprise network. Likewise, email and Internet traffic are prevented from entering the control system network.

- **Manufacturing Zone**

  The Manufacturing Zone is comprised of the cell/area networks included in levels 0, 1, and 2, as well as systems that manage site-wide automation and control functions in level 3. These are all the devices, systems, and computers dedicated to manufacturing product. To preserve smooth functioning of plant operations, systems, and networks, this zone requires clear isolation and protection from the above levels of plant enterprise operations.

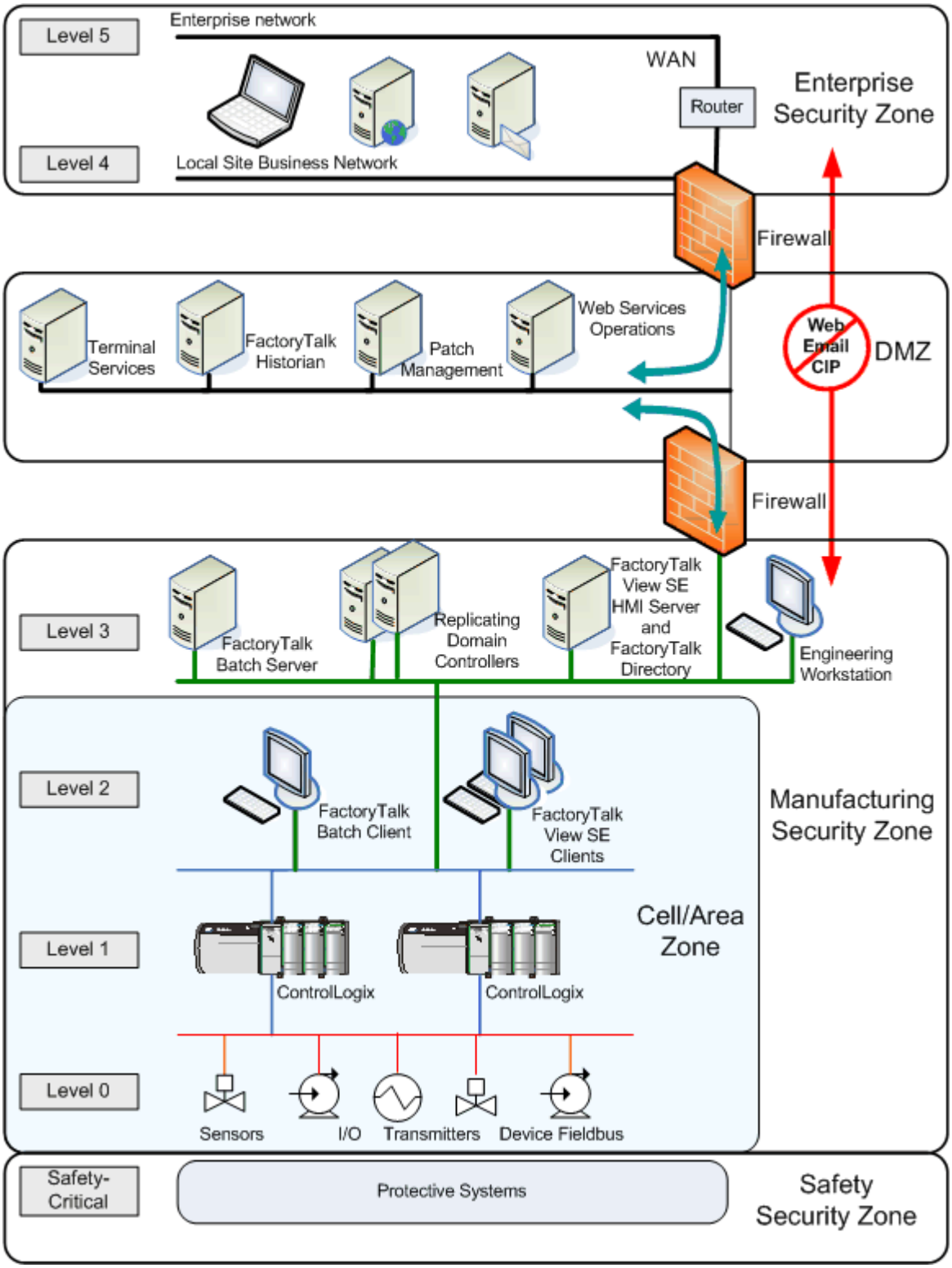
  - **Cell/Area Zone**

    The manufacturing zone may contain several cell/area zones. The cell/area zone is a functional area within a production facility. A cell/area zone contains a set of devices, controllers, and other equipment that participate in the real-time control of a functional aspect of the automation process. For example, in an automotive plant, one cell/area zone may contain a body shop, and another cell/area zone may be an assembly line. In a food and beverage facility, the batch mixing area could be defined as a cell/area zone. A cell/area zone may be as small as a single controller and its associated devices on an assembly line, or it could contain multiple controllers on several tanks. Most production facilities have multiple cell/area networks.

- **Safety Zone**

  Includes safety-instrumented systems and protective systems.

The following network reference architecture shows an example of the types of systems and Rockwell Automation products that should be located in each level and security zone. This diagram does not show all Rockwell Automation products that you may have in your automation and control system. It simply illustrates some common types of software and systems, and their placement in the overall network architecture model.



Example network reference architecture with security zones

Control System LAN

A LAN (Local Area Network) should connect all servers, workstations, and clients running HMI and other software components used for supervisory control (level 2) to computers used for manufacturing operations (level 3). These systems, along with the Programmable Automation Controllers (PACs) used for process control (level 1) and the field devices, such as sensors and I/O (level 0), should be located in the Manufacturing Security Zone.

Each cell/area network connects devices, controllers, and any other devices that need to communicate with each other in real-time (I/O communication).

Best Practice...

Rockwell Automation recommends designing the cell/area network by functional role of the devices and systems, rather than by device-type. Devices and controllers that communicate with each other need to be in the same cell/area.

From a security perspective, a security policy for the Manufacturing Security Zone should address the control equipment itself, the users of that equipment, the connections between control system components, and the interconnections with business systems and other networks.

Connecting the Control System to the Enterprise Network

While it is essential to sufficiently isolate the automation and control system LAN to protect it from the business network and the Internet, external access by some corporate users and selected third parties is required. Some network paths must exist from the plant floor to the business network for the transfer of production and maintenance management information. Vendors may need to access controllers to address technical support issues or technicians may need to access controllers remotely to perform emergency maintenance.

Firewalls

Firewalls are used to block network traffic. They are designed to prevent network traffic on one segment of a network from reaching another. A firewall within the control system network could cause problems for a distributed system that requires remote communications. The use of firewalls within the control system environment, should be carefully evaluated and should address the context of the security zones within a plant.

The firewall design should permit secure methods for authorized remote support of control systems. Opening ports within a firewall may present a security risk. For this reason, an IT security expert should be involved in the configuration.

TCP Ports

Computers make their services available to the TCP/IP network using numbered ports, one for each service that is available on the computer. For example, if a computer is running a Web server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21. Client computers connect to a service at a specific IP address and on a specific port.

The static TCP/UDP ports used by Rockwell Automation hardware and software products can be found on the Rockwell Automation Knowledgebase (http://www.rockwellautomation.com/knowledgebase/). See the following Knowledgebase article for more information:

Product	Article	ID
All Rockwell Automation software and hardware products	TCP Ports Used By Rockwell Products	29402

Many Rockwell Automation software products use DCOM, which uses dynamic TCP port assignments. See the MSDN Library document, Using Distributed COM with Firewalls for information on using DCOM in a restricted network environment. This document is available at http://msdn2.microsoft.com/en-us/library/ms809327.aspx.

Wireless Connections

Wireless connections are not recommended for connecting devices and computers within the manufacturing security zone, which includes levels 0,1,2, and 3.

While wireless connections are not recommended within the manufacturing security zone, they can enable portability and mobility when connecting to the control system network from the enterprise network. (For more information on the security zones, see “Control System LAN” on page 11.)

Although wireless technology for control systems is limited today, wireless access can be beneficial for information applications, as well as system and device configuration. Wireless connections can promote a more efficient workflow by providing access to multiple information sources without travel or second-party involvement.

If you choose to implement wireless connections in your enterprise applications, be aware that it introduces a level of unpredictability in terms of bandwidth, as well as additional security concerns. Without the proper security in place, a wireless device on a plant floor is like having an open Internet connection, which leaves the control system vulnerable to disruptive communications that could cause operational failures.

Remote Access

The common method for remote access to a control system network is to use Terminal Services through a secure VPN (Virtual Private Network) connection. Terminal Services offers a number of advantages, including acceptable performance over slow links and no need for application software maintenance on remote clients.

Network Packets

Data is transmitted over the Ethernet/IP network in packets. There are 3 basic types of packets on a network:

Packet Type	Originate from a single source to	Example
Unicast	a single node on the network	HMI traffic and MSG instructions
Multicast	multiple nodes on the network simultaneously	Input data from I/O devices and produce/consume tags
Broadcast	all nodes on the network	DHCP requests, ARP requests, NetBIOS election messages

Best Practice...

Limit the amount of broadcast and multicast traffic on the supervisory control network.

Eliminating unwanted traffic reduces the load on devices, switches, and the network. Eliminating unnecessary incoming broadcast traffic also minimizes network load.

It is important to prevent network traffic from coming into the supervisory control (level 2) and manufacturing operations (level 3) network from other levels. Likewise, it is equally important to ensure that traffic on the control system network does not get propagated into the plant enterprise network.

Limiting Multicast Traffic from I/O Modules

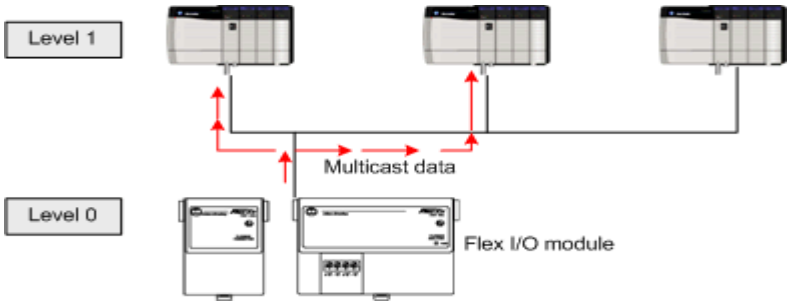
On the EtherNet/IP network devices generate data for consumption by other devices. The devices that generate the data are called producers, and the devices receiving the information are called consumers. The data exchange model is therefore referred to as the producer-consumer model.

The producer-consumer model specifies that producers of I/O data communicate via UDP unicasts or multicasts. Multicast is often more efficient than unicast because in many cases, multiple consumers want the same information from a particular producer. This means that each frame is transmitted throughout the system to make sure it reaches all the possible devices in the multicast group. The consumers (for example, controllers) typically respond with UDP unicast messages.

Since I/O modules generally produce at very fast rates, 10 milliseconds, the network can easily become flooded with multicast traffic. This also forces each end device to spend time evaluating and discarding numerous multicast frames and can significantly affect response time in the network. Rockwell Automation therefore, recommends the use of IGMP snooping to manage the multicast traffic flow. *See "IGMP (Internet Group Management Protocol) Snooping" on page 17.*

Properly configuring the RPI (Requested Packets Interval) rate for the controllers also can help to limit multicast traffic. The RPI value is the rate at which the controller attempts to communicate with the I/O module. I/O modules send input values to the controller at the specified RPI.

For guidelines on configuring the RPI rate for I/O modules, see the *Logix5000 Controllers Design Considerations Reference Manual*. More information is also available in the *Ethernet/IP Performance Application Solution*.



Multicast packets from I/O modules

CHAPTER 3

Network Hardware

This chapter describes specific types of routers, switches, and cabling, along with guidelines for where they should be used in your control system network.

Routers

Routers are computer networking devices that forward data packets toward their destinations between separate networks. When a router receives a packet, it determines the path it should take based on the source and destination addresses (IP addresses). Routers support a rich set of protocols, applications, and functionality including VPN, security, and multiservice capabilities.

Best Practice...

A router is typically used to connect the business LAN at your site to the enterprise WAN.

Switches

Industrial-rated switches are recommended for connecting the computers and other devices in the supervisory level (level 2) to each other and to higher level networks in the network reference architecture. They are preferred in a plant-floor environment.

WARNING

Hubs are not recommended because network traffic and collision rates in hub-based systems are too high for industrial control environments. Hubs are layer 1 repeaters that transmit everything received in one port to all ports; they do not interpret data or sort the messages that pass through them. Hubs do not contain any fault-tolerance mechanisms or traffic optimization functionality.

Unmanaged Switches

Although unmanaged switches are relatively inexpensive and simple to set up, they do not provide any management capabilities, security, or diagnostic information. Therefore, they are extremely difficult to troubleshoot. For these reasons, using unmanaged switches is not recommended.

Managed Switches

Although managed switches are typically more expensive than unmanaged switches and require some level of support for initial configuration and replacement, they provide many key advanced features that enable better network performance in your control system. Managed switches are able to manage multicast traffic, provide diagnostics data and security options, and other advanced features.

Best Practice...

Select industrial-rated managed switches with the following features:

- VLAN
- Full duplex capability on all ports
- Autonegotiation and manually configurable speed/duplex
- IGMP snooping
- Port mirroring
- STP
- QoS
- SNMP

VLAN (Virtual Local Area Network)

A virtual LAN (VLAN) is a switched network segmented on a functional, application, or organizational basis as opposed to a physical or geographical basis. Switches filter destination MAC addresses and forward VLAN frames only to ports that serve the VLAN to which the traffic belongs. A VLAN consists of several end systems, either hosts or network equipment (such as switches and routers), all of which are members of a single logical broadcast domain. A VLAN does not have physical proximity constraints for the broadcast domain.

Best Practice...

Rockwell Automation recommends configuring separate VLANs for different work cells or areas of your plant.

Cell zone devices on the factory floor should include only traffic (application, consumer/producer) that is relevant to running that particular cell. This can be achieved by logically segmenting traffic with the use of VLANs. Only one VLAN is recommended for all data traffic relevant to that particular area/cell zone. Because 80—90 percent of traffic is local to one cell, this is the optimal design.

All devices with multicast connections must be on the same VLAN. I/O, or peer communication traffic between PACs uses multicast messaging.

VLANs offer the following features:

- **Broadcast control**

  Just as switches isolate collision domains for attached hosts and forward only appropriate traffic out a particular port, VLANs refine this concept further and provide complete isolation between VLANs. A VLAN is a bridging domain, and all broadcast and multicast traffic is contained within it.

- **Security**

  High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside of that VLAN can communicate with them. VLANs can also assist in securing plant-floor systems by limiting access of production floor personnel (such as a vendor or contractor) to certain functional areas of the production floor.

- **Performance**

  The logical grouping of devices prevents traffic on one VLAN from burdening other network resources. Performance within the VLAN is also improved because the VLAN acts as a dedicated LAN.

- **Network management**

  A device can be logically moved from one VLAN to another by configuring a port into the appropriate VLAN. The device does not have to be physically disconnected from one network and reconnected to another which can result in expensive, time-consuming recabling.

Full duplex capability on all ports

Configuring the ports on a switch to run in full duplex operation gets the link up as fast as possible, maximizing uptime. With full duplex transmission, data can be simultaneously transmitted in both directions on a single cable. Switches running in full duplex mode provide point-to-point connections for end devices, virtually eliminating collisions between devices on the network.

Autonegotiation and Manually Configurable Speed/Duplex

Autonegotiation is designed to let devices select the most optimal way to communicate without requiring you to configure the devices. However, if you connect a manually configured device to an autonegotiation device, there can be problems which result in a high rate of CRC (Cyclic Redundancy Check) errors.

A switch that supports both autonegotiation and manual modes eliminates potential incompatibilities in the implementation of the autonegotiation by different device vendors.

Best Practice...

When configuring a switch, hard-code the fixed baud rate and duplex of your devices. TCP network settings are configurable at point to point. Refer to the User Guides for your personal computers and hardware devices to find their baud rate.

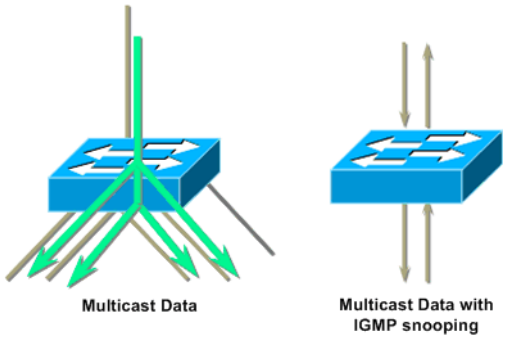
IGMP (Internet Group Management Protocol) Snooping

The Internet Group Management Protocol (IGMP) is a communications protocol that is used to manage the membership of IP multicast groups. By default, a Layer 2 switch floods multicast packets to all ports within the same subnet, creating unnecessary network traffic to devices within that subnet. Layer 2 switches can use IGMP snooping to constrain this flooding of multicast traffic by dynamically configuring the

multicast traffic to be forwarded to only those access interfaces associated with devices requesting the multicast group.

The LAN switch “snoops” or inspects the Layer 3 destination addresses specified in the network packets it receives from devices, and keeps track of multicast groups and member ports. A table lists which devices are participating in multicast groups. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. When hosts want to leave a multicast group, they can either silently leave by not responding to an IGMP query message, or they can send an IGMPv2 leave message.



The switch shown on the left shows the default method of transmitting multicast data. The switch on the right using IGMP snooping significantly reduces network traffic. Source: Cisco

IGMP Querier

The purpose of the IGMP snooping with querier is to generate periodic query messages. Consumers of particular multicast groups should respond with an IGMP report message stating that they still want to receive the data stream. If the client is finished with the stream, it does not issue the report message. The Ethernet switch, using IGMP Snooping, removes that port from the IP multicast group, which has the same effect as the client issuing an unsolicited IGMP leave message.

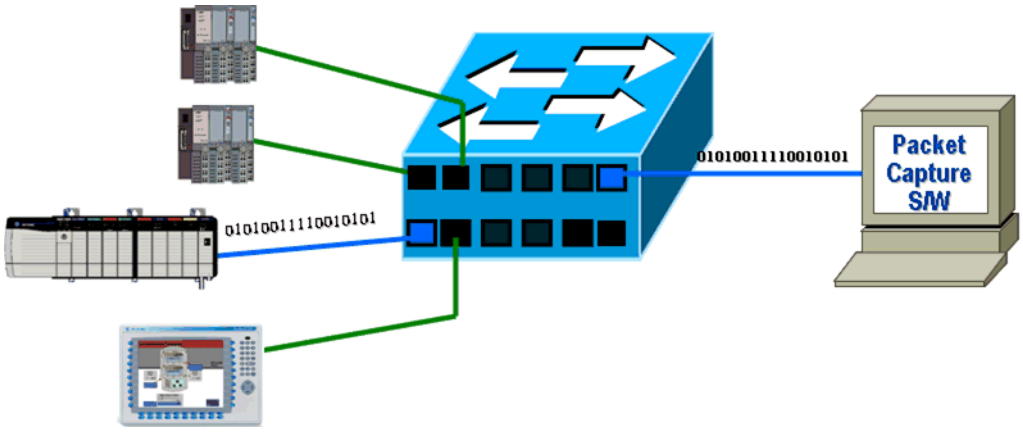
Port Mirroring

The port mirroring feature allows a switch to send a copy of all network packets seen on a switch port, a group of switch ports, or a VLAN, to a network-monitoring connection on another switch port. This is very useful for troubleshooting network issues.

Best Practice...

Rockwell Automation also recommends using a network analyzer to troubleshoot your network and to determine if multicast traffic is being managed.

Wireshark is a free, commercial-quality network analyzer that decodes over 400 protocols, including EtherNet/IP and CIP (Common Industrial Protocol). For more information, see http://www.wireshark.org.



Port Mirroring, Source: Cisco

STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol)

The Spanning Tree Protocol (STP) ensures that although multiple paths may exist between two devices connected to the infrastructure, only a single path will be used for communications at any one time. The switch should have the ability to enable and disable this feature on each port individually. Response time depends on the number of nodes on your network.

Rapid Spanning Tree Protocol (RSTP) is designed for fast network recovery. It eliminates the forwarding delay on point-to-point links by using an explicit hand-shaking protocol.

QoS (Quality of Service)

Quality of Service (QoS) refers to control mechanisms that can provide different priority to different users or data flows, or help to achieve a certain level of performance for a data flow in accordance with requests from the application program. This helps minimize latency and jitter of time-critical I/O traffic.

SNMP (Simple Network Management Protocol)

Simple Network Management Protocol (SNMP) is a TCP/IP protocol for obtaining statistical information about a device. SNMP software allows a network manager to view and modify a wide variety of network parameters, and also provides a common way to manage many diverse vendor products.

WARNING

Improper use of SNMP could tax the network infrastructure and cause disruptions or failure of your control system network.

Where to Use Layer 2 Switches and Layer 3 Switches

The following recommendations are based on a network approach that is very common and well-known in the IT world: the three-layer model of access, distribution, and core.

- The access layer provides the first level of access to the network.

  Use Layer 2 access switches within a cell/area zone to connect Level 0, 1, and 2 components (devices, controllers, and HMIs) to the network.

- The distribution layer aggregates the access layer switches and provides security and network policy enforcement.

  Use a Layer 3 distribution switch to connect a cell/area zone to other cell/area zones. In cell/area VLANs, the Layer 3 Distribution switch also performs the IGMP querier function and other LAN roles.

- The core is the backbone of the network. This layer is designed to be fast converging, highly reliable, and stable. This layer aggregates the distribution switches and often integrates connectivity to the DMZ.

For more information, see Cisco's *Ethernet-to-the-Factory Design and Implementation Guide*, available for download at http://www.cisco.com/web/strategy/manufacturing/ettf_overview.html.

Cabling

The actual wire used for the network is referred to as the physical media. The following table describes the physical media, or cabling that Rockwell Automation recommends for your Ethernet network. Select the appropriate type or types for your environment. Generally, shorter cable runs are less susceptible to EMI (electromagnetic interference) and RFI (radio-frequency interference) from electrical circuits, motors, and other machinery.

Cable Type	When to Use	Noise Immunity	Maximum Segment Length	Implementation Recommendations
Fiber Optic	■ For long distances ■ For high magnetic fields such as induction heating processes ■ For extreme high noise environments ■ For poorly grounded systems ■ For outdoor applications (including between buildings)	High	For multimode fiber, depends on the fiber and light source.	■ Multi-mode for general purposes, costs less ■ Single-node yields higher distance, but costs more
STP (Shielded Twisted Pair)	■ In environments where noises are radiated and/or conducted ■ For applications requiring metal conduit	Medium	327 feet (100 meters)	■ Shields MUST be properly grounded ■ Category 5e, 6, and 6a cables and connectors are recommended for industrial applications ■ Termination sequence 568A is preferred for industrial applications
UTP (Unshielded Twisted Pair)	■ For general connectivity where fiber is not desired or possible	Low	327 feet (100 meters)	■ Category 5e, 6, and 6a cables and connectors are recommended for industrial applications ■ Termination sequence 568A is preferred for industrial applications.

Performance Expectations

The original Ethernet specification was for 10,000,000 bits per second (10 Mbit/second). The need for even faster networks eventually resulted in the Fast Ethernet (100 Mbit/second) specification, and then the Gigabit Ethernet (1000 Mbit/second) specification. Most Ethernet-capable devices today are “10/100” or “10/100/1000”, which means they support 2 or all 3 of the specifications, respectively.

Type of Ethernet Wire	When to Use
10 Mbit/second (Traditional Ethernet)	Not recommended for new installations. This was the first method and is rarely used today. Although some small plant-floor networks consisting of I/O devices, sensors, actuators, drives, and other device interfaces, use Traditional Ethernet, faster bit rates are now encouraged.
100 Mbit/second (Fast Ethernet)	On a network that uses multiple switches, the links between the switches may benefit from this higher speed.
1000 Mbit/second (Gigabit Ethernet)	For the backbone network to connect two or more 100 Mbit/second LAN segments that may be located in separate buildings. High-demand servers are usually placed on the Gigabit backbone. You may also want to consider using a Gigabit Ethernet server adapter to transmit data at faster speeds and obtain the best performance for your server investment.

Media Converters

Media conversion should be done at the switch level, if possible. If your installation requires a media converter (copper to fiber, for example), proper selection is critical to network performance. Media converters that are layer 1 devices should be avoided because they may cause latency and slower network performance. Instead, use media converters that are layer 2 devices.

Configuring Computers on the IP Network in the Manufacturing Zone

Appropriately configuring the computers on your Manufacturing Zone network is critical to effective communication and transfer of data between the computers and devices in your automation and control system.

IP Addresses

An IP address identifies each node or machine on an IP network, or on a system of connected networks. Each TCP/IP node on a network must have a unique IP address.

IP addresses are written as four-decimal integers (0-255) separated by periods where each integer gives the value of one byte of the IP address. The four numbers in an IP address are called octets because they each have eight positions when viewed in binary form. When you add the number of positions together, they equal 32. This is why IP addresses are considered 32-bit numbers. An example of an IP address is: 215.27.61.137. The first octet in this example is 215.

The 32-bit number is divided into two parts: a network ID and a host ID. The network ID section identifies the network that a computer belongs to. The network ID always contains the first octet in the IP address. The host ID identifies the actual computer on the network. The host id always contains the last octet in the IP address. Each node on the same physical network must have an IP address containing the same network ID and a different host ID, giving it a unique IP address.

The network ID can be assigned to a particular business, government, or other entity. Because networks vary in size, there are five classes of networks. Each class has a designated range of IP addresses.

Network Class	For	IP Address Range
Class A	Large networks with many devices, such as a major international company.	0.x.x.x - 127.x.x.x
Class B	Medium-sized networks, such as a large college campus.	128.x.x.x - 191.x.x.x
Class C	Small to mid-size businesses.	192.x.x.x - 223.x.x.x
Class D	Multicast addresses.	224.x.x.x - 239.x.x.x
Class E	Experimental purposes only	

Subnets

Subnet addressing is an extension of the IP address scheme that allows a site to use a single network ID for multiple physical networks. Inside a site, the subnet mask is used to redivide the IP address into a custom network ID portion and a host ID portion.

For more information see the Microsoft KnowledgeBase article, Understanding TCP/IP Addressing and Subnetting Basics, http://support.microsoft.com/kb/164015.

Static IP Addressing

Rockwell Automation recommends assigning static IP addresses to all computers hosting a server in your control system. This includes domain controllers, FactoryTalk Directory, HMI servers, data servers, and any Rockwell Automation software server. Assigning static IP addresses to all servers helps to ensure that client computers can identify and communicate with servers.

DHCP IP Addressing

DHCP (Domain Host Configuration Protocol) can be used for computers running Rockwell Automation client software. Using DHCP reduces the IT administration required. DHCP is not recommended for Rockwell Automation software servers.

TIP You can use DHCP and BOOTP to commission a module, and then assign the module a static IP address.

Name Resolution for Distributed Software Systems

FactoryTalk software depends on “computer” name to IP address resolution to function properly. The following sections summarize the key issues for name resolution as it applies to FactoryTalk View SE and other Rockwell Automation software products.

There are two types of computer names:

- NetBIOS (Network Basic Input Output System) names

  These are also referred to as computer names.

- Host names

  These are also referred to as DNS (Domain Name System) names or FQDN (Fully Qualified Domain Name)

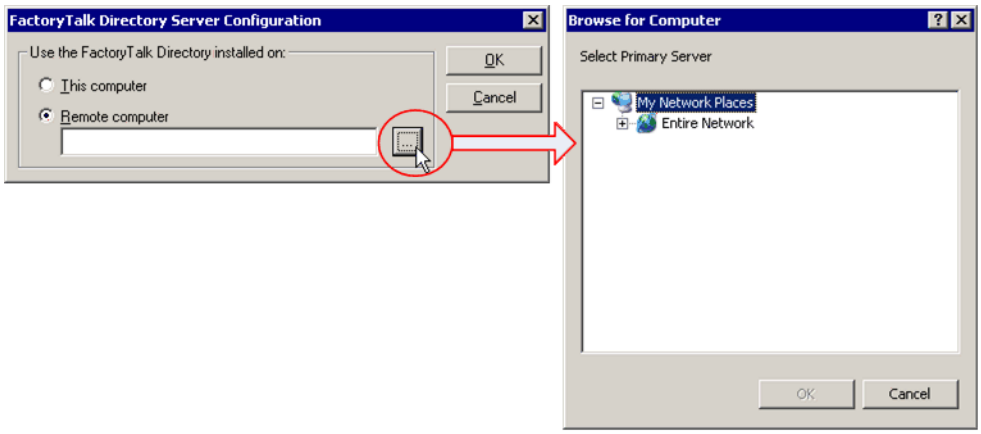
Rockwell Automation highly recommends both NetBIOS and Host name resolution for distributed software systems.

NetBIOS Names

Every computer running the Windows® operating system has a NetBIOS name, which you establish when you install the operating system. NetBIOS names are unique to Windows computers, and are limited to 15 characters.

You can find the NetBIOS name for a Windows computer by entering the command **nbtstat-n** from the command prompt.

The most common use of NetBIOS is browsing **My Network Places** to look for shares, such as folders and printers, on other computers. Rockwell Automation FactoryTalk software products also utilize NetBIOS names to locate other computers in **My Network Places**. For example, when you specify the location of the FactoryTalk Directory Server on a remote computer, you are browsing **My Network Places**.



NetBIOS Name Resolution

NetBIOS name resolution is unique to Windows networks. NetBIOS names are resolved to IP addresses using one of the methods described in the following table:

Method	Dynamic or Static	Description	Recommended For
Broadcasts	Dynamic	This is the default NetBIOS Name Resolution method for Windows networks. When each computer starts up, it announces its presence on the network. One computer is elected as the master browser. This computer keeps a list of all the computers on the network. While dynamic, this is a relatively inefficient and unreliable method due to the broadcast traffic and periodic elections of the master browser (and backup browsers).	Not recommended. Configure LMHOSTS files or WINS to disable the Broadcast method.
LMHOSTS files	Static	Each computer has a static text file that lists the NetBIOS names and their corresponding IP addresses of all Windows computers on the network. This method is best for networks where the computers are static. Using LMHOSTS files requires all computers to also use static IP addresses.	Small system architectures of ten or fewer computers deployed in a workgroup, with no server operating system.
WINS (Windows Internet Name Service)	Both Dynamic and Static	A Windows Server OS computer keeps a "database" of NetBIOS names and their corresponding IP addresses. This method is dynamic, but requires configuration and maintenance of the WINS server. Both a primary and an alternate WINS server on the network are recommended to provide fault tolerance. (See “Configuring and Managing the WINS and DNS Servers” on page 29 for more information.)	Distributed system architectures that contain at least one server operating system.

Host Names

You can find the host name for a computer by entering the commands **hostname** or **ipconfig/all** from the command prompt.

Host names are required by the TCP/IP protocol, and are used by TCP/IP applications such as web browsers, FTP, and telnet, to communicate with computers on a network. Every computer running TCP/IP has a host name, regardless of the operating system. Host names are limited to 255 characters. A computer can actually have several host names.

Do not confuse the Host name with the NetBIOS name. Host names apply to all operating systems that use the TCP/IP protocol, including Windows, Unix, Linux, MacOS, and others. A NetBIOS name is unique to computers running a Windows operating system.

WARNING

For easier operation and maintenance, Rockwell Automation recommends that the Host Name be the same as the NetBIOS name on computers running Rockwell Automation software products.

Best Practice...

Name all supervisory computers using 15 characters or less. This helps ensure that the NetBIOS name and Host name are the same on each computer. Do not use underscores or periods, and do not include any software product names in the computer name.

To connect to a computer running the TCP/IP protocol using its host name, the host name must be resolved to an IP address.

Host Name Resolution

Host name resolution is the name resolution method of the Internet. Host names are resolved to IP addresses in one of the following ways:

Method	Dynamic or Static	Description	Recommended For
HOSTS files	Static	Each computer has a static text file that lists the host names and corresponding IP addresses of all computers on the network. This method is best for networks where the computers are static. Using HOSTS files typically requires that you also use static IP addresses.	Small system architectures of ten or fewer computers deployed in a workgroup, with no server operating system.
DNS (Domain Name System)	Both Dynamic and Static	A Windows Server OS computer keeps a "database" of host names and their corresponding IP addresses. This method is dynamic, but requires configuration and maintenance of the DNS server. Both a primary and an alternate DNS server on the network are recommended to provide fault tolerance. (See “Configuring and Managing the WINS and DNS Servers” on page 29 for more information.)	Large distributed system architectures, of 10 or more computers, which contain at least one server operating system.

TIP Some Microsoft tools used to diagnose host name resolution problems are **`nslookup`** and **`netdiag`**.

Comparison of NetBIOS Names and Host Names

The following chart lists the key differences between NetBIOS names and Host names:

	NetBIOS Names	Host Names
Operating Systems	Windows only	All using TCP/IP (Windows, Unix, Linux, MacOS, others)
Maximum Number of Characters	15	255
Static Name Resolution Methods	LMHOSTS files	HOSTS files
Dynamic Name Resolution Methods	Broadcasts WINS	DNS

Configuring and Managing the WINS and DNS Servers

All computers using NetBIOS over TCP/IP should be configured with the IP address of the WINS server. Likewise, all computers using TCP/IP should be configured with the IP address of the DNS server.

- Add the WINS and DNS server roles to a server computer. Both these roles are typically assigned to the same computer, but they do not have to be.
- For large system architectures of 10 or more computers, using a Windows domain is highly recommended. On Windows 2000 and Windows 2003, the domain controller (Active Directory) requires DNS. Therefore, the computer that functions as the domain controller typically also hosts the DNS server role.
- You should manually configure all server computers on the network with the IP address of the primary and alternate WINS and DNS servers.

Best Practice...

Before deploying your Rockwell Automation control system, use the **`nslookup`** utility to verify DNS operation.

Configuring the Operating System

Securing access to the Windows operating system is critical to the development of a security policy for your control system. Only authorized users should have access to the operating system. Users should only have access to the files, systems, and services required to perform their jobs.

Best Practice...

When you install the Windows operating system on computers in the manufacturing security zone, do not install anything that is unnecessary for the operation of the automation and control system. Only install the features of Windows that you need, and antivirus software.

Windows XP SP2 and Windows Server 2003 SP1 Security Features

With the release of Windows XP SP2 and Windows Server 2003 SP1 and R2, and later versions, Microsoft has significantly increased security. Among other security measures, these service packs change permissions for launching and accessing DCOM servers, and add the Windows firewall to the operating system. The Windows firewall blocks incoming network traffic.

Windows Firewall Configuration

The Windows firewall is a host-based firewall provided with the Windows operating system to protect the computer on which it is installed. If the Windows firewall or a third-party firewall is enabled, Rockwell Automation software products require some exceptions to the Windows firewall. If the Windows firewall is enabled when you install Rockwell Automation software products, the installation program automatically adds the required Windows firewall exceptions.

Rockwell Automation also provides the Windows Firewall Configuration Utility, which you can use to modify the Windows firewall settings after Rockwell Automation software has been installed. This utility does not configure third-party firewalls. You will need to manually configure exceptions for Rockwell Automation software if you are using a third-party firewall.

Windows XP Configuration

On computers running Windows XP in a Workgroup configuration, turn off simple file sharing. For details, see Windows XP Help.

Operating System Versions and Updates

Microsoft implements service packs, security updates, hot fixes, and patches as necessary to fix vulnerabilities in the operating system.

A list of the operating systems, service packs, patches, and security updates that are supported and validated for each release of Rockwell Automation software products is provided on the Rockwell Automation Knowledgebase, http://www.rockwellautomation.com/knowledgebase/. See the following Knowledgebase articles for more information:

Product	Article	ID
FactoryTalk View SE	RSView SE Operating System and Service Pack compatibility matrix	20450
All Rockwell Automation software	Software Platform/Hardware Compatibility Matrix	42682

From these articles, a Patch Qualification compatibility matrix is also available for customers with a TechConnect contract.

For information on Microsoft security updates and patches you can subscribe to the Microsoft Technical Security Notifications:

http://www.microsoft.com/technet/security/bulletin/notify.mspx

For information on current and past hot fixes, see the Microsoft Security Bulletin Search:

http://www.microsoft.com/technet/security/current.aspx

Microsoft Service Packs

Rockwell Automation software products are tested and validated to run with specific operating system service packs with each scheduled software release. Only those service packs that have been tested to run with a specific release of Rockwell Automation software are supported. Do not apply Microsoft service packs to computers running Rockwell Automation software until Rockwell Automation has validated the service packs for compatibility with Rockwell Automation software products. See your Rockwell Automation product documentation and release notes for the supported operating systems and service packs.

Microsoft Security Updates, Patches, and Hot Fixes

Microsoft provides monthly updates (patches) to all its supported operating systems, primarily to address known security flaws. Patches introduce smaller program changes than service packs. However, Rockwell Automation does not recommend automatically applying these latest updates to plant-floor automation systems.

Plant-floor systems should be protected from security threats from external networks, either by completely isolating them or by using appropriate networking technology, such as a firewall. However, periodic updates to the plant-floor control systems may still be required to guard against internal threats. For this reason Rockwell Automation qualifies Microsoft updates with our products immediately after the updates are released.

Do not install Microsoft updates on your control system computers until they have been validated by Rockwell Automation for compatibility with our products.

Before implementing any updates to computers in your control system, verify them when your production system is inactive, or on a computer which is not being used to create, manufacture, or ship product.

Rockwell Automation Software Patch Management

Rockwell Automation publishes software patches as needed between scheduled product releases to address any urgent issues with a released version of software. On a monthly basis, patches that have been released are combined into a single roll-up. You can either apply patches individually, or apply the monthly roll-up. The patches and roll-ups are available from the Rockwell Automation Knowledgebase, http://www.rockwellautomation.com/knowledgebase/. For current patch information see the following Knowledgebase articles:

Product	Article	ID
FactoryTalk View SE	RSView SE 4.00.00 CPR 7 Patch Roll-up	35680
All Rockwell Automation software	Software Platform/Hardware Compatibility Matrix	42682

Internet Information Services

IIS (Internet Information Services) is required for HMI software (FactoryTalk View SE and ME, and RSView 32). However, IIS is not needed for FactoryTalk Transaction Manager.

Antivirus Software

Virus protection is a critical part of the security strategy for your control system. Antivirus software should be included as part of the base installation on all control system computers. Rockwell Automation supports, and has tested, Norton AntiVirus software for use with Rockwell Software products. Once antivirus software is installed, it is critical that you subscribe to updates provided by Norton AntiVirus, and develop a system for delivering these updates to all computers on your network.

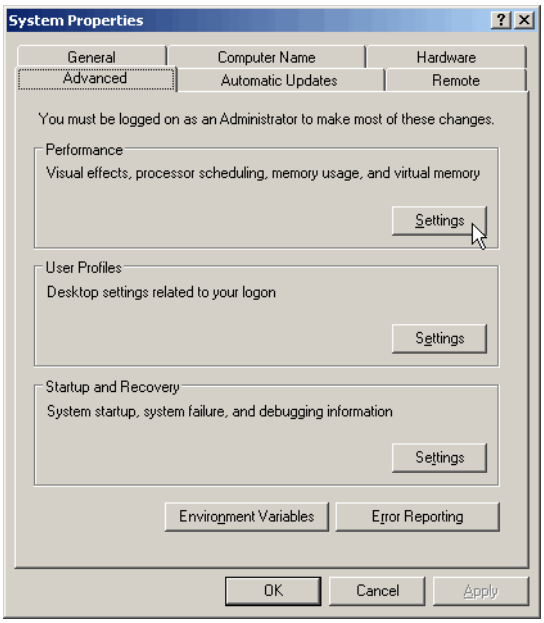
Rockwell Automation discourages performing full scans of computers in your production environment because it can cause disruptions to CPU performance.

Performance Settings for Servers

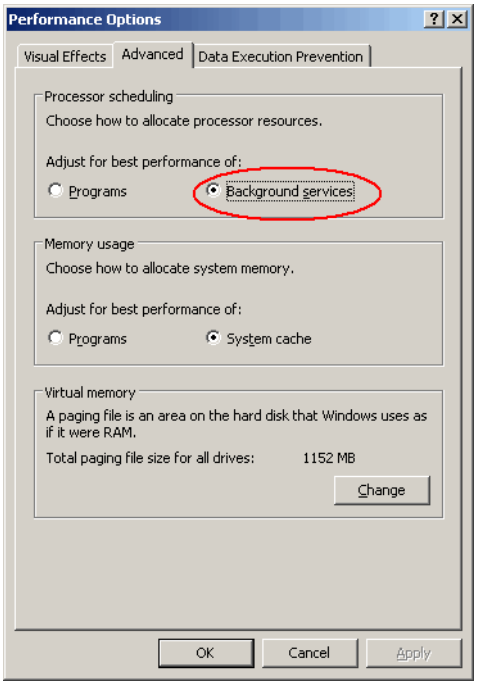
Rockwell Automation recommends the following Windows Performance Options setting for computers running Rockwell Automation software servers. For additional performance setting recommendations, see the user documentation and installation guide for the specific products you are using.

1. From the Windows Control Panel, double-click **System**.

2. In the **System Properties** dialog box, click the **Advanced** tab.



3. In the Performance area, click the **Settings** button.
4. In the **Performance Options** dialog box, click the **Advanced** tab.
5. In the Processor scheduling area, verify that the **Background services** option is selected. This is the default setting on server operating systems.

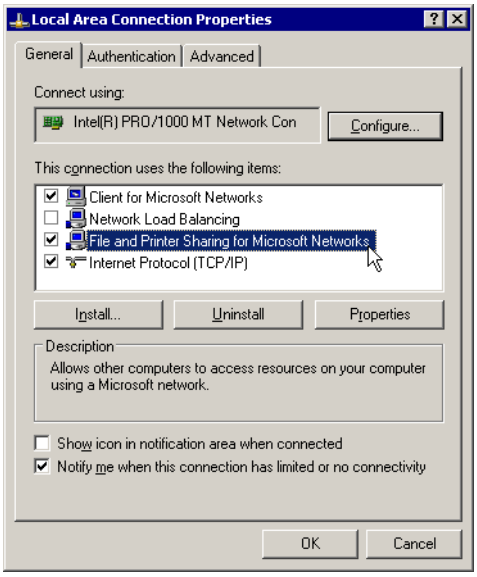


6. Click the **Data Execution Prevention** tab, if you want to check the DEP settings on your computer. For more information, see “DEP Settings” on page 36.

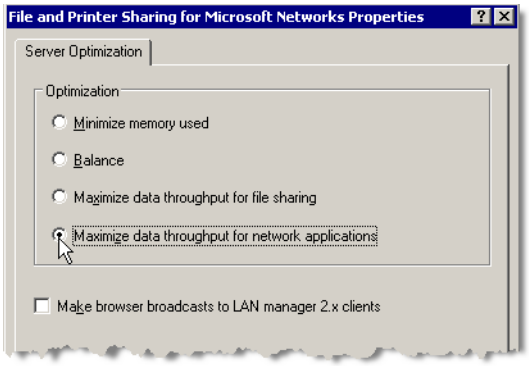
Server Optimization Settings

On Windows 2003 server computers running Rockwell Automation software servers, complete the following steps to modify the Server Optimization setting. For additional performance setting recommendations, see the user documentation and installation guide for the specific products you are using.

1. From the Start menu, select Control Panel > Network Connections > Local Area Connection.
2. In the **Local Area Connection Status** dialog box, click the **Properties** button.
3. In the **Local Area Connection Properties** dialog box, select File and Printer Sharing for Microsoft Networks.



4. Click the **Properties** button.
5. On the **Server Optimization** tab, select Maximize data throughput for network applications.



This option is recommended for improving the performance of distributed network applications.

Performance Settings for Servers and Clients

The following guidelines help improve performance of both client and server computers in your control system. For additional performance setting recommendations, see the user documentation and installation guide for the specific products you are using.

Remove Unnecessary Software and Services

Use the Add/Remove Programs utility available from the Windows Control Panel to remove unnecessary software. Use the Add/Remove Windows Components wizard in the Add/Remove Programs window to remove unnecessary services.

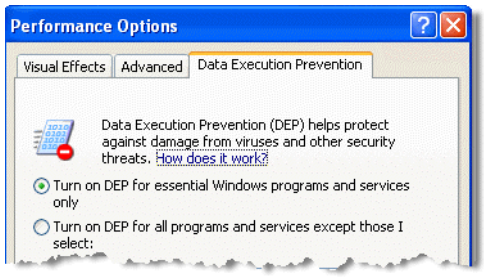
Remove Unnecessary Protocols on the Network Adapter

You can improve network performance by removing unnecessary protocols from the network adapter.

1. From the Windows Control Panel, open Network Connections > Local Area Connection.
2. In the **Local Area Connection Status** dialog box, click the **Properties** button.
3. Uninstall the following protocols if they are not being used:
   - NetBEUI
   - NWLink IPX/SPX

DEP Settings

DEP (Data Execution Prevention) is available in Microsoft Windows XP, SP2 or later and Windows 2003 SP1 or later. DEP is a hardware-based technology that protects your computer from viruses and other security threats that can attack by running malicious code from locations that only Windows and other programs should use. DEP monitors the programs on your computer to determine if they use system memory safely, and prevents programs from running in certain memory locations.



DEP Setting	Means This
Turn on DEP for essential Windows programs and services only.	This is the default setting. Rockwell Automation software can successfully run with this setting.
Turn on DEP for all programs and services except those I select.	You must add DEP exceptions for some Rockwell Automation software program files. See your product documentation for a list of specific files that must be added.

Performance Settings for Clients

Dedicated clients are computers that function as a workstation and do not act as a server in any capacity. Dedicated clients use the Windows XP operating system. You can increase performance of these clients and potentially decrease network traffic by disabling unused services. Some of the services that can be disabled on clients include:

- Server service (disable or set to Manual)

  Disabling this service provides the added benefit of increased security for the client. However, disabling the Server service prevents file sharing and remote management.

- Computer Browser service (disable or set to Manual)

  Disabling this service will not prevent you from browsing the network if NetBIOS over TCP/IP is enabled and other computers on the network are running the Computer Browser service.

- Smart Card (if you don't have a Smart Card system)

- Uninterruptible Power Supply (if you don't have a UPS connected to the computer)

- Remote Registry Service

  This service allows the registry to be edited remotely, which could present a security risk if it is not disabled.

There are many other services that you can disable to release resources on client computers and on the network. However, make sure you understand the ramifications before you disable them. If you are in doubt about the purpose of a particular service, do not disable it.

APPENDIX A

Glossary

Automation and Control System

Computer, devices, network infrastructure, and other systems which are used to create, manufacture, and ship product.

Automation DMZ
Automation Demilitarized zone

An isolation zone between a protected automation and control system network and external users, which ensures that all production traffic moving between the control system network and those external users passes through an access control device, such as a firewall. *See "DMZ Demilitarized zone" on page 40.*

Broadcast

Network packets that are directed from a single source to all nodes on a network. DHCP requests are an example of broadcast packets.

Cyber Attacks

Intrusive network traffic, malicious code, or an attempt to gain access to the non-public network from the Internet or an outside network, which is intended to disrupt operations, destroy data, or access proprietary information.

DCOM
Distributed Component Object Model

Microsoft COM (Component Object Model) is a technology in the Microsoft Windows-family of operating systems enables software components to communicate. COM is used by developers to create re-usable software components, link components together to build applications, and utilize Windows services.

The DCOM protocol transparently provides support for reliable, secure, and efficient communication between COM components such as ActiveX® controls, scripts, and Java applets residing on different machines in a LAN, a WAN, or on the Internet.

DEP
Data Execution Protection

A security feature that is supported by both hardware and software and intended to prevent the execution of malicious code in the Microsoft Windows XP (Service Pack 2) and Microsoft Windows Server 2003 (Service Pack 1 and R2) operating systems.

DHCP
Domain Host Configuration Protocol

A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. Along with IP addresses, other parameters can also be passed, such as default gateways, time services, and WINS configuration. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without requiring a unique IP address to be manually assigned.

DMZ
Demilitarized zone

A network that acts as a buffer zone between two other networks, allowing secure access to the two networks it protects. *See "Automation DMZ Automation Demilitarized zone" on page 39.*

DNS
Domain Name Service

A dynamic method of resolving computer host names to IP addresses.

Ethernet

A Layer 1 and Layer 2 protocol set forth by IEEE standards 802.2 and 802.3

EtherNet/IP
Ethernet Industrial Protocol

EtherNet/IP is a network that layers the Common Industrial Protocol over the standard protocols used by the Internet (TCP/IP and UDP). EtherNet/IP uses TCP/IP for general messaging and information exchange services, and UDP/IP for I/O messaging services for control applications.

Firewall

Hardware and/or software that protects devices on a network by blocking unwanted network traffic from entering the protected network, and limiting the communication between the protected network and other networks. A network firewall is a hardware device that protects an entire network. A host-based firewall is software that protects the asset on which it is installed.

HMI
Human Machine Interface

Computer hardware and software that enables an operator to monitor and control large machinery remotely.

Host Name

The computer name which is used by the TCP/IP protocol to identify computers on a network.

HOSTS file

A static text file that lists the host names and corresponding IP addresses of all computers on the network. The HOSTS file is copied to each computer on the network.

IEEE
Institute of Electrical and Electronics Engineers

A professional association that seeks to advance technology and develop standards in the areas of aerospace systems, computers and telecommunications, biomedical engineering, electric power, consumer electronics, and others.

IGMP
Internet Group Management Protocol

A communications protocol used to manage the membership of Internet Protocol multicast groups.

IGMP Snooping

A switch feature that takes advantage of the IGMP protocol, and constrains the flooding of multicast traffic by dynamically configuring switch ports so that multicast traffic is forwarded only to ports associated with a particular IP multicast group. *See "IGMP Internet Group Management Protocol" on page 41.*

IP Address

A four-decimal integer which uniquely identifies a computer or device on a TCP/IP network, and identifies which network the computer belongs to. Each integer can have a value ranging from 0 to 255. An example of an IP address is: 215.27.61.137.

ISA SP-99
Instrument Society of America Standards and Practices

ISA is a professional organization for industrial automation professionals. SP-99 is a sub-committee of the ISA which is dedicated to developing standards that address the subject of security for industrial automation and control systems.

LAN (local area network)

A communications network designed to connect computers and other intelligent devices in a limited geographic area.

LMHOSTS File

A static text file that lists the NetBIOS names and corresponding IP addresses of all Windows computers on the network. The LMHOSTS file is copied to each computer on the network.

Media Converter

A device that connects two different types of cabling, or physical network media; for example, copper to fiber. Media converters provide a fiber link for remote locations, allowing a switch or hub to interface with a fiber connection over a greater geographical distance.

MES
Manufacturing Execution System

A software system that companies can use to measure and control critical production activities. Some of the benefits of MES solutions are increased traceability, productivity, and quality. Other functions served by MES solutions may include equipment tracking, product geneaology, labor tracking, inventory management, costing, electronic signature capture, defect and resolution monitoring, Key Performance Indicator monitoring and alarming, Executive Dashboards and other various reporting solutions.

Multicast

Network packets that are directed to multiple nodes on a network simultaneously. For example, input data from I/O devices is sent in multicast packets.

NetBIOS Name

The computer name you assign to a computer when you install the Windows operating system. NetBIOS names are typically used for interoperability with older Windows computers and services, such as Windows NT, Windows 98, and earlier operating systems.

Network Reference Architecture

Guidelines for the network infrastructure design of automation and control systems containing Rockwell Automation products and the connection of the automation and control system network with other networks.

Packets

A package of data transmitted over a network. In addition to the data packets contain, they also include the sender's address, the receiver's address, where the package fits in relation to other packets, and how the receiving computer or device can verify that the package arrived intact.

QoS
Quality of Service

A managed switch feature that enables the switch to prioritize specific users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program.

Router

A hardware networking device that directs network traffic between different networks, or from one network to another.

SCADA
Supervisory control and data acquisition

A computer system that is used to monitor and control a manufacturing plant or industrial equipment. SCADA systems are also used to gather and analyze real time data about the control systems they are monitoring.

SNMP
Simple Network Management Protocol

A TCP/IP protocol for obtaining statistical information about a device. With SNMP software, a network manager can view and modify a wide variety of network parameters and manage many diverse vendor products.

STP
Spanning Tree Protocol

A managed switch feature which ensures that only a single path will be used for communications at any one time, even though multiple paths may exist between two devices connected to the infrastructure.

Subnet

A method of extending a site's IP address scheme so that it can use a single network ID for multiple physical networks.

Switch

A hardware networking device that provides a separate connection for each node within a network. Switches improve network performance by filtering and directing network traffic.Switches enable direct communication from one device on a network to another device on the same network.

TCP/IP
Transmission Control Protocol/Internet Protocol

A transport layer protocol (TCP) and a network-layer (IP) commonly used in business environments for communication within networks and across internetworks. EtherNet/IP communication modules use TCP/IP for explicit messaging, that is, messages in which time is not a critical factor, such as uploading or downloading programs.

Terminal Services

A Windows service that provides remote client computers access to Windows-based programs that are running on a server.

UDP/IP
User Datagram Protocol/Internet Protocol

A transport protocol that is much simpler than TCP/IP It is connectionless and provides a very simple capability to send datagrams between two modules. UDP is used by applications that implement their own handshaking between modules and only require a minimal transport service. UDP is smaller, simpler, and faster than TCP and can operate in unicast, multicast, or broadcast mode. EtherNet/IP modules use UDP/IP for real time I/O messaging.

Unicast

Network packets that are directed to a single node on the network. For example HMI traffic is sent in unicast packets.

VLAN
Virtual local area network

A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN.

WAN
Wide area network

A communications network designed to connect computers over a large distance, such as across the country or world.

APPENDIX B

Network Architecture Recommendations

This section summarizes the key network architecture recommendations presented in this guide.

Supervisory and Manufacturing Network Design Recommendations

- **Ethernet**

  Use an Ethernet network for supervisory applications in an industrial manufacturing environment.

  See "Designing the Supervisory and Manufacturing Ethernet" on page 7.

- **Security Zones**

  Establish the following security zones in your plant: Enterprise Zone, DMZ (Demilitarized Zone), Manufacturing Zone, Safety Zone.

  See "Security Zones" on page 8.

- **Firewalls**

  Place firewalls outside of the automation and control system; not within it. Firewalls and a DMZ should block network traffic between the Manufacturing Zone and the Enterprising Zone.

  See "Demilitarized Zone (DMZ)" on page 8 and "Firewalls" on page 11.

- **Wireless Connections**

  Do not use wireless connections to connect computers and devices in your control system to each other within the Manufacturing Zone. Use wireless technology to access computers and devices in your control system from the business network. Implement proper security measures.

  See "Wireless Connections" on page 12.

- **Remote Access**

  Use Terminal Services to establish remote connections to the automation and control system network.

  See "Remote Access" on page 12.

Network Hardware Recommendations

- **Routers**

  Use a router between the business LAN at your site and the enterprise WAN.

  See "Routers" on page 15.

- **Switches**

  Use industrial-rated managed switches to connect the computers and devices to each other within the supervisory-level network and to higher-level networks. The following switch features are recommended:

  - VLAN
  - Full duplex capability on all ports
  - Autonegotiation and manually configurable speed/duplex
  - IGMP snooping
  - Port mirroring
  - STP
  - QoS
  - SNMP

  See "Switches" on page 15.

- **Media Converters**

  Do not use media converters.

  See "Media Converters" on page 22.

IP Addressing Recommendations

- **Static IP Addressing**

  Assign static IP addresses to all computers hosting a server in your control system.

  Use static IP addresses for all computers in a Workgroup configuration.

  See "Static IP Addressing" on page 24.

- **DHCP**

  Use DHCP for computers running Rockwell Automation client software.

  See "DHCP IP Addressing" on page 24.

- **Name Resolution**

  NetBIOS and host name resolution is required.

  See "Name Resolution for Distributed Software Systems" on page 24.

- **NetBIOS Name Resolution**

  Use LMHOSTS files for small system architectures of ten or fewer computers deployed in a workgroup, with no server operating system.

  Use WINS for distributed system architectures that contain at least one server operating system.

  See "NetBIOS Name Resolution" on page 26.

- **Host Name Resolution**

  Use HOSTS files for small system architectures of ten or fewer computers deployed in a workgroup, with no server operating system.

  Use DNS for distributed system architectures that contain at least one server operating system.

  See "Host Name Resolution" on page 28.

Operating System Recommendations

- **Microsoft Service Packs**

  Apply only service packs that have been validated by Rockwell Automation for use with our products. See your Rockwell Automation product documentation and release notes for supported service packs.

  See "Microsoft Service Packs" on page 32.

- **Microsoft Security Updates, Patches, Hot Fixes**

  Do not install Microsoft security updates, patches, or hot fixes on your control system computers until the Microsoft updates have been validated by Rockwell Automation for compatibility with our products.

  See "Operating System Versions and Updates" on page 32.

Index

T

U

V

W

Z