



# Hirschmann Networking Interoperability to Industrial/Process and EtherNet/IP Environments

*White Paper*

Hirschmann Interoperability  
White Paper

[www.industrialnetworking.com](http://www.industrialnetworking.com)

**Main Office**

Dallas  
972-248-7466  
Fax: 972-248-9533

**West Coast Office**

California  
530-885-1552  
Fax: 530-823-0196

**Gulf Coast Office**

Houston  
713-462-8112  
Fax: 713-462-8182

**East Coast Office**

Florida  
407-852-1714  
Fax: 407-852-1409





## Contents

### HIRSCHMANN NETWORKING INTEROPERABILITY TO INDUSTRIAL/PROCESS AND EtherNet/IP ENVIRONMENTS

<b>Introduction</b>	1
<b>1. Layer 2 and Layer 3 interoperability issues</b>	4
<b>1.1 General network design and configuration factors</b>	4
<b>1.2 Specific interoperability factors</b>	5
1.2.1 Switches vs. Hubs	5
1.2.2 Speed and duplex mode	7
1.2.3 Switching performance	9
1.2.4 Port mirroring	9
1.2.5 Multicast filtering	10
1.2.6 VLAN implementation	11
1.2.7 DHCP Relay Agent	12
1.2.8 QoS	13
1.2.9 Real time (IEEE1588)	13
1.2.10 Network management	14
<b>2. Redundancy interoperability issues</b>	15
<b>2.1 Need for redundancy</b>	15
<b>2.2 Recovery time</b>	17
<b>2.3 Types of redundancy</b>	17
2.3.1 Spanning Tree and Rapid Spanning Tree Protocols	17
2.3.2 Redundant coupling	18
2.3.3 Dual homing	20
2.3.4 Link aggregation (trunking)	20
2.3.5 Hirschmann HIPER Ring	20
<b>3. Interoperability of proprietary methods with enterprise systems</b>	22
<b>4. Basic interoperability features for network security</b>	22
<b>4.1 Device security</b>	22
<b>4.2 Access control</b>	23
<b>4.3 Connection security</b>	23



## Hirschmann Networking Interoperability to Industrial/Process and Enterprise Environments

### Introduction

Originally published by Xerox in 1976 and introduced as the IEEE 802.3 standard in 1985, the networking protocol popularly known as “Ethernet” has steadily evolved to encompass commercial, residential, and industrial applications, in roughly that order.

Late to participate, industrial users are readily adopting Ethernet, encouraged by GM’s March 2003 endorsement that the “technology is now proven and ready to be deployed on the factor floor.” Ethernet’s acceptance is a result of the protocol’s ability to satisfy five needs required in industrial networking: performance (response time, bandwidth and scalability), resilience, ruggedness, economy, and interoperability.

#### Regarding EtherNet/IP:

EtherNet/IP is a network suitable for use in industrial environment and time-critical applications. It utilizes standard Ethernet and TCP/IP technologies and an open Application Layer protocol called Control and Information Protocol (CIP). CIP is also used in DeviceNet and ControlNet networks. The open Application Layer protocol makes interoperability and interchangeability of industrial automation and control devices on EtherNet/IP a reality for automation and control applications.

EtherNet/IP supports both time-critical (implicit) and non time-critical (explicit) message transfer services. Exchange of time-critical messages is based on the producer/consumer model where a transmitting device produces data on the network and many receiving devices can consume this data simultaneously.

EtherNet/IP supports both “implicit” time-critical (multicast, UDP/IP packets) and “explicit” non-time critical (unicast, TCP/IP packets) messaging required by CIP. Time-critical exchanges use a producer/consumer model, whereby a transmitting device produces data that many devices can consume simultaneously.

Consequently, EtherNet/IP support several communication functions:

- Time-critical message exchange (for I/O control)
- Human Machine Interface
- Device configuration and programming
- Device and network prognostics and diagnostics
- Compatibility with SNMP and devices with embedded TCP/IP and Web-browser services

Throughout this paper you will see the statement: EtherNet/IP interoperability requirement. This indicates areas directly covered by the EtherNet/IP specifications. In areas of this paper that do not have this entry, this means that even though there is not a direct correlation to an entry within the EtherNet/IP specification, this is good information to be aware of in designing your industrial controls network.

Regarding performance, at least seven versions of Ethernet can be employed in industrial applications (Figure A-1). The protocol scales to meet the various performance requirements of I/O, controller, workstation, and enterprise traffic. Exploiting Ethernet’s capabilities, Hirschmann industrial Ethernet products are used in discrete manufacturing and factory automation to



connect, for example, robots, paint shops, and supplier logistics centers in the automotive industry. They are also used in process industries: refineries, steelworks, refineries, and hydroelectric power stations. And they equip communication networks in airports, rail, and highway transportation systems. The Hirschmann line includes: DIN-rail-mounted (RS2) and modular (MICE) switches and hubs, backbone-oriented chassis (MACH 3000), and workgroup stackable (GES) gigabit switches.

As for resilience, Hirschmann equipment incorporates a variety of technologies that allow redundancy to be built into the network. These technologies include support for standards-based Rapid Spanning Tree Protocol (RSTP), as well as proprietary methods (Hiper-Ring) employing redundant links.

Concerning ruggedness, Hirschmann has extended its accomplishments in manufacturing enterprise-level equipment to making hardened, IP20 protection-class products for demanding factory-automation and process-control environments. Equipment is shock and vibration rated, and is designed for fan-less operation at temperatures ranging from -40° to 158°F (-40° to +70°C) for the extended environmental unmanaged switches and 32° to 140°F (0 to +60°C) for managed switches. Product approvals include UL, cUL, CSA, CE, and IEC (Figure 2).

Regarding economy, Ethernet equipment is financially attractive to industrial users, because mass-produced components are more affordable than proprietary fieldbus communication modules and interfaces. And while enterprise-level Ethernet switches have been expensive, Hirschmann switches are more affordable thanks to a lower port density suitable for industrial networks.

Concerning interoperability, this paper addresses how Hirschmann products interface with factory and process control equipment made by several industrial vendors (Rockwell Automation, Emerson, and others) and with various enterprise equipment vendors.

The focus in the following portion of this paper is interoperability at Layers 1 (physical), 2 (data link) and 3 (network) of the Open Systems Interconnect (OSI) Reference Model. It examines interoperability in terms of conformance to standards and Hirschmann's responses to those standards. The goal is to guide users about the theoretical advisability of combining different equipment.

The remaining parts examine interoperability of Hirschmann equipment in specific vendor environments to inform users how different equipment combinations work together in actuality.

Version	Speed	Cable type	Segment length (meters)	Interconnection
10BASE-T	10 Mb/s (Ethernet)	Category 3 or better	100	I/O—Controller
10BASE-FL		Fiber	2000	
100BASE-TX	100 Mb/s (Fast Ethernet)	Category 5 or better	100	Controller—plant LAN
100BASE-FX		Fiber	2000	
1000BASE-T	1000 Mb/s (Gigabit Ethernet)	Category 5	50	Plant LAN—Enterprise
1000BASE-LX		50/125 Fiber	525	
1000BASE-SX		SMF	3000	

Figure 1: Ethernet versions for industrial application



Temperature Operating Operating (extended range) Storage	32° to 142°F (0° to +60°C) -40° to 158°F (-40° to +70°C) -13° to 176°F (-25° to +85°C)
Ingress protection	IP20 (IEC 536)
Mechanical stability Shock Vibration	IEC 60068-2-27 IEC 60068-2-6
Approvals	UL 60950, cUL 508 CE (EN 61131-2, EN 60950, EN55011, EN 50178) CSA 22-2.213 Class 1 Div. 2 FM 3810 FM 3611 Div.2/Class A, B, C, D GL-Germanischer Lloyd (select products)
Electromagnetic characteristics: Interference immunity  Radio interference level Conducted emission Radiated emission	EN 50081-1 and -2 (Class B), EN50082-1 and -2  FCC Part 15 (Class B) EN 55022 Class B EN 55022 Class A
Link aggregation (trunking)	IEEE 802.3ad
Transparent bridging	IEEE 802.1d
Fast Ethernet/Autonegotiation	IEEE 802.3u
Flow control/port authentication	IEEE 802.3x
VLAN	IEEE 802.1q
Spanning tree protocol	IEEE 802.1d
Rapid spanning tree protocol	IEEE 802.1w
Gigabit Ethernet	IEEE 802.3z
IGMPv1	RFC1112
IGMPv2	RFC2236
SNMPv1	RFC 1157 (superseded)
SNMPv2 SMI	RFC 1902 (superseded)
SNMPv3	RFC 3410
MIB II	RFC 1158 and RFC 1158
RMON	RFC 1757
QoS tagging and port-based priority	IEEE 802.1p

**Figure 2: Standards-based features in Hirschmann products**



## 1. Layer 2 and Layer 3 interoperability issues

### 1.1 General network design and configuration factors

Compared to commercial networking, interoperability involves different factors in an industrial context. In office-network and enterprise equipment, the standard and proprietary features are extensive and well known.

For enterprise equipment, the feature set is very rich—and becoming more so. The guiding principle in the enterprise market is: “try to match this.” Thus, the interoperability challenge is to confirm whether or not an important feature is actually supported by a particular piece of equipment.

For industrial devices, the issue of interoperability is more basic. Incorporating Ethernet interfaces into factory automation and process control devices is relatively recent. Consequently, an Ethernet interface in industrial equipment—which may exist as a card, module, or embedded chip—will support a narrow range of features carefully selected by the vendor. Consequently, features and settings commonly found in enterprise equipment may actually interfere with the specific functions required by the industrial device’s communication needs. So on the industrial side, the primary interoperability issue is to confirm that devices work together without interference. The guiding principle is: “do no harm.”

Industrial-network components, therefore, must serve two masters—the enterprise and the factory. But due to its elaborate feature-set requirements, the enterprise is driving the new features being included in today’s industrial-network equipment.

While this trend may please IT engineers by giving them a familiar set of tools when working with industrial Ethernet switches, it is no consolation. As will be shown, features that may be taken for granted in the enterprise may be a booby-trap in the industrial environment.

Different skill sets are required when designing industrial networks, due to the decentralized/distributed architecture of industrial networks—and the critical control information they carry.

Unlike the office in which all wiring is brought back to central switching closets, industrial switches and hubs may be contained in high-voltage equipment enclosures or in the machinery itself. The distribution of network equipment—and extensive use of media converters and protocol gateways—is a by-product of the bus infrastructure used in industry, commonly known as “fieldbus.”

Networking equipment may be distributed in various manufacturing cells or located in distant process areas. Consequently, special steps must be taken to simplify configuring industrial network components.

For example, to configure RS, MICE, and MACH 3000 components quickly, Hirschmann developed the auto-configuration adaptor (ACA 11). This device stores and retrieves switch configuration data. In the event a new or replacement switch must be installed, configuration data can be quickly transferred over a terminal interface—no programming nor special personnel are required.

Another configuration option is DHCP Option 82. This allows static IP addressing based on DHCP requests. This creates an environment where devices that have malfunctioned can be replaced with another device of the same type and IP addressed and configured automatically.



After the IP address is received, the device issues a TFTP request asking for its particular configuration file. It is then downloaded, written into memory and rebooted automatically.

## 1.2 Specific interoperability factors

While properly configuring individual components with the correct settings is critical, it is equally important that each component supports features that enable devices to work together. Hirschmann has identified several factors that are critical to interoperability:

### 1.2.1 Switches vs. Hubs

#### Technology overview:

Hubs, also known as multiport repeaters or concentrators, are passive network components that simply share the bandwidth across all ports, with all connected nodes sharing the same collision domain. A hub has no logic to make traffic-direction decisions based on a MAC address or other packet contents—it merely relays the signal to other ports. For example, if eight nodes are using a hub on a 100-Mb/s network, then a single node can access only the bandwidth leftover by the other seven (Figure 3). Hubs are used to extend the physical (Layer 1) network by making it possible to add nodes or -because of a hub's ability to regenerate the signal- to add to the cabling run.

Switches are active network components that can allocate bandwidth to each port, as well as bind each port to a single collision domain. Therefore, switches are used to segment a collision domain with many nodes into multiple collision domains as granular as one port for one domain with one node (Figure 4). A switch incorporates the logic to direct traffic based on a packet's MAC address (Layer 2). Routers direct packets using IP header information.

Managed switches make it possible to allocate bandwidth and direct traffic on a priority basis using a variety of standard techniques discussed later. As a general example, if eight nodes are connected to a 100-Mb/s switch, then ports A and B can be configured to access either the full 100-Mb/s on demand, a maximum 10-Mb/s, a guaranteed use of 1-Mb/s, or some other fraction. In any case, none of the other ports will see the traffic directed to port B (Figure 4).

At the wire level, full duplex communication can be enabled in Fast Ethernet and Gigabit Ethernet switches, which uses one pair of wires in a four-pair TP cable to transmit while another pair receives. In contrast, hubs employ a half-duplex standard.

The combination of port binding, guaranteed bandwidth availability and full-duplex operation prevent delays caused by extraneous traffic on the link/segment and by packet collisions/retransmissions.

Consequently, the “gold standard” for industrial networking involves a combination of Fast Ethernet and a fully switched network. Switches enable reliable, deterministic, digital communication previously obtainable only with fieldbus protocols. The difficulty, however, is determining a network design and switch configuration that will always operate deterministically.

Differences in switch features are of little significance on lightly loaded office networks. But in complex topologies in critical industrial or enterprise applications, proper switch selection, configuration, and integration with hubs and routers are decisive.

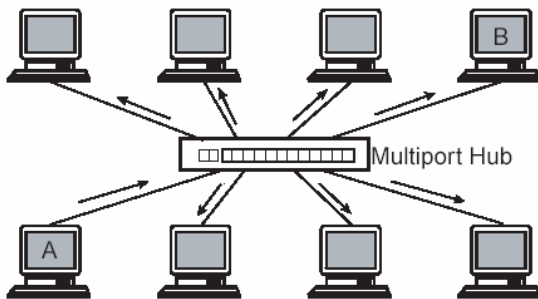


Figure 3: A hub is a multiport repeater that forms a single collision domain (Courtesy of *Industrial Ethernet Networking Guide*, Delmar Learning)

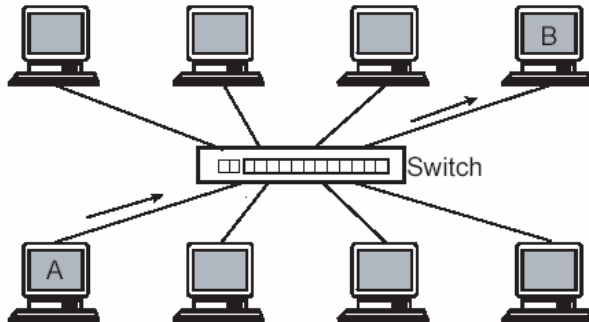


Figure 4: a switch contains multiple ports, but each port is its own single collision domain (Courtesy of *Industrial Ethernet Networking Guide*, Delmar Learning)

### Interoperability factors:

Hubs comply with IEEE 802.3 for half-duplex operation. Full-duplex hubs are proprietary products and typically only work with equipment from the same manufacturer.

Regarding configuration, hubs have no programmed settings that can conflict with other device settings. Interoperability problems are more the result of improper application in the network design. For example, network reliability will be impaired when hubs are used to add nodes that overutilize the resources of a collision domain or when half-duplex hubs are connected to full-duplex switch ports creating bottlenecks. These “interoperability” problems are more the result of user error or inexperience than incompatible vendor equipment.

Managed hubs, also known as smart hubs, may employ different serial terminal interfaces using different command structures. This is a hassle for users trying to retrieve performance information. Web-based remote access greatly simplifies the task.

Switches comply with IEEE 802.1d for transparent bridging. As a feature-rich device, they should also comply with many other standards for operating logic (Figure 2). Consequently, improper network design and switch configuration can cause a number of problems, such as: floods due to asymmetric routing, spanning-tree protocol topology changes, forwarding table overflows, and accidental VLAN merging.



Hirschmann switches comply with common standards (Figure 5) and offers additional features for applications requiring the highest network resilience.

Hirschmann device capabilities:	RS2 DIN rail mountable switches	MICE Modular industrial switches	MACH 3000 Backbone switches	GES Workgroup switches
Ethernet (10 Mb/s)	x	x	x	x
Fast Ethernet (100 Mb/s)	x	x	x	x
Gigabit Ethernet			x	x
Autonegotiation	x	x	x	x
Auto polarity	x	x	x	x
Auto crossing (MDI/MDI-X)	x	x	x	x
Wire-speed fabric	x	x	x	x
<b>Supported services:</b>				
Port mirroring	x	x	x	x
Spanning Tree:				
802.1d - STP	Q1, 2004	Q1, 2004	x	x
802.1d - RSTP	Q1, 2004	Q1, 2004	x	
HIPER-Ring	x	x	x	
IGMP snooping	x	x	x	x
GMRP	x	x	x	
VLAN	x	x	x	x
DHCP Relay Agent (Option 82)	Q1, 2004	Q1, 2004	Q1, 2004	
SNMP/NMS support	x	x	x	x
RMON	x	x	x	x
Security				
Strong password	x	x	x	x
Port security (ACL)	x	x	x	x

Figure 5: Features supported by Hirschmann equipment

## 1.2.2 Speed and duplex mode

### Technology overview:

Autonegotiation is a procedure in which a switch automatically selects the operating mode of its ports with regard to:

- Speed (10 or 100 Mb/s)
- Transmission mode half-duplex (HDX) or full-duplex (FDX)
- Flow control

When a link is set up for the first time, the switch selects the lowest common denominator shared by the interfaces. Both sides of the link must use the speed and mode variables, otherwise a link-down condition, excessive late collisions, CRC errors, and network delays will occur.

### Interoperability factors:

Autonegotiation conflicts are common. It has been said that “autonegotiation is the source of more connectivity problems and troubleshooting issues than just about anything else,” (David Newman, president Network Test, quoted in Network World Fusion, 3/31/03).

The IEEE 802.3u Fast Ethernet standard involving autonegotiation, for example, was published in 1995. Therefore, it's possible to encounter non-compliant network adapters that run an older



proprietary scheme called autosensing, which detects speed but not duplex or flow-control settings.

Full-duplex connections can only be established in point-to-point connections with devices that support full-duplex mode, such as switch-port to switch-port, switch-port to PLC, and workstation to workstation. If a half-duplex connection has to be established, network extension becomes a consideration.

Hirschmann switches are set to autonegotiate by default—like most switches available today. Autocrossing is mostly also supported when autonegotiation is enabled; thus, a Hirschmann switch will automatically configure its ports to accommodate either MDI or MDI-X pin assignments, allowing the use of either straight or cross-over cables, respectively. Auto polarity exchange is likewise supported, so if the receive line pair is incorrectly connected (RD+ and RD-reversed) polarity is automatically reversed.

Manually setting the interface to accept only one speed and a common transmission mode is a sure, but laborious way to prevent problems. Turning off autonegotiation is required by some industrial devices, as described below.

Flow control is usually not an interoperability issue. The method of flow control depends on whether the ports are set to full- or half-duplex. A non-standard scheme, called back-pressure, was used in half-duplex links. The prevailing IEEE 802.3x flow control standard applies to full-duplex links.

Switch side	User side	Result
Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Link: 100Mb/s, FDX No speed or duplex mismatch issues
Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Autonegotiating: On Support of: 10Mb/s, HDX/FDX and 100Mb/s, HDX	Link: 100Mb/s, HDX No speed or duplex mismatch issues
Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Autonegotiating: On Support of: 10Mb/s, HDX/FDX	Link: 10Mb/s, FDX No speed or duplex mismatch issues
Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Autonegotiating: Off Forced to: 100Mb/s, FDX	Link: 100Mb/s Duplex mismatch issue: Port x: HDX, Port y: FDX
Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Autonegotiating: Off Forced to: 100Mb/s, HDX	Link: 100Mb/s, HDX No speed or duplex mismatch issues
Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Autonegotiating: Off Forced to: 10Mb/s, FDX	Link: 10Mb/s Duplex mismatch issue: Port x: HDX, Port y: FDX
Autonegotiating: On Support of: 10/100Mb/s, HDX/FDX	Autonegotiating: Off Forced to: 10Mb/s, HDX	Link: 10Mb/s, HDX No speed or duplex mismatch issues
Autonegotiating: Off Forced to: 100Mb/s, HDX	Autonegotiating: Off Forced to: 100Mb/s, HDX	Link: 100Mb/s, HDX No speed or duplex mismatch issues
Autonegotiating: Off Forced to: 100Mb/s, FDX	Autonegotiating: Off Forced to: 100Mb/s, HDX	Link: 100Mb/s Duplex mismatch issue: Port x: FDX, Port y: HDX
Autonegotiating: Off Forced to: 10Mb/s, FDX	Autonegotiating: Off Forced to: 100Mb/s, HDX	Link: No stable link Speed and Duplex mismatch issues

Figure 6 Autonegotiating scenarios



## 1.2.3 Switching performance

### Technology overview:

Switch logic operates by looking at incoming packets and associating the MAC address to the incoming port ID (“learning”), comparing it to a lookup table of destination MAC addresses associated with outgoing ports (“filtering”), then transmitting the packet to the appropriate port (“forwarding”). Routers look deeper into the packet to read IP addresses.

Switch operating modes differ in the method of handling traffic (store and forward, cut-through, modified cut-through), which minimally affects network latency by taking a few microseconds to process packets.

Switch operation uses different physical mechanisms (shared-memory, matrix/mesh, or bus architecture), which impact data rate.

With matrix or mesh technology, faster distribution is achieved through an internal grid that interconnects input and output ports. Each incoming packet is quickly compared to the lookup table and then connected on the grid, called a crossbar matrix, where the input and output port intersect.

The matrix, generically known as a switch fabric, is complex, proprietary, and expensive. Fabrics are measured in bits per second (b/s) and rated in gigabits per second (Gb/s) to indicate the maximum traffic the switch can handle before a packet is dropped or stored in memory.

“Non-blocking” switch fabrics immediately make the connection at the full data rate without delay. “Blocking” switches are limited in the number of simultaneous connections that can be made at the full data rate.

### Interoperability factors:

Switch logic is based on IEEE 802.1d standard for transparent bridging. Switch mechanisms—the physical design of the fabric—are determined by the manufacturer.

Hirschmann switch modes support store-and-forward. The RS and MICE switch fabrics use a non-blocking matrix design to ensure predictable, wire-speed data throughput and minimum latency—features that benefit time-critical transmission of control data.

## 1.2.4 Port mirroring

### Technology overview:

Port mirroring forwards copies of incoming and outgoing packets from one port of a network switch to another port. The mirrored port serves as a duplicate image of the original target port and can be used to send packets to a network diagnostic tool without disrupting the client on the original port. Common diagnostic tools include network analyzers or remote monitoring (RMON) probes. Port mirroring is often used on Gigabit Ethernet switches to monitor traffic on 10/100-Mb/s links and to view traffic on all links of a VLAN.

### Interoperability factors:

Hirschmann managed RS2, MICE and all Gigabit switches support port mirroring. Note: To see full-duplex traffic on a 100-Mb/s link, the mirror port needs a capacity of 200-Mb/s (100-Mb/s x 2).



## 1.2.5 Multicast Filtering

### Technology overview:

Internet Group Management Protocol (IGMP) and GARP Multicast Registration Protocol (GMRP) are ways to restrain broadcast or multicast traffic in a switched network.

With unicast traffic, a switch learns MAC address by looking into the source address field of every frame. But with multicast packets, the switch must deal with a multicast MAC header, which may or may not appear in its bridging table. Consequently, multicast packets are copied and transmitted (“flooded”) to every port.

During multicast floods, devices are unable to use the network, wasting bandwidth at best, preventing control data from being sent at worst. The effect of multicast floods is particularly serious with full-duplex links, because the bandwidth consumed is proportional to the number of attached nodes, each of which invites a multicast packet.

IGMP prevents a flood of packets from congesting a network segment where no node is interested in receiving the packets. IGMP is an integral part of IP and is used by Routers to report their multicast status to nearby routers. These IGMP enabled routers are referred to as queriers. Queriers send out multicast group membership requests to look for multicast group members. The members send back membership reports. In this scenario, only the end stations participating in multicasts and the queriers know the multicast environment. Switches treat multicast traffic just like broadcast traffic, flooding it out all ports. To prevent this, switches can be programmed to support IGMP Snooping. When a switch must peek into the MAC header and snoop into the IP header before handling the packet, this capability is called “IGMP snooping.” This enables the switch to listen in on the Membership reports and queries and build multicast MAC address tables so that only the end stations destined to see the multicast packets see them. The multicast packet is then directed only to those nodes listed in the router’s table of multicast addresses said to be “interested” in receiving the traffic.

Because double dipping into two headers exacts a performance penalty, alternatives to IGMP snooping are sometimes used, such as laborious entry of addresses in the multicast table or faster automatic entry enabled by a proprietary protocol. In any case, the ultimate goal is to configure routers and switch to avoid multicast floods and multicast packet leaks to nodes that have not registered an interest in receiving such packets.

GMRP (GARP Multicast Registration Protocol) is employed to configure switch ports dynamically to forward IP multicast traffic to ports used by multicast hosts. It is based on using the Layer 2 Multicast address (MAC), rather than the Layer 3 Multicast address. For efficient operations, IGMP Snooping requires hardware filtering support in the switch, to differentiate between hosts membership reports and actual IPv4 multicast traffic. Especially in many older switches this support does not exist. Vendors tried to find a way around this issue to provide the benefit of constraining IPv4 multicast traffic in a switched LAN without having to build more expensive switch hardware. GARP/GMRP was designed to allow older switch hardware to support efficient multicast networks, but at layer 2. GMRP must be supported at the end device to work as it is the end device which provides the registering of the multicast group it wants to join, much like IGMP.

### EtherNet/IP interoperability requirement:

IGMP v2, using the join and leave group services subsequent to opening and closing CIP connections.

## Interoperability factors:

IGMP snooping requires a router that sends out IGMP query messages to find interested nodes. Membership reports are returned to the router, which builds a mapping table of the group and associates forwarding filters for the member port. If no router is available, some switches can take on the query function.

IGMP versions include:

- IGMPv1 (RFC1112), which allows multiple devices to send queries (configuring all switches with “querying” enabled is recommended where there is more than one multicast producer on the network)
- IGMPv2 (RFC2236), which allows only one active querier on the network.

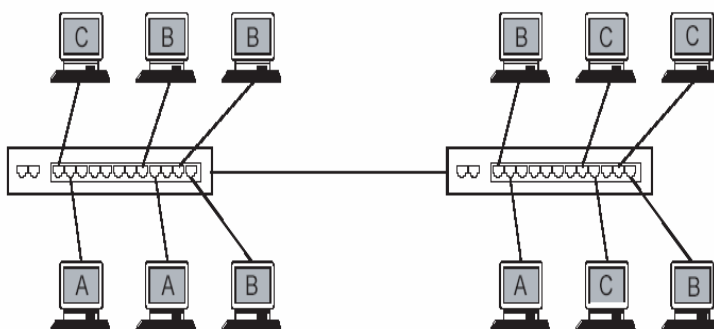
Hirschmann recommends that the two IGMP versions should not be used on the same network. GMRP and IGMP snooping and querying are supported on most Hirschmann managed switches.

## 1.2.6 VLAN implementation

### Technology overview:

Virtual LAN (VLAN) is a technique to provide network segregation across the physical environments for security reasons and to support logical groups of devices even though the nodes are on separate segments physically. The benefit is that instead of installing physical hardware to segment a network—which is difficult on large factory floors and process fields—VLANs can do it programmatically.

For example, it is possible to specify switch X ports 2 and 9 and switch Y port 2 for Supervisory LAN A, switch X ports 8, 11, and 12 and switch Y ports 1 and 12 for Process LAN B; and switch X ports 1 and switch Y ports 8, 9, and 11 to Process LAN C (Figure 7). Thus, data flow is segregated within the respective domains and insulated from general network traffic. But if a change is required—due to the need to constantly poll the device on switch X port 1, for example—a simple software command can assign that device to supervisory LAN A.



**Figure 7: VLAN enables stations of two switches to be segmented in three LANs: A, B, and C. (Courtesy of *Industrial Ethernet Networking Guide*, Delmar Learning)**

From a security aspect, a VLAN capability is useful for separating a high-security application from unauthorized users. Other uses include:



- Team applications
- Bandwidth allocation
- Plant layout/organization
- Broadcast/network-access control

#### EtherNet/IP interoperability requirement:

While 802.1q VLANs are not an explicit requirement, they are useful for providing security and logical separation of control networks. Logical separation of networks allows the user to utilize the same physical architecture and save money over buying separate physical networks.

#### Interoperability factors:

VLAN configuration can be based on either port ID, MAC, or IP addresses. The port-based VLAN standard is IEEE 802.1q. Vendor-based add-ons can support MAC or IP-based VLANs, but each switch in the VLAN must be capable of implementing such policies. Port and MAC assignment involve Layer 2 switch capabilities, but IP assignment requires a router with static routes. Determinants of interoperability include: basic link, extended trunk link, access link, and hybrid link that can confirm the exchange of VLAN-tagged and untagged frames with VLAN-aware devices.

Hirschmann managed RS2, MICE, MACH and GES products support IEEE 802.1q port-based VLANs.

## 1.2.7 DHCP Relay Agent

#### Technology overview:

DHCP Relay Agent is a switch function that allows a DHCP Discovery packet generated by an end device to be sent to and return from the DHCP server with the same IP address every time. This function is referred to as DHCP Option 82. There are 2 requirements to make this work; the port number and MAC address of the switch the DHCP Discovery packet came into and the MAC address-to-IP address mapping table on the DHCP server.

Option 82 is used to provide dynamically allocated IP addresses which are mapped to unique MAC addresses. This capability verifies that any end node receives the same IP address every time it boots up and goes into service.

Option 82 Utilizes these identifiers to determine the route the DHCP ACK packet takes to get back to the specific end device. They are added by the DHCP Relay Agent as the DHCP Discovery packet in inbound to the switch port.

This IP address provisioning is location specific. The IP addressing is based on the port number (circuit ID) and identifier (remote ID) of the switch the requesting device is directly attached to.

The circuit ID is the SNMP port index number of the switch.

The remote ID is the MAC address, IP address or other unique system identifier of the switch.

#### EtherNet/IP interoperability requirement:

DHCP Option 82 is being evaluated as the default IP address allocation tool for the EtherNet/IP environment.

#### Interoperability Factors:



Due to its very nature, Option 82 requires that all switches in the EtherNet/IP network support the DHCP Relay Agent functionality. This also allows the plant floor personnel to replace any switch that is there by just turning the power on, hooking up the cables to the network, and walking away. The IP addressing and even the download of the switches configuration from a TFTP server are done automatically. Hirschmann MICE, RS2 and MACH switches support DHCP Relay Agent operation.

## 1.2.8 QOS

### Technical Overview:

802.1p QOS is a queuing mechanism which supports multiple traffic queues at the switch port level. There are 2 queues; normal and high. There may also be multiple sub-queues under each major queue. The queuing is based on a section of the 802.1q tag on the packet. This packet with tag is generated by the end device. The 802.1q VLAN tag is 16 bytes long, 12 bytes for the VLAN tag with 4 bytes left over. 802.1p utilizes these leftover 4 bytes. The queue number placed into the 802.1q tag is mapped to a specific queue within the switch.

### EtherNet/IP interoperability requirement:

The EtherNet/IP Implementers workshop has standardized on 802.1p for the default traffic queuing mechanism. Implicit messaging would be in the high queue while explicit messaging would be in the normal queue.

### Interoperability Factors:

In order for 802.1p to work, it must be supported throughout the switched architecture of the network. Hirschmann switches support 802.1p queuing.

## 1.2.9 Real Time IP (IEEE1588)

### Technology Overview:

If hard real-time requirements are to be met, then the communication system must be able to guarantee deterministic behavior. This means always being able to exchange the required amount of data within a predefined time and that the system has to provide mechanisms to synchronize all participants very precisely.

The new IEEE Standard Precision Time Protocol (PTP) IEEE1588 is now a very comprehensive solution to do very precise time synchronization in an Ethernet network. Using IEEE1588, it is possible for the first time to synchronize, in the sub-microsecond range, the local clocks in sensors, actuators and other terminal devices using the same Ethernet network that also transports the process data.

The protocol is designed for small local networks. The designers paid particular attention to low resource usage so that the protocol can also be used in low end and low cost terminal devices.

The basic function is that the most precise clock on the network synchronizes all other users. A clock with only one network port is termed an ordinary clock. There are two clocks, Master and Slave. In principle any clock can perform both the master and slave function.

The precision of a clock, more exactly stated of their time sources, is categorized by the protocol in classes (stratum). Here the highest class is an atomic clock, which has the stratum value 1. The selection of the best clock in the network is performed automatically using the best master clock algorithm.



Every slave synchronizes to its master's clock by exchanging synchronization messages with the master clock. The synchronization process is in principle divided into two phases. First the time difference between master and slave is corrected; this is the offset measurement. The second phase of the synchronization process, the delay measurement determines the delay or latency between slave and master. Using this synchronization process, timing fluctuations in the PTP elements and the latency time between the master and slave are eliminated.

#### EtherNet/IP interoperability requirement:

Real Time IP is being evaluated by The EtherNet/IP implementer's workgroup as a standard based solution to synchronize network elements for timing. There are going to be levels of timing, depending on the type of network and the application requirements.

#### Interoperability Factors:

Because of the nature of RTP, it is recommended that the switching elements of the network support and provide the time synchronization functions for the end devices. Hirschmann MICE series switches have modules specifically made for RTP and are able to provide master timing for the RTP network.

### **1.2.10 Network management**

#### Technology overview:

Simple Network Management Protocol (SNMP) is a well-known tool that defines a structure and set of rules for managing network devices. An SNMP-managed network consists of a managed device that contains an SNMP agent itself, the SNMP agent, and a network-management system (NMS) that executes applications to monitor and control managed devices.

SNMP commands to monitor and control a managed device include: read (get information), write (change variables), trap (report an event to network management system), and traversal (allow the NMS to determine which variable a managed device supports).

SNMP versions include:

- SNMPv1 (RFC 1157)
- SNMPv2 SMI (proposed in 1993—RFC 1902)
- SNMPv3 (recently introduced to add a level of security by authenticating that a transmission originates from an authorized SNMP device, and then encrypting the transmission)

NMS operation uses SNMP to poll the device at user-defined intervals to collect information. SNMP polling should be set to the minimum needed so as not to clog the network with management traffic.

RMON (Remote Monitoring) protocol is an alternative to SNMP that transfers the monitoring responsibility to the managed device, rather than the NMS station. Thus, the agent can transmit data at convenient times and send alarms immediately without waiting to be polled.

Management Information Base (MIB) is a database maintained by the SNMP agent that logs the device's condition and the traffic passing through the device (Figure 8). The Internet Engineering Task Force (IETF) has defined MIBs for Ethernet hubs, switches, and routers.



- MIB I (RFC 1156—contains 114 database entries/objects)
- MIB II (RFC 1158 and RFC 1158 for TCP/IP network management, which supercedes MIB I and contains 185 objects)
- Proprietary MIBs can also be created with additional data and support proprietary capabilities.

#### EtherNet/IP interoperability requirement:

SNMP is needed for network visibility. It tells the network support personnel what the status of any SNMP manageable device is and be able to catch possible performance issues. The ability to catch issues before they become a network-down situation is of prime importance for a controls network.

#### Interoperability factors:

MIB is critical to interoperability. The NMS talks to the device through SNMP, but pulls information from the MIB. A common SNMP and MIB structure make it possible to operate disparate pieces of equipment, because the NMS can work with a common interface.

Managed Hirschmann switches incorporate SNMPv1 agents and MIB I objects. Hirschmann offers the HiVision NMS. Managed Hirschmann equipment also interoperates with other NMS-based software that can read MIB data directly, such as IntraVUE.

System type (hub, switch, router)
System name
Number of interfaces on device
Interface info (type, speed, address, etc.)
For each interface:
Number of bytes received
Number of unicast frames received
Number of non-unicast frames received
Number of good frames received and discarded (so as to free up buffer space)
Number of bad frames received and discarded because of errors in packet
Number of frames received and discarded because of unrecognized protocol
State of interface (on/off/testing)
Number of bytes transmitted
Number of frames transmitted
Number of non-unicast frames transmitted
Number of frames discarded before being transmitted
Number of frames that could not be transmitted because of errors
Number of collisions
Number of excessive collisions
Status of components (such as fans, memory, etc.)
Temperature (alarm if too high)

**Figure 8: Typical information contained in a MIB (Courtesy Industrial Ethernet Networking Guide, Delmar Learning)**

## 2. Redundancy interoperability issues

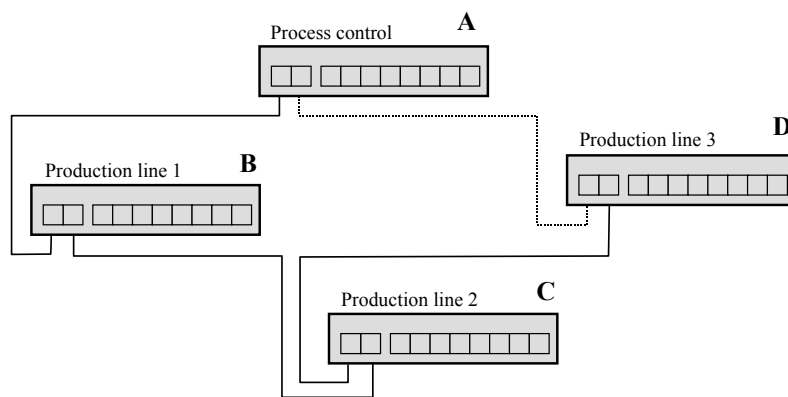
### 2.1 Need for Redundancy

Redundancy is a network-design feature in which redundant links are utilized in a linear backbone or tree topology to create an alternate path for a signal to use if a connection or device fails. For example with a backbone linking four switches, two nodes will be affected if the connection between switches B and C fails (Figure 9). But adding a cable between switches A and D as a

redundant link, the signal has another path to reach switches C and D. Unfortunately in creating an alternate path, this ring topology also creates the possibility that packets will loop indefinitely between switches—a condition known as “packet looping.”

Packet looping is triggered by several conditions, but of interest here are switch-related unicast and broadcast floods.

Unicast floods occur when an Ethernet switch transmits unicast packets to learn port numbers and MAC addresses in transparent bridging. Since learning is usually a rapid process, unicast traffic is not repeatedly flooded unless the switch didn't learn the address due to a connection or device failure, or the MAC address was aged out of the bridging table, or a redundant link caused two switches to loop packets between each other. When packet looping is the result of unicast floods, it is called a “unicast storm.”



**Figure 9: Disruption in network with a redundant link**

Broadcast floods can be initiated by NetBIOS name queries, workstation announcements, browser queries, or faulty devices incessantly transmitting ARP requests. These services are all transmitted as broadcast packets.

Note: It's good housekeeping to disable unneeded broadcast-based services, such as Windows NetBEUI for printer and file sharing. But when a broadcast flood encounters a redundant link, switches on either end will flood all ports with copies of the packet and transmit them between each other in an endless loop. This condition is known as a “broadcast storm.”

Because switches transmit unicast packets sequentially, the increase in unicast packets is additive, which means unicast storms grow linearly in intensity. But because broadcast packets are copied and flooded to multiple ports, the increase in broadcast packets is multiplicative, which means broadcast storms grow geometrically. Either problem will bring a network down.

Consequently, techniques have been developed to permit redundant links, but prevent packet looping. Six methods of redundancy will be examined below. But first, it is important to understand the correlation between the redundancy methods employed and network recovery time.



## 2.2 Recovery Time

Recovery time is a measure of how fast the network regains full availability after a failure. Obviously, the shorter the time the better in order to minimize the time to restore full network availability (Figure 10).

1. Recovery time
2. Time for transmitting stations to detect error and retransmit
3. Network load and flooding
4. Latency added by intervening devices (transceivers, gateways, etc.)
5. Latency of signal transmission through cabling
6. Switch fabric speed

**Figure 10: Factors in determining worst-case time to restore network availability**

The amount of recovery time required is a factor of how fast the switch can activate the alternate physical connection and regenerate its LAT or learned address table with new MAC addresses and port IDs.

For example in Figure 9, the primary path to send packets to switches C and D is no longer valid. Consequently, the switches need the time and the intelligence to rebuild their address tables. When the physical and logical connections are restored, the network is said to be “recovered” or “healed.”

The length of recovery time depends on the type of redundancy being employed (Figure 11).

Redundancy Method	Number of stations	Recovery Time (approximate)
Spanning tree protocol (STP)	7	45 seconds minimum up to 5 min.
Rapid spanning tree protocol (RSTP)	7 – 39	<1 to 7 seconds
Redundant coupling	N/A (point to point)	0.32-0.35 seconds
Dual homing	N/A (point to point)	1-3 seconds
Link aggregation (trunking)	N/A (backbone)	<1 to some seconds
HIPER-Ring	50	0.3-0.5 seconds

**Figure 11: Approximate recovery time correlated to redundancy method**

## 2.3 Types of Redundancy

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

#### Technology overview:

STP obtains redundancy without looping by using an algorithm that enables a switch to calculate its path efficiency and to “bid” on becoming the single “Root Bridge.” The losers of the bid sort out their best ports to reach the root bridge and allocate each of their remaining ports to a specific segment. Once active ports are allocated, the ports to redundant links are blocked to prevent packet looping.

Port states with STP are either blocking, listening, or forwarding.

STP standards are defined in IEEE 802.1d. RSTP is defined in IEEE 802.1w and improves on STP by offering greater resilience, greater network availability, and much faster recovery time.

#### Interoperability factors:

STP may take a minimum 45 seconds up to 5 minutes to detect the changes and reconfigure (Figure 11).

RSTP can reconfigure and restore service on link failures in less than a second. RSTP is forward compatible with STP and should be set as the default spanning tree implementation.

Note: When only a single switch or a strictly hierarchical topology is used, disabling the spanning tree feature can significantly reduce startup time. STP is intended for redundant links in topologies where looping can occur. Disabling STP can save time that switches would otherwise use calculating blocking and forwarding ports—a waste with tree or hierarchical topology.

Hirschmann managed switches support RSTP as stated in IEEE802.1w (Figure 15).

## 2.3.2 Redundant Coupling

### Technology overview:

Redundancy is obtained when two network segments—either linear (Figure 12) or redundant-ring (Figure 13) structures—are connected over two separate paths, each using a switch linked by a control line (Figure 14). The control line (a crossover cable) prevents packet looping. A DIP switch setting assigns one switch as the master, and the other as a redundant slave that does not transmit traffic. The two switches inform each other about their operating states via the control line. In normal operation, no data packets are transmitted over the redundant connection. But if a failure occurs in a main line of the master switch, the status is communicated over the control line to enable the slave switch to use the redundant line. If the main line is restored, the main line will be enabled and the redundant line will be disabled automatically.

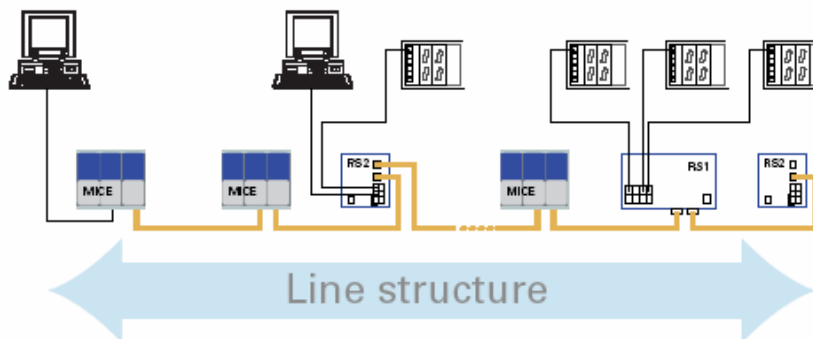


Figure 12: Line structure

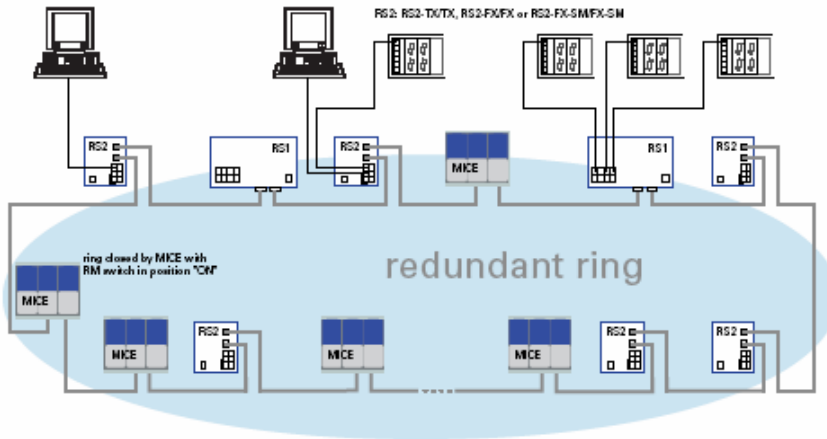


Figure 13: Redundant ring

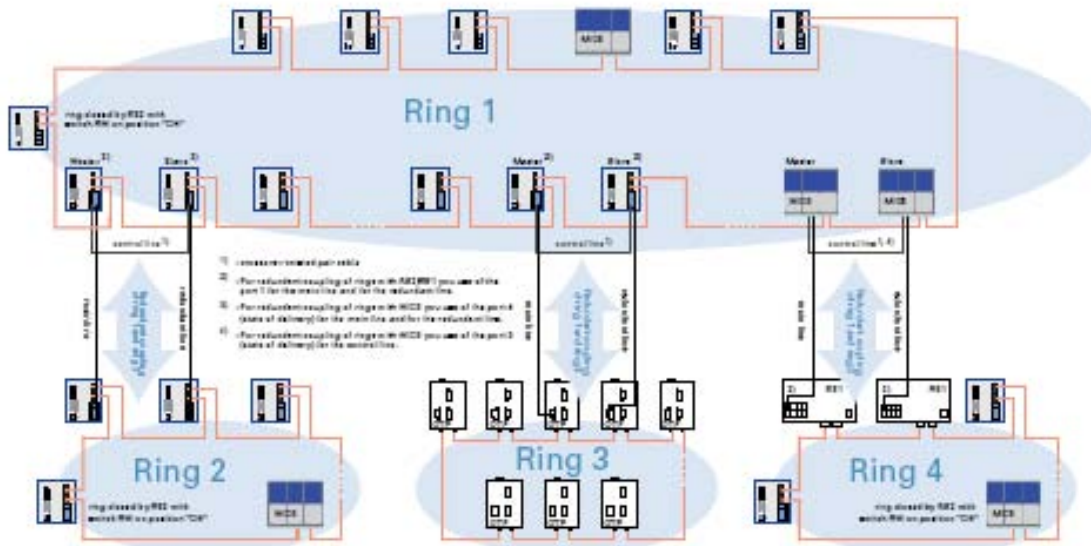


Figure 14: Redundant coupling of rings

Interoperability factors:

Redundant coupling can be used to interconnect star or redundant ring topologies. In either case, recovery time is 0.3-0.5 seconds.

Hirschmann RS2 and MICE switches support the use of redundant coupling by itself or in conjunction with the HIPER-Ring redundancy method (Figure 14).



### 2.3.3 Dual Homing

#### Technology overview:

Redundancy is obtained by using two ports: One port in the switch is for the active link, where data is transmitted. The other port is a hot standby. The hot standby link is constantly tested and will kick in if the active link fails or is disconnected.

#### Interoperability factors:

Dual homing recovery time ranges in seconds.

Hirschmann MACH 3000 switches support dual homing (Figure 15).

### 2.3.4 Link aggregation (trunking)

#### Technology overview:

Redundancy is implemented in backbone switches by creating two or more physical links bundled together to form a group. Logically, the link aggregation group is treated as a single entity by another switch. A link aggregation layer protocol controls the multiple MAC interfaces and gives them a single MAC number. Consequently, trunking multiplies bandwidth as each interface's bandwidth is added together. It also provides a level of redundancy—if one interface or connection fails, the others are available to pick up the slack.

#### Interoperability factors:

Recovery time is not strictly an issue, because the load can be shared across bundled links, ensuring some bandwidth will be available even if the total original bandwidth is not. Switches should comply with Link Aggregation Control Protocol (LACP) as defined by IEEE 802.3ad. Additional proprietary features may be encountered, however, which will affect interoperability.

Hirschmann MACH 3000 and GES switches support link-aggregation as defined in IEEE802.3ad.

### 2.3.5 Hirschmann HIPER-Ring

#### Technology overview:

Redundancy is achieved when two ends of a backbone in a line topology are closed to form a ring structure (Figure 13). Packet looping on the ring is eliminated and redundancy facilitated by activating a Redundancy Manager (RM) on a compliant switch to close the segment's redundant path to normal Ethernet traffic. The Redundancy Manager monitors the health of the network by transmitting "watchdog" packets, then listening for the packets on the return port connected to the redundant link. If a pre-determined number of watchdog packets are not received on the return port, the redundancy manager recognizes that the topology is broken and opens the redundant path to restore normal traffic. Thus, the broken ring is changed back into a line structure. Recovery time ranges between 0.3 to 0.5 s for Fast Ethernet and 0.02 to 0.1 s with Gigabit Ethernet.

#### Interoperability factors:

All Hirschmann managed RS, MICE and MACH 3000 switches support the HIPER-Ring feature, which can be used in combination with dual-homing and redundant-coupling technologies (Figure 15). The HIPER-Ring technology has gained broad acceptance in industrial applications.

With regard to STP and RSTP, HIPER-Ring redundancy is not a conflicting, but rather a complementary technology. Thus, if switches in an office LAN or high-level plant LAN use STP or RSTP to recover, these protocols will not affect switches on the control LAN using HIPER-Ring protocol as a recovery method. Conversely, HIPER-Ring watchdog packets will not be seen by enterprise switches. Thus, the two types of redundancy logic function independently, but cooperatively in parallel, each providing their respective level of redundancy services.

Redundancy mechanism	RS2 DIN rail mountable switches	MICE Modular industrial switches	MACH 3000 Backbone switches	GES Workgroup switches
HIPER-Ring	X	X	X	
STP/RSTP	Q1, 2004	Q1, 2004	X	X
Redundant coupling	X	X	X	
Dual homing			X	
Link aggregation			X	X

Figure 15: Redundancy mechanisms supported by Hirschmann products

Hirschmann equipment supports a combination of redundancy mechanisms that allows the network designer to implement different levels of resilience to handle a wide range of applications.

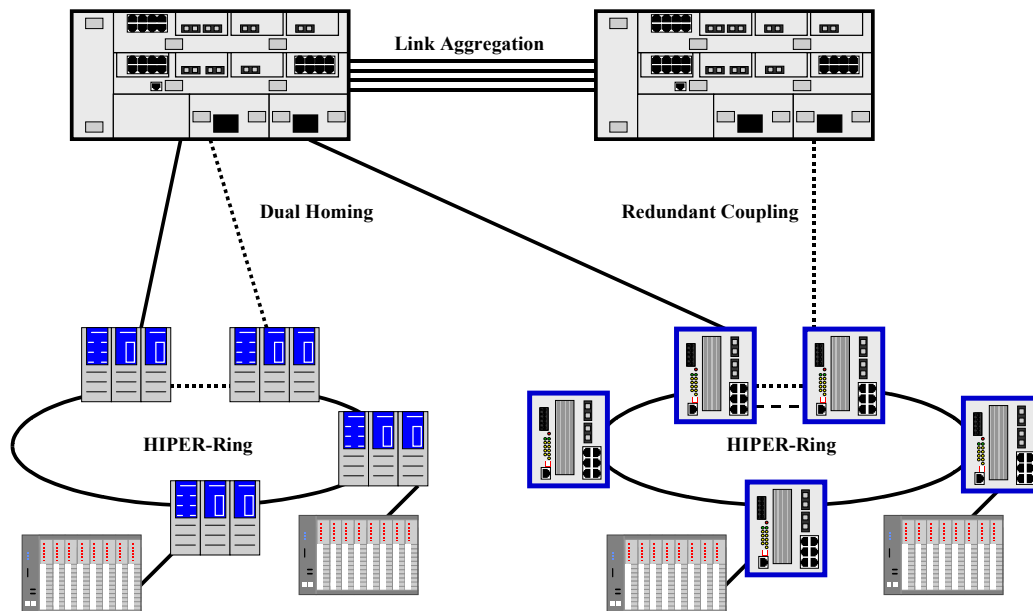


Figure 16: Redundancy



### 3. Interoperability of Proprietary Schemes with Enterprise Systems

Redundancy and other schemes must face the issue of interoperability with the enterprise. Customers expect that if a switch is standards based, then interoperability should be easily, even transparently, achieved. For example if a Hirschmann switch uses the IEEE 802.3ad link aggregation feature, it should be simple to integrate it with enterprise switches based on the same standard. Interoperability with this feature is, in fact, achievable between Hirschmann MACH 3000 switches and Cisco switches that comply with the IEEE 802.3ad link-aggregation standard.

Understanding the importance of interoperability with the enterprise, Hirschmann switches comply with many prevalent standards wherever practicable (Figure 2).

But to provide a level of functionality best suited to industrial applications, additional protocols should be employed where proven to meet user needs. That is the case with HIPER-Ring Redundancy protocol or auto-configuration adapter.

As a practical matter, the importance of using this or any proprietary feature is proportional to the need for resilience in the application.

If, for example, a slow or elastic recovery time is tolerable in a plant network, then switches with standards-based redundancy schemes can be deployed at that level. In such a case, Hirschmann switches comply with STP/RSTP standards, and they will interoperate with other compliant switches to regenerate the plant network. But in the control LAN, using Hirschmann switches that incorporate the more robust HIPER-Ring redundancy feature will provide a predictable recovery time to instill greater confidence in control-network availability.

Similarly, where plant networks can benefit from an exact resilience metric, than building the plant and control LANs with HIPER-Ring-based equipment is a sure choice (Figure 16).

As mentioned earlier, connecting directly with standards-based enterprise-level switches can be accomplished through IEEE 802.1ad-compliant trunking. But more likely, the connection between the factory LAN and the enterprise will be by means of a Layer 3 switch (router). The Layer 3 functionality of the MACH 3000 switch easily interconnects with existing enterprise and WAN infrastructures, while providing high capacity and resiliency for the industrial network—the best of both worlds.

### 4. Basic interoperability features for network security

Network security is a matter of configuring network components to permit access to network resources only by authorized users, applications, and processes. To achieve this goal involves device hardening, access control, intrusion detection, and connection security.

#### 4.1 Device security

##### Technology Overview:

Password protection: PLCs, remote I/O, HMIs, and workstations may support basic “logon” using a simple password, usually no more than eight ASCII characters long. When these devices are connected to a network, simple passwords can be easily overcome by password-cracking



programs. As much equipment as possible should support “strong passwords,” that is a combination of ASCII upper and lowercase characters, plus numbers and symbols, over eight characters long.

Port protection: Network switches and routers can be hit by port scanning programs, which try to locate a port that is open and ready to service a network protocol—such as telnet or SNMP. Because the telnet interface is often used to configure network devices remotely, care should be taken that the port is configured with a strong password to deny access. Every logon attempt should also be noted in a historical log accessible by the Network Management System (NMS).

#### Interoperability:

Hirschmann managed RS, MICE, MACH and GES switches support Password protection and Port protection.

## **4.2 Access control**

#### Technology Overview:

Access control list: Routers and other gateway devices can provide high-level network security by using extensive static or dynamic packet filtering techniques to control egress or ingress to the LAN from outside traffic. But switches are now available that incorporate the intelligence to permit or deny network access within the LAN by means of an access control list (ACL). An ACL is a table used in a switch that lets applications use, or not use, a particular port. Switches that comply with the IEEE 802.1x standard on port-based network access control can be configured to allow only authenticated devices to connect to switch ports.

Of course, settings can be manually entered to close certain ports—such as telnet port 23—to all traffic. But switches may also incorporate intelligent filtering that allows the NMS to create policies that can filter out traffic based on IP or MAC addresses.

Finally, access control can also be applied to VLANs. Because a VLAN allows multiple IP subnets within a single Ethernet switch—separating, for example, low-priority engineering traffic from high-priority control traffic—access control can securely allow program downloads from the office subnet to a PLC on the factory subnet.

#### Interoperability:

Hirschmann managed RS, MICE, MACH and GES switches support ACL as defined in IEEE802.1x and VLANs as defined in IEE802.1q.

## **4.3 Connection security**

#### Technology Overview

Sniffer countermeasures: Even with the above measures, it is possible for packet sniffers or IP spoofing to intercept legitimate traffic. Sniffers are legitimate tools generally used to troubleshoot network problems. The sniffer application can set a NIC card into promiscuous mode so it accepts all traffic within the system’s collision domain. A sniffer can also be placed on a backbone to tap into all traffic passing by. Sniffers can be counteracted by using switches that direct packets to the intended device on a specific port or to the VLAN subnet, instead of across an entire collision domain.



IP spoofing countermeasures: IP spoofing redirects traffic to another device before it arrives at its intended destination. The rerouted traffic is then captured and forwarded without detection. A countermeasure is to use virtual private networking (VPN) technology to encrypt packets between devices, which requires devices that support VPN client software, as well as a VPN-capable router, switch, or hub that can initiate a VPN session using point-to-point tunneling protocol (PPTP).

Browser security: Secure browser sessions can be conducted by employing secure socket layer (SSL) with HTTPS protocol, which encrypts application layer data, or by IP security (IPSec) standards, which encrypts and authenticates the whole packet.

Secure remote terminal login can employ secure shell (SSH) protocol as an alternative to telnet. SNMP sessions can use SNMPv3 to encrypt management commands and data. Both are typically available in enterprise-level routers and switches.

Hirschmann RS2, MICE, MACH and GES switches support SNMP v1. Hirschmann RS2, MICE and Mach switches can also encrypt their passwords. An issue with passwords is that they are passed in clear text across a network and can be captured by protocol analyzers which can be present and scanning the network.