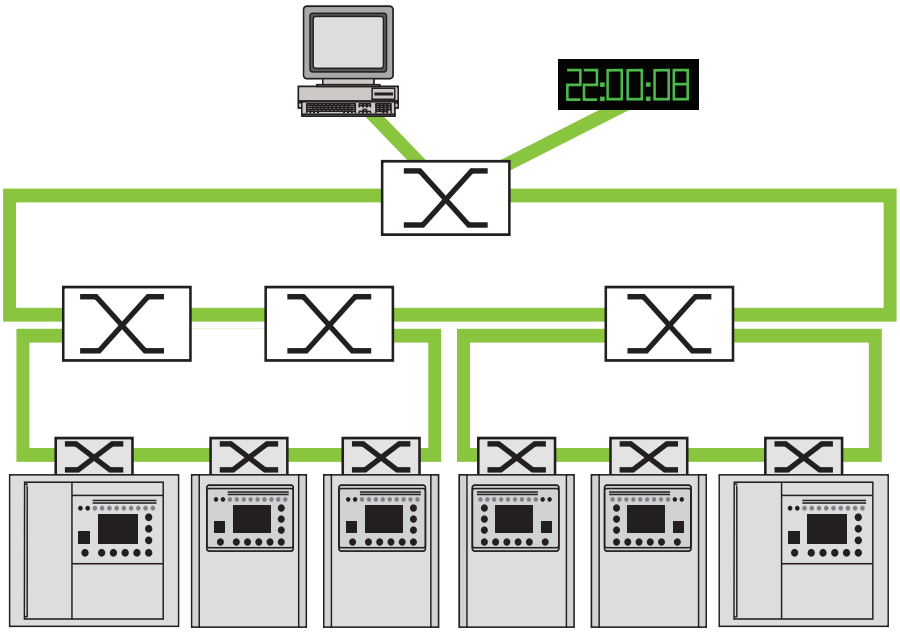
Electrical network protection

Sepam Ethernet Guide

10/2010



Schneider Electric

Contents

Presentation
About the guide

Why a Sepam Ethernet Guide?

The IEC 61850 standard requires the use of Ethernet networks in the substation but does not specify how to implement and use them nor how to achieve the requirements for performance and availability.
The use of these networks to convey critical data such as tripping orders is sometimes considered a real challenge.
The Sepam Ethernet Guide is intended to help the reader become more familiar with these technologies. It is intended to provide the reader with a level of knowledge sufficient to:

- understand networks design and operation
- set up and configure network devices
- perform first level troubleshooting
- avoid common pitfalls
- understand the peculiarities of IEC 61850.

The Sepam Ethernet Guide is focused on substation communication networks including Sepam protection relays.
Although more orientated to IEC 61850, it also applies to Modbus/TCP networks.

What this guide is not

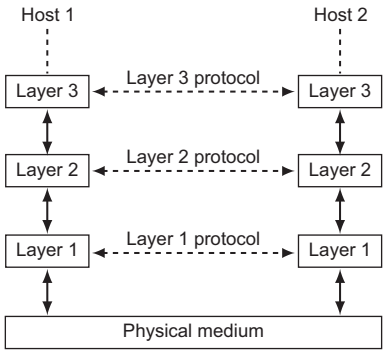
The Sepam Ethernet Guide is not a communication network reference guide. It is not either a communication network design manual.
It is not a comprehensive testing and troubleshooting guide.
And finally it is not a detailed description and explanation of standards.

Guide structure and content

The Sepam Ethernet Guide comprises 3 main parts:

- The first part introduces the fundamentals of communication with Ethernet and TCP/IP. It can be skipped if the reader is already familiar with these concepts.
- The second part describes network design and operation. It provides some practical recommendations as well as configuration guidelines.
- The last part explains how to test a network and how to find and solve commonly encountered problems.

DE80906



Layers cooperation principle.

Introduction

Networking technology frequently makes reference to a multi-layer architecture. Although several models are available, the most widely used is the Open Systems Interconnection Reference Model (OSI Model) which makes use of 7 layers. It is therefore often referred to as the OSI Seven Layer Model.

A layer is a collection of conceptually similar services provided to the layer above it and using services from the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. Conceptually 2 instances at one layer are connected by a horizontal protocol connection on that layer.

The OSI Model

	Layer	Data unit	Function
Host layers	7. Application	Data	Network process to application
	6. Presentation		Data representation and encryption
	5. Session		Interhost communication
	4. Transport	Segment	End-to-end connections and reliability
Media layers	3. Network	Packet	Path determination and logical addressing
	2. Data Link	Frame	Physical addressing
	1. Physical	Bit	Media, signal, and binary transmission

■ Layer 1:
Physical Layer. It defines the electrical and physical specifications for devices and media as well as the relationship between them.
■ Layer 2:
Data Link Layer. It provides the means of transferring data between network entities and to detect and possibly correct errors that can occur in the Physical layer.
■ Layer 3:
Network Layer. It provides the means of transferring variable length data sequences from a source to a destination, via one or more networks, while maintaining a given level of quality of service.
■ Layer 4:
Transport Layer. It provides transparent and reliable transfer of data between end users. This is achieved through error control, flow-control, segmentation, and reassembly.
■ Layer 5:
Session Layer. It establishes, manages, and terminates the connections between the applications.
■ Layer 6:
Presentation Layer. It provides independence from differences in data representation by translating from application to network format and vice-versa.
■ Layer 7:
Application Layer. This layer interacts directly with software applications that implement communication. It typically provides means of identifying the communication partners, determining resources availability, and synchronizing communication.

Introduction to Ethernet
Overview

What is Ethernet?

Ethernet is a family of technologies commonly used for Local Area Networks (LAN). It defines the wiring and signalling methods for the physical layer, the frame format, and a common addressing policy.
The name is supposed to come from the initial use of a shared media, like the "ether". Ethernet was first standardized as IEEE 802.3 in 1982. It is now an international standard: ISO/IEC 8802-3 but is still best known under its previous name.
IEEE 802.3 is a member of the large IEEE 802 family of standards describing LAN and WAN networking.

A bit of history

Ethernet was born in the early 1970s, in the Xerox Palo Alto Research Center. Its invention is attributed mainly to Robert Metcalfe.
The expansion of Ethernet however really began when DEC and Intel joined Xerox to define the so-called "DIX" standard, published in 1980 that specified a 10 megabits/second Ethernet, with 48-bit destination and source addresses and a global 16-bit type field.

At that time, Ethernet was based on a shared medium, a single coaxial cable, using an access method called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
The advantage of CSMA/CD over its competitors, such as Token Ring and Token Bus, is the simplicity, as every device is directly connected to the cable and can transmit whenever it wants to. On the other hand, this principle can cause frame collisions to occur if several devices start to transmit at the same time.
CSMA/CD provides a mechanism to prevent such collisions and detect them with certainty when they occur. This is the origin of segment length limitations and packet minimum size that still apply today: a packet must reach all parts of the medium before the transmitter stops to effectively discover collisions.
Ethernet technology has gained an increasing success over the years and evolved to simplify wiring and reduce costs: thin coaxial wire, twisted pair, hubs, switches, etc. Today, Ethernet is a versatile nevertheless complex networking technology, very different from the origins.

Modern Ethernet

The only real drawback of Ethernet is the occurrence of collisions that can dramatically reduce the usable throughput of the network. The advent of switching technology enables the creation of collision-less, full-duplex networks in which the shared media are replaced by point-to-point connections.
Higher speeds of 100 Mbits/s, 1 Gb/s or even 10 Gb/s are commonly used nowadays and give Ethernet unprecedented capabilities.

Some definitions

Collision domain

A collision domain is a physical network subset where frames sent on a shared medium can collide with one another. Collisions decrease overall network throughput and should be avoided as much as possible. Large networks are therefore divided into separate smaller collision domains, using layer 2 network components such as switches.

Unicast, multicast and broadcast

A unicast transmission occurs between a source and a single destination recipient. Conversely, a multicast transmission is a transmission from a source to multiple recipients on the network.
Broadcast transmission is a special case of multicast transmission where the data is meant to reach every available node on the network.

Broadcast domain

A broadcast domain is the logical division of a network containing all the nodes that can reach each other by broadcasting.
Broadcast domains help reduce the amount of traffic that would otherwise be spread over the whole network.
Layer 3 devices form boundaries between broadcast domains.

Duplex mode

A communication channel is half-duplex when transmission can occur in only one direction at a time. It is full-duplex when transmission in both directions can occur simultaneously.
With the legacy CSMA/CD access method, transmission is always half-duplex as the receive channel of a transmitter is used to listen for collisions.
However, when using point-to-point links between devices and switches, the collision domain is limited to these 2 nodes and full-duplex can be used with the following advantages:
- collisions are definitively eliminated (deterministic performance)
- the bandwidth is doubled.

Autonegociation

The majority of recent Ethernet devices support autonegotiation which is the ability for 2 devices on a point-to-point link to share their capabilities and then choose the best common transmission parameters (speed and duplex mode).
Autonegotiation is a physical layer mechanism that makes use of encoded link pulses transmitted during communication idle time.
As of today, autonegotiation is not available on fiber optics devices, at least for current speeds.

VLAN or V-LAN

A virtual LAN, commonly known as a VLAN, is a group of devices with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. Conversely, VLANs are used to divide a network into smaller broadcast domains.
Using a VLAN to segment traffic can increase network performance by reducing the traffic loads. It offers a flexible way to modify groups in an environment that may change. A VLAN can provide additional security safeguards as well.
There are several ways of grouping devices into a VLAN. In our networks we only take into consideration:
- 802.1Q tagging: a 4 bytes 802.1Q header is added to the Ethernet frame. It contains the identifier of the VLAN to which the frame belongs.
- Port-based VLANS: if frames do not include a VLAN tag, the VLAN membership is determined by the configuration of the switch port to which the device is connected.

Physical layer variants

Ethernet can use different physical layers and media. To identify each implementation, a 3 fields notation is used:
<data rate> <modulation type> <additional distinction>

- The data rate, if only a number, is in Mb/s, and if suffixed by a "G", is in Gb/s.
- The modulation type (e.g., BASE or BROAD) indicates how encoded data is transmitted on the medium.
- The additional distinction identifies transmission or medium characteristics and, in some cases, the type of encoding (PCS) used. It contains one or several figures or letters or a combination of both. For instance:
  - "T" for twisted pair
  - "S" for short wavelength optics
  - "X" for a block PCS coding used for that speed of operation.

Although numerous implementations exist, we only mention here:

- 10BASE5 and 10BASE2 which are the well known legacy implementations using coaxial cables.
- 10BASE-T and 100BASE-TX which are the most common implementations using twisted pair cables.
- 10BASE-FL and 100BASE-FX which are the most common implementations using fiber optic cables.

As the modulation type is always BASE in modern networks, this field is often omitted (eg: 100-FX instead of 100BASE-FX).

DE80734

Field	Field size (in octets)	Cumulated field size (in octets)
Preamble	7	72...1530
Start-of-Frame delimiter	1	
MAC destination	6	
MAC source	6	
802.1Q header (optional)	4	64...1522
Ethertype/Length	2	
Payload (Data and padding)	46...1500	
CRC32	4	
Interframe gap	12	84...1542

Frame structure.

The Ethernet frame

Frame fields

■ The preamble and start-of-frame-delimiter (SFD) are required for hardware synchronization of network interfaces. They do not convey information and are not passed to the software.
■ The source and destination MAC addresses identify the sender and the receiver of the frame.
■ The optional 802.1Q header is used for VLAN tagging. It is no longer shown in this document unless specifically addressed.
■ Ethertype/length: see "Frame type" below.
■ The payload is the data field of the frame. Due to collision detection mechanisms, the length of the frame (excluding preamble and SFD) must be at least 64 octets. If necessary, the payload is padded with meaningless octets to reach that size. The maximum size for the payload is 1500 octets.
■ The CRC32 is used to check frame integrity.
■ Interframe gap: after a frame has been sent, transmitters are required to transmit 12 octets of idle characters before transmitting the next frame.

Frame type

Ethernet frames are of 2 kinds that are distinguished by the use of the Ethertype/length field:
■ The Ethernet II frame (second format defined by the DIX standard, hence the name). This frame uses the field as an Ethertype, describing the type of protocol conveyed by the payload.
■ The Ethernet 802.3 frame (defined later by the IEEE standard). This frame uses the field as the length of data.

Fortunately, Ethertype have been originally assigned values above 1500 making it easy to distinguish between both frame types:
■ Ethertype/length field ≤ 1500 Ethernet 802.3
■ Ethertype/length field > 1500 Ethernet II

IEEE 802.3 and Ethernet II can coexist on the same network.

MAC addressing

Address format

The Media Access Control (MAC) address is a unique identifier assigned to every network interface in a network. Ethernet MAC addresses are made of 48 bits that are represented in human-friendly form by 6 groups of 2 hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order,
e.g. `01-23-45-67-89-ab` or `01:23:45:67:89:ab`.

Address administration

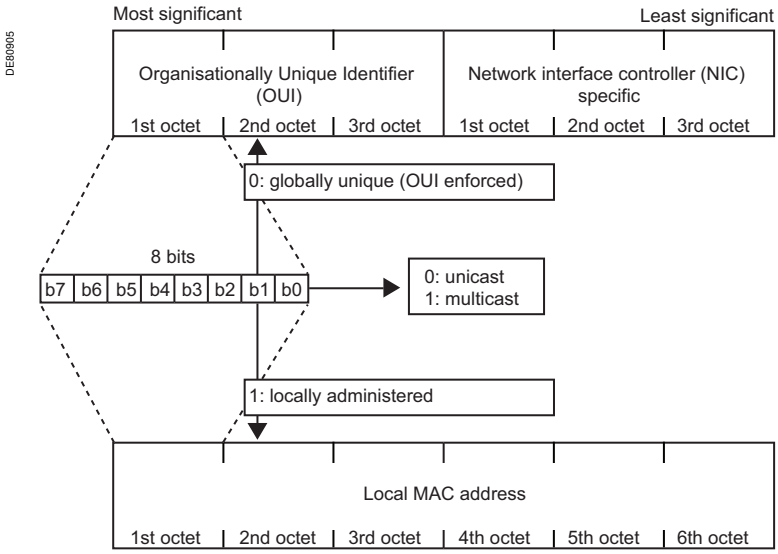
A MAC addresses can be:

■ A universally administered address is uniquely assigned to a device by its manufacturer. It is build of 2 parts:

□ The first 3 octets identify the device manufacturer and are known as the Organizationally Unique Identifier (OUI). The OUIs are managed by the IEEE Registration Authority.

□ The last 3 octets are assigned by the manufacturer with the only constraint of uniqueness.

■ A locally administered address is assigned to a device by a network administrator, generally overriding a universally administered address. This kind of address does not contain OUI.



MAC address structure.

Universally administered and locally administered addresses are distinguished by setting the second least significant bit of the most significant octet of the address. If the bit is 0, the address is universally administered. If it is 1, the address is locally administered. Consequently, this bit is 0 in all OUIs.

Unicast versus multicast

■ A unicast address represents a single network device, either source or destination of a frame.

■ A multicast address represents a collection of destination network device.

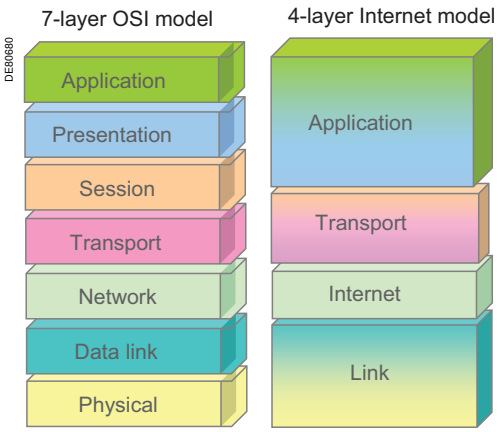
Unicast and multicast addresses are distinguished by setting the least significant bit of the most significant octet of the address. If the bit is 0, the address is unicast. If it is 1, the address is multicast. A special case of multicast address is the broadcast address where all the bits are set to 1: `FF:FF:FF:FF:FF:FF`. Frames sent to this broadcast address are received by all the devices on the network.

Note: *As each octet is transmitted starting with its least significant bit, this means that the unicast/multicast bit is the first transmitted bit of the address, immediately followed by the address type (local/universal).*

The Internet protocol suite
Overview

Introduction

The Internet Protocol Suite (commonly known as TCP/IP) is the set of communication protocols used for the Internet and other similar networks. It is named from 2 of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first 2 networking protocols defined in this standard.
The Internet protocol suite is described in a set of documents called RFCs that are maintained by the Internet Engineering Task Force (IETF).



Layer models.

The TCP/IP model

The Internet Protocol Suite, like many protocol suites, may be viewed as a set of layers. Each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the upper layer protocols based on using services from some lower layers.
However the TCP/IP model is different from the OSI model and consists of only 4 layers. From lowest to highest, these are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.

The link layer

This Layer encompasses the hardware specific interface methods. These methods, such as Ethernet, ISDN, DSL, FDDI or Wireless are however not part of the Internet Protocol Suite but are defined by other documents such as the IEEE 802.x series of standards.
It also includes specific protocols such as the Address Resolution Protocol (ARP) and its counterpart the Reverse Address Resolution protocol (RARP).

The Internet layer

The Internet layer is a group of methods, protocols, and specifications which are used to transport data packets (datagrams) from an originating node to a destination node, crossing network boundaries, if necessary.
The most important of them is the Internet Protocol (IP) which exists in version 4 (IPv4, the most common) and version 6 (IPv6).
The Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP) can also be found in this layer.

The Transport layer

2 main protocols belong to the transport layer:
- The Transmission Control Protocol (TCP) provides connection oriented transmissions that ensure reliable end-to-end data transfer. TCP takes care of packets acknowledgments, lost data retransmission and flow control.
- The User Datagram Protocol (UDP) is much simpler but also much more effective. It is used when exchange reliability is not a must or is ensured by the Application layer.

Transport layer end points inside the nodes are called ports. Ports are numbered from 1 to 65536. Some port numbers are reserved for specific application protocols, such as port 21 for FTP or port 80 for HTTP.

The Application layer

This layer contains all protocols and methods that are application related. Numerous protocols exist at this level, such as FTP, HTTP, SNMP, NTP, RSTP, POP, SMTP, DHCP, DNS, SOAP, Telnet, and many others.

IP addresses

The Internet Protocol requires that each device participating in the network has its own address: the IP address.
IP version 4 defines a 32 bits address scheme whereas IP version 6 defines a 128 bits one. IPv6 is expected to replace IPv4 due to its depletion of possible addresses. However, IPv4 is still the prevailing version today and the only one available with Sepam devices. For this reason we describe only this version.

IPv4 addresses

The 32 bits of the IPv4 address are usually and conveniently represented in dot-decimal notation (4 numbers, each ranging from 0 to 255, separated by dots, e.g. 139.25.1.166).

Address classes

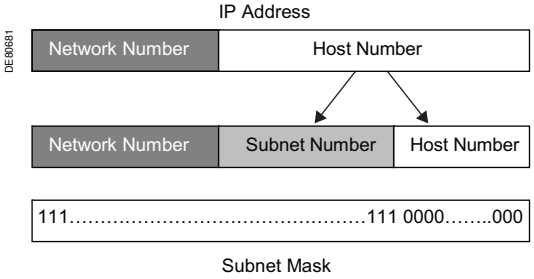
Historically, the IP address is interpreted as a 2-part value:
- The network number portion is made of the most significant bits of the address.
- The host number portion is made of the remaining bits.

5 address classes are defined, according to the size of each part or to special uses.

Class	Leading bits	Network number size	Host number size	First address	Last address
A	0	8	24	0.0.0.0	127.255.255.255
B	10	16	16	128.0.0.0	191.255.255.255
C	110	24	8	192.0.0.0	223.255.255.255
D	1110	N/A	N/A	224.0.0.0	239.255.255.255
E	1111	N/A	N/A	240.0.0.0	255.255.255.255

Class D addresses are IP multicast addresses.
Class E addresses are reserved.

Network numbers are allocated by the Internet Assigned Numbers Authority (IANA).



Classless addresses .

Subnetting

Address classes proved not scalable enough to meet the fast growth of Internet. They have been abandoned in favour of classless addresses based on variable length subnet masking as described below. However, this concept of classes still remains in some areas and should be kept in mind.

With subnetting, the previous host number portion of the address is further divided into:
- a subnet number, taken from the most significant bits
- a host number made of the remaining bits.

A subnet mask is used to determine the bits belonging to the network and subnet part on one side (1s in the corresponding mask bits) and the host number on the other side (0s in the corresponding mask bits).
The network number and subnet number play the same role and are often referred to globally as the network number. The length of this network number is sometimes indicated by a **`/n`** following the network address, such as 192.168.0.0/20.

Private addresses

IP addresses are normally uniquely assigned to a particular device. However, this has proved to be a real concern as private networks developed and public address space needed to be conserved.
3 ranges of IP addresses (one for each of the A, B, and C classes) are reserved for private networks (not directly connected to the Internet). These addresses are not routed on the Internet and thus their use need not be coordinated with an IP address registry.

Class	Network number size	First address	Last address
A	10.0.0.0/8	10.0.0.0	10.255.255.255
B	172.16.0.0/12	172.16.0.0	172.31.255.255
C	192.168.0.0/16	192.168.0.0	192.168.255.255

Private networks can themselves be subdivided into smaller subnets inside these address ranges (e.g. 192.168.0.0/24).

Routing

Devices that belong to different networks (subnets) cannot communicate directly. They must use interposing devices (routers) that will determine the best path to use for each transmitted frame. In order to communicate with other networks, each network must then have at least one router, poorly designated as the default gateway.
The sending device uses the subnet mask to determine if the frame must go to another subnet. When this is the case, the destination MAC address for that frame is not the MAC address of the final destination (which is not known) but the MAC address of the router.

The ARP protocol

IP addresses are logical addresses used for end-to-end communication over the Internet. They are however not understood by the physical layers such as Ethernet that require MAC addresses.
The Address Resolution Protocol (ARP) is used to obtain the MAC address associated with a given IP address. To do so, an ARP request is broadcasted on the network `who has the address a.b.c.d?`. If present, the device with IP address a.b.c.d replies, giving its MAC address.
ARP probes are also used by a starting device to test if the IP address assigned to it is already in use.

DHCP and BOOTP

IP addresses can be assigned to devices either statically or dynamically.
The Bootstrap Protocol (BOOTP, now obsolete) and the Dynamic Host Configuration Protocol (DHCP) are used to dynamically retrieve IP addresses and device configuration from a server.
These protocols are however not supported by Sepam devices for which only static IP addresses are allowed.

The DNS protocol

Using IP addresses can be quite cumbersome, especially for humans, and a more friendly naming system has been developed (e.g. www.schneider-electric.com). However, the IP protocol only uses the IP addresses, not the names. Consequently, each name must be converted to its corresponding address. This is the role of the Domain Name Service (DNS) which is build around a set of Domain name servers (databases) which provide the requested data through the DNS protocol.
The DNS protocol is not supported by Sepam devices.

The Internet protocol suite
Main application protocols

The Internet protocol suite comprises numerous application protocols. We only mention here those that can be used with Sepam devices.

The client-server model

Many application protocols are based on the client-server model. This model describes the relationship of cooperating programs in an application.
The server component provides a function or service to one or many clients, which initiate requests for such services. The server permanently listens to these incoming requests. Often clients and servers are located on separate hardware, but both client and server can also reside in the same system.

ICMP

The Internet Control Message Protocol (ICMP) is used to exchange service messages. It is not, strictly speaking, an application protocol (it really belongs to the network layer), however its best known use case is at the application level through the **`ping`** command. This command sends ICMP echo messages to test if given nodes are reachable.

FTP

The File Transfer Protocol (FTP) enables the transfer of files in both directions between a client and a server. It is mainly used for loading CID configuration files into the devices.

HTTP

The Hyper Text Transfer Protocol is the protocol used between a web browser and a web server. Sepam interfaces have an embedded website/web server.

SNMP

The Simple Network Management Protocol can be used to access management data contained in devices. This data is arranged as normalized structures called Module Information Bases (MIBs).
Sepam interfaces provide an SNMP agent and several MIBs.

SNTP

The Simple Network Time Protocol is used to distribute time among network devices. Sepam interfaces act as an SNTP client.

The Internet protocol suite
Dedicated protocols

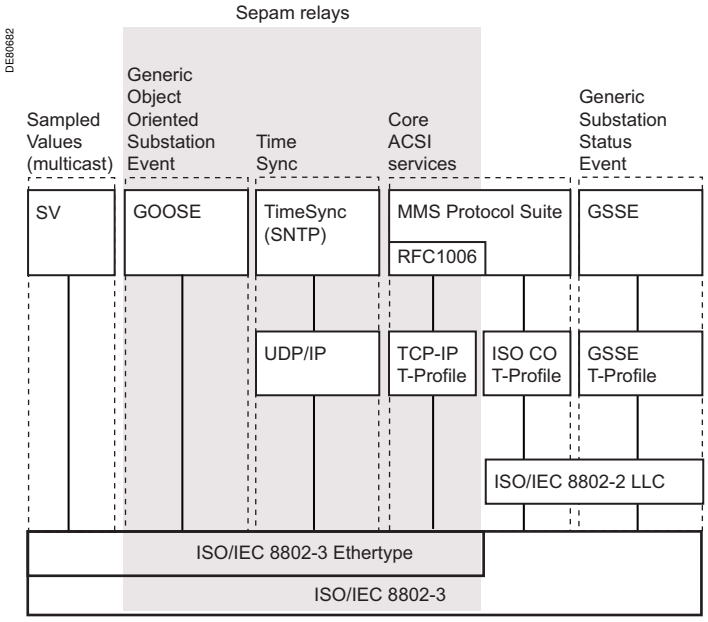
The following protocols are application protocols dedicated to industrial communication. They are not part of the Internet suite but are layered on top of it.

Modbus

Originally designed for the exchange of data between Programmable Logic Controller over a serial asynchronous communication channel, the Modbus protocol is now available on a variety of supports, including TCP/IP.
The protocol specifications are in the public domain. They are managed by the Modbus organization (www.modbus.org).

IEC 61850

The IEC 61850 protocol is intended for seamless communication inside substations. It is managed by the IEC (www.iec.ch).
The IEC 61850 communication services are purely virtual (Abstract Communication Services Interface - ACSI) and need to be mapped on a real world network. This mapping is presently only available on Ethernet and is described in part 8-1 of the IEC 61850 standard.



IEC 61850 mapping to Ethernet.

Client-server operation

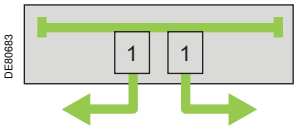
The client-server part of IEC 61850 is mapped to the Manufacturing Message Specification (MMS - ISO 9506). MMS is designed to operate on top of an ISO communication stack. In the case of a TCP/IP communication stack, an intervening `RFC1006` layer is used which replaces the missing layers.
The IEC 61850 standard allows using either the ISO or TCP/IP protocol stacks, Sepam relays use the TCP/IP one.

GOOSE operation

To allow for fast real-time communication, GOOSE messages do not make use of any protocol stack. GOOSE messages are directly encoded into an Ethernet frame. These messages are multicasted at MAC level.
GOOSE messages are only available on Sepam series 80 with ACE850.

Network architecture
Infrastructure components

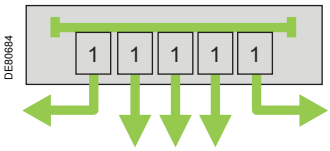
To achieve the desired network architecture, it is necessary to use a number of infrastructure components that have a precise role and behavior. The main components are described here.



Repeater.

Repeaters

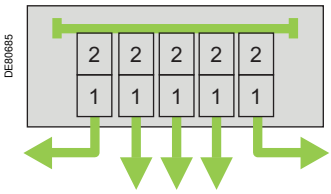
Repeaters are layer 1 devices that regenerate frames and enable an increase in the distance and the quantity of devices on a segment. They are inexpensive electronic devices with no embedded intelligence. Their usage is no longer appropriate.



Hub.

Hubs

Hubs, sometimes called multiport repeaters, are also layer 1 devices used to interconnect several devices in a star configuration and extend the network length. In general, hubs are plug-and-play devices that require no configuration. Hubs are transparent to other devices, they receive information through any of their ports and pass along that information to all of their other ports. A limited number of hubs can be cascaded.
Devices interconnected by hubs are in the same collision domain and must operate at the same speed.
Hubs are generally replaced today by switches, but some of them can still be found on networks. They may also be used temporarily to connect diagnostic equipment to a network.



Switch.

Switches

Switches are active components used to connect several devices in a star configuration but unlike hubs they operate at layer 2, thus providing many benefits:
- Every port and its associated device is a separate collision domain, enabling full-duplex operation, if the device is able to.
- Ports can operate at different speeds and use different media.
- An incoming packet is sent only to the relevant destination ports, which greatly alleviates network traffic.
- Switches can isolate traffic belonging to different virtual networks to improve security and availability.
- Switches can provide flow control.
- An unlimited number of switches can be cascaded to extend the length of the network.

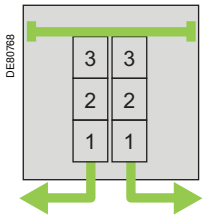
Switching technology

There are 2 types of switching, cut-through and store-and-forward:
- Cut-through switching begins to forward a packet when its first bytes are received, which can cause network disruption if the packet is corrupt.
- Store-and-forward switching waits for the entire packet to arrive and checks the packet for corruption before forwarding it to the correct port. It also allows for improved switching features. The time delay for the process is minimal, less than 1 ms on an industrial network.

Only store-and-forward switches are considered in this document as they are much more powerful and also the most widely used today.

Managed versus unmanaged

Unmanaged switches are not addressable and cannot be configured; therefore they offer only the basic switching capabilities described above.
Conversely, managed switches have their own IP address and can be configured using SNMP or private interfaces and offer many other features:
- isolation of traffic belonging to different virtual networks to improve security and availability
- flow control and rate limiting
- topology management
- advanced diagnostics capabilities.



Router.

Bridges

Bridges are devices used to connect multiple network segments at the data link layer (layer 2). In Ethernet networks, the term bridge refers to devices that behave according to the IEEE 802.1D standard. In this context, the words bridge and switch are often used interchangeably.

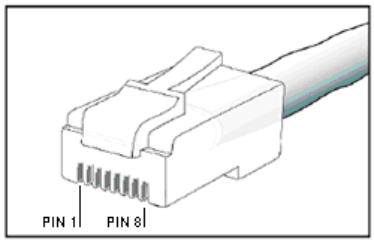
Routers

Routers are layer 3 devices used to interconnect several separate networks using the same upper layers.
A typical use of a router is to interconnect IP subnetworks. It is then often (and inappropriately) called a gateway.
They create or maintain a table of the available networks and use this information to determine the best route for a given data packet from the source network to the destination network.
Routers can be used to break up broadcast domains.

Firewalls

A firewall is a network component that is designed to block unauthorized access while permitting authorized communications. It operates at level 3 or higher.
A firewall can be implemented in either hardware or software, or a combination of both. It inspects network traffic passing through it, and denies or permits passage based on a set of rules.
It is normally placed between a protected network and an unprotected network and acts like a gate to ensure that nothing private goes out and nothing malicious comes in.

DE80686



RJ45 plug.

Copper Cabling

Twisted pair cables

The modern copper implementations of Ethernet use twisted pair cables, and most often the Unshielded Twisted Pair (UTP). Twisted pair cabling is a common form of wiring in which 2 conductors are wound around each other to cancel electromagnetic interference (crosstalk).

Cables categories

LAN cables are identified with a category rating. The American National Standards Institute/Electronic Industries Association (ANSI/EIA) standard 568 is one of several standards that specify categories of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain effectively. The specifications describe the cable material and the types of connectors needed to conform to a category.

Standard	Cable	Connector	Max cable length	
			Half-Duplex	Full-Duplex
10BASE-T	UTP Cat 3 or better (2 pairs used)	RJ45	100 m (328 ft)	100 m (328 ft)
100BASE-TX	UTP Cat 5 or better (2 pairs used)	RJ45	100 m (328 ft)	100 m (328 ft)

Straight and crossover cables

Ethernet cables route transmitted signals from one device to another. Depending on these devices, 2 types of cable are used:

- Straight cables (drop cables) connect an end device to an infrastructure device.
- Crossover cables are installed between 2 end devices that communicate with each other directly, or between 2 infrastructure devices.

These cables differ in the way individual wires are connected to the RJ45 plugs. The following schematics apply to the widely used EIA/TIA 568B cables.

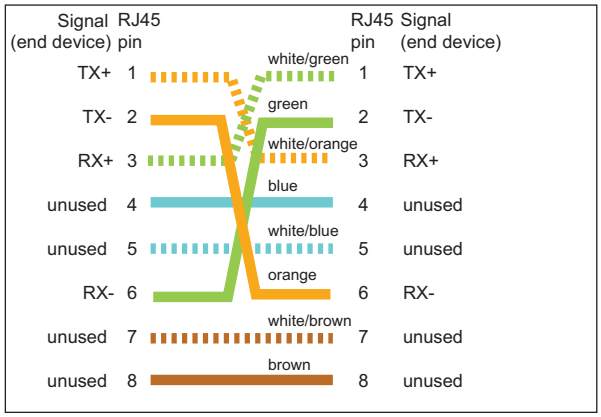
DE80687

Category 5e UTP Ethernet cable.

DE80688

Straight cable (otherwise called patch cable).

DE80689



Crossover cable.

***Note:** This crossover cable layout is not suitable for 1000Base-T operation (all 4 pairs should be crossed).*

MDI/MDI-X

Today most of the devices offered on the market support the medium dependent interface MDI/MDI-X functionality in their Ethernet ports. This functionality allows the auto-switching of transmit and receive wire pairs. To connect this type of device, use either straight or crossover cable; the device senses and accommodates the TX/RX pairs.

Fiber optic cabling

Fiber optic cable has the ability to transmit signals over longer distances and at faster speeds than copper cable. Also, because fiber optic cable transmits light, it does not present the problems of electromagnetic interference associated with copper cabling. It is ideal for harsh environments and outside connections due to its high immunity to moisture, as well as to lightning.

Parts of a fiber cable

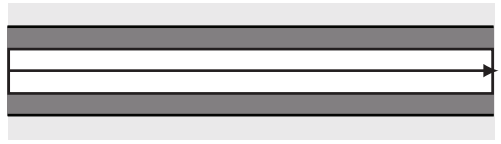
Typically, a fiber optic cable consists of 3 parts:
- core: thin ultra-pure glass (silica) or plastic center of the fiber that transmits light
- cladding: outer optical material that surrounds the core and reflects light back into the core
- buffer jacket: outer plastic jacket or coating that protects the fiber from damage and moisture.

A light signal can propagate through the core of a fiber along a single path (called single-mode fiber) or multiple paths (called multimode fiber).

Single-mode fibers

Single-mode fiber has a small core diameter (about 9 µm) and transmits infrared laser light (wavelength = 1300 to 1550 nm). It provides only one optical mode that forces light along a linear path through the cable end and causing much lower dispersion and attenuation than multimode.
Single mode fiber is more expensive and harder to handle. It is only used when its significantly highest bandwidth and distance ratings are of interest.

DE80691



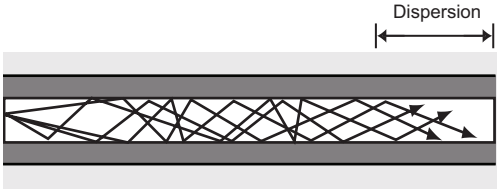
Single mode.

Multimode fibers

There are 2 types of multimode cable:
- Step-index: has an abrupt change between core and cladding. It is limited to about 50Mb/s.
- Graded-index: has a gradual change between core and cladding. It is limited to 1Gb/s.

When cable is graded, the amount of refraction is reduced gradually outward from the core. Because light travels faster when refraction is lower, light travelling through the outer material travels faster than light at the center of the core. The propagation dispersion is then reduced.

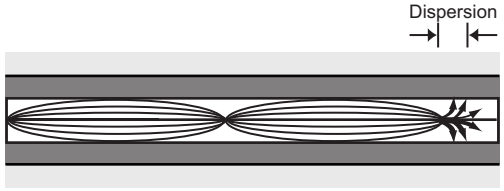
DE80690



Step index multimode.

Multimode fiber has a large core diameter (typically 50, 62.5 or 100 µm) and transmits infrared light (wavelength = 850 to 1300 nm) from light-emitting diodes (LEDs). The cladding diameter is usually 125 µm.
Fiber size is commonly indicated by the core diameter followed by a slash and the cladding diameter, without units (eg: 62.5/125).

DE80793



Graded index multimode.

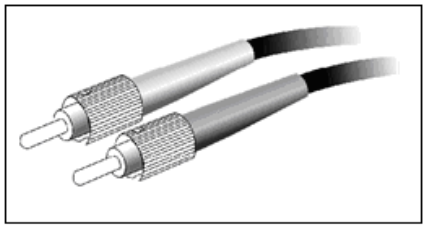
The following table synthesizes some of the most common optical standards.

Standard	Cable type	Wawelength (nm) min - max (typical)	Preferred connector	Minimum range
10BASE-FL	MM 62.5/125 or MM 50/125	770-860 (850)	ST	2000 m (6550 ft)
100BASE-FX	MM 62.5/125 or MM 50/125	1270-1355 (1300)	SC	2000 m (6550 ft)
1000BASE-SX	MM 62.5/125 or MM 50/125	770-860 (850)	SC	220 m (720 ft)
1000BASE-LX	MM 62.5/125 or MM 50/125	1270-1355 (1300)	SC	550 m (1800 ft)
1000BASE-LX	SM 9/125 or SM 8/125	1270-1355 (1310)	SC	5000 m (16400 ft)

The real range of a fiber optic link can deviate considerably from the typical values indicated in the table:
- It can be higher, depending on the devices transmit and receive characteristics
- It can also be shorter, due to poor fiber quality or cabling losses (mainly due to bending and intervening connections).

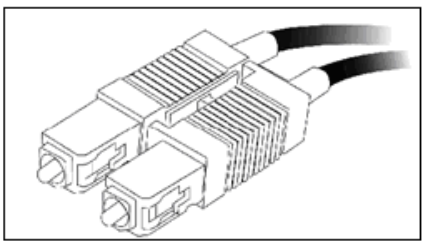
A precise optical budget calculation should be made in every case, unless the distance is very short.

DE80692



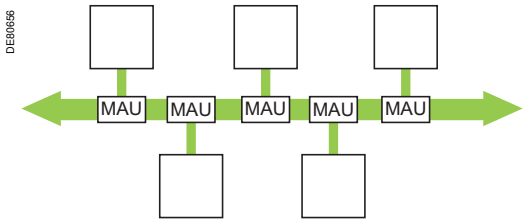
ST connector.

DE80693



SC connector.

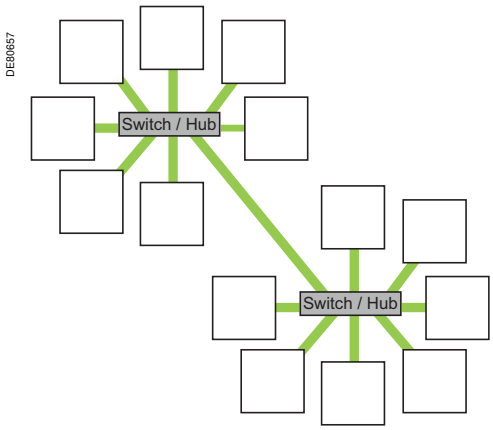
Network architecture
Network topologies



Bus topology.

Bus topology

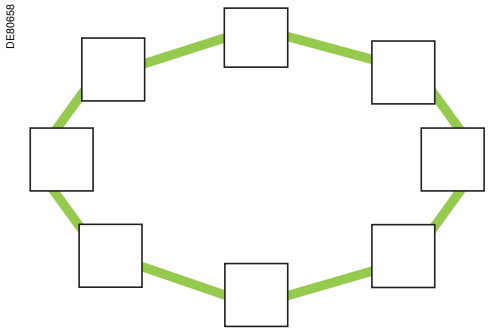
This is the historical topology which is no longer used today.
A single backbone cable connects all the devices on the network. Terminators are placed at each end of the backbone to allow signals to be sent and cleared over the network.
Devices are directly connected to the medium through a Medium Attachment Unit (MAU), sometimes reduced to a simple T-connector.
A section of backbone cable is known as a segment. Several segments can be connected using bridges or repeaters.



Star topology.

Star topology

In a star topology, all the devices are connected through a central device that can be a hub or a switch.
A star topology is a common network layout for office environments and sometimes also for industrial environments.
The use of switches rather than hubs brings a very high performance level.



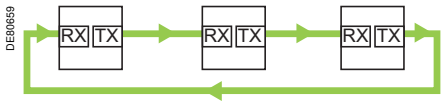
Ring topology.

Ring topology

In a ring topology, all devices or network infrastructure components are connected to form a ring. Packets travel on the ring being passed from one device to the next until the destination is reached. Two variants are possible.

Simple ring

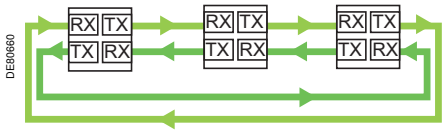
This solution is only practical with fiber optics media. The transmitter part of the Ethernet port of one device is connected to the receiver part of the next device in the loop. The only advantage here is the low cost, opposed to the lack of availability (any break in a link disables the whole ring).



Simple ring.

Dual or redundant ring

This solution requires that each device has 2 Ethernet ports. It is therefore mainly used with switches. It has the major advantage of offering a redundant path to the frames. If one of the links is broken, every device in the ring can still be reached through the remaining link.

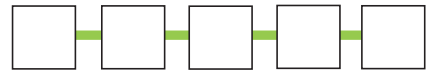


Dual or redundant ring.

Rings require the use of topology management (See Spanning Tree Protocol).

Network architecture
Network topologies

DE80661



Line topology.

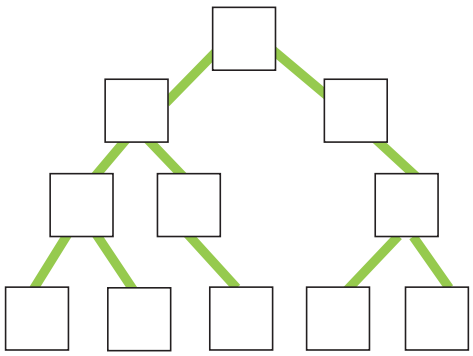
Line topology (daisy chain)

This topology is a non closed dual ring. It requires dual ported devices but does not offer the redundant path. It is mainly intended to reduce costs.

DE80662

Daisy chain.

DE80663

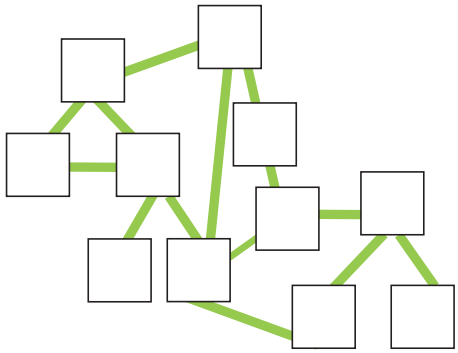


Tree topology.

Tree topology

A tree topology is a topology in which there is a single path between any 2 devices.

DE80664



Mesh topology.

Mesh topology

Real networks are often a mix of the previously described topologies. The result is a mesh topology where each device has a connection to one or more other components of the network.
In a full mesh network, each device is directly connected to every other device in the mesh.
Mesh networks offer redundant data paths and increase availability. They require the use of topology management (See Spanning Tree Protocol).
Mesh topologies are generally created intentionally, to benefit from the improved availability (in network backbones for instance). They are also sometimes created involuntarily as a result of unmastered growth in large networks.

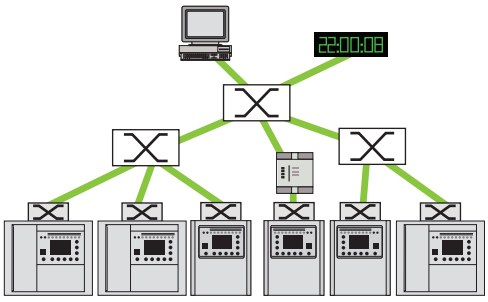
Network architecture
Recommended architectures

The architectures described here are typical use cases of substation networks. They are provided only as examples and other architectures can be used, if more appropriate.

Non redundant architectures

The following architectures offer no redundancy. They should apply only when no GOOSE messaging is used. These are typical architectures when Sepam devices are connected with ECI850.

DE80694

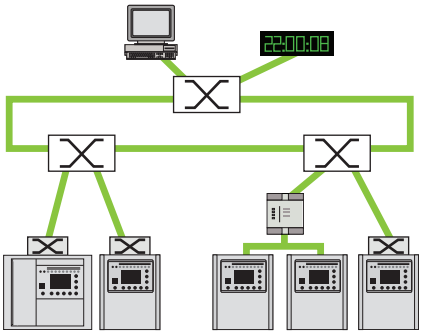


Star architecture.

Star architecture

In this architecture, one or several levels of switches are connected in a star fashion. Each end device is connected to only one main switch through a single link.

DE80695



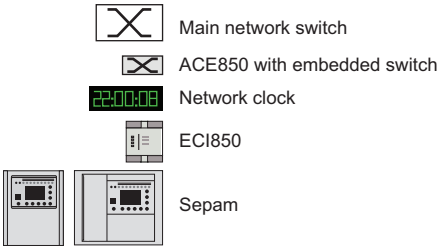
Mixed ring and star architecture.

Mixed ring and star architecture

In this architecture, a ring backbone connects main switches. Devices are connected to this backbone through a single link.

Legend of the architectures

DE80696



Network architecture
Recommended architectures

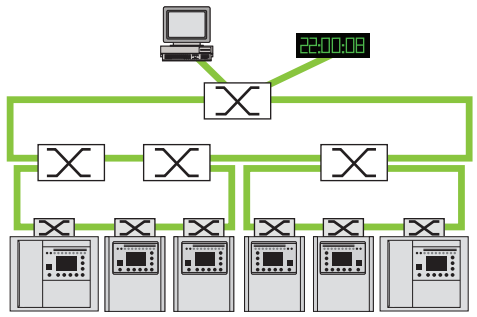
Redundant architectures

The following architectures offer some level of redundancy. They are the preferred architectures when GOOSE messaging is used.

Ring and sub-rings architecture

In this architecture, a backbone ring is used to connect sub-rings. These sub-rings are created by linking the devices.
Each sub-ring is tolerant to one link failure.
The right sub-ring ends are connected to the same main switch and no fault-tolerance exists in case of a failure on this switch.
The left sub-ring ends are connected to different main switches which also provides tolerance to a fault on the backbone ring.

DE80697

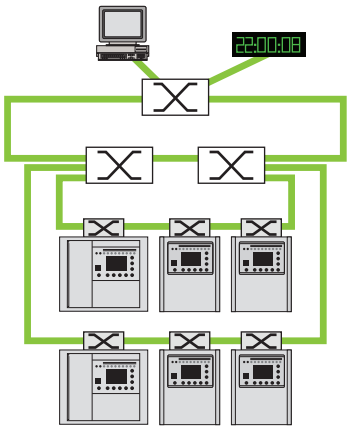


Ring and sub-rings architecture.

Ring and multiple sub-rings architecture

This is a generalization of the previous architecture with multiple sub-rings attached to the same main switches.
This architecture is a good compromise between cost and performance.

DE80698

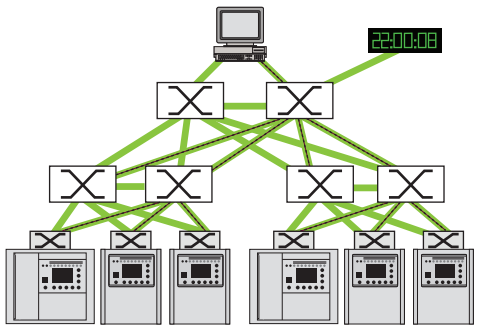


Ring and multiple sub-rings architecture.

Dual homing

This architecture is a mesh topology in which every device is connected to at least 2 other nodes providing independent communication paths (alternate paths are shown with black-dotted lines in the illustration opposite).
It offers one of the best fault tolerant solutions but requires an important increase in the number of switches and therefore in the cost.

DE80699



Dual homing.

Recommended switches

A smooth operation of the network requires the use of store and forward, managed switches. These switches should be compliant to IEC 61850-3 regarding their environmental withstanding.
Sepam devices have been tested with the following switches which are therefore recommended.
The configuration examples found later in this document are based on the RSG2100 switch.

DE80700

RSG2100 switch.

RuggedCom™ RSG2100

The RSG2100 is a 19" rack mountable managed Ethernet switch with up to 19 ports. The modular architecture offers 100BaseFX /1000BaseX fiber and 10/100/1000BaseTX copper port combinations. Fiber ports can be fitted with multimode or single mode optical transceivers.

DE80701

RS900 switches.

RuggedCom™ RS900

The RS900 is a managed Ethernet switch with up to 9 ports: 6 Base 10/100BaseTX ports with option for 3 additional Fiber or Copper ports. Fiber ports can be fitted with multimode or single mode optical transceivers.

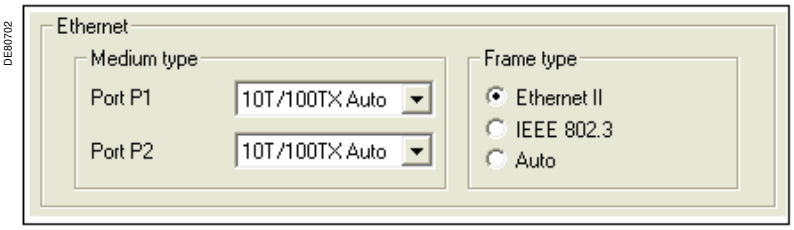
Before connecting devices to the network, their network configuration (Ethernet and IP) must be set. Details of this configuration are provided in the corresponding device manual. The main points are summarized here.

Network configuration on ACE850

This configuration is done using the SFT2841 setting software. The initial configuration must be done using the Sepam front face connection of SFT2841. Subsequent modifications can be done via a remote connection.

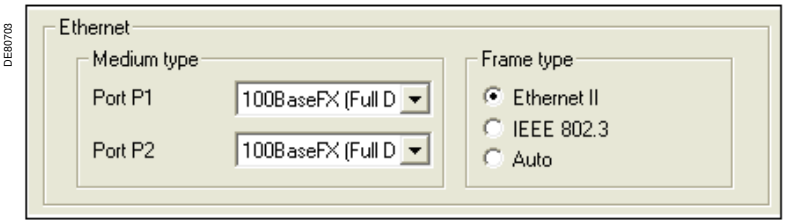
ACE850-TP Ethernet configuration

The default Ethernet configuration should be kept whenever possible. It provides more flexibility and better performance.



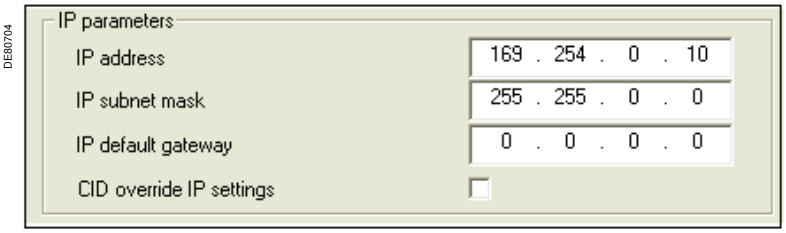
ACE850-FO Ethernet configuration

The default Ethernet configuration should be kept whenever possible. It provides better performance.



ACE850 IP configuration

Assign IP parameters according to your IP addressing scheme.



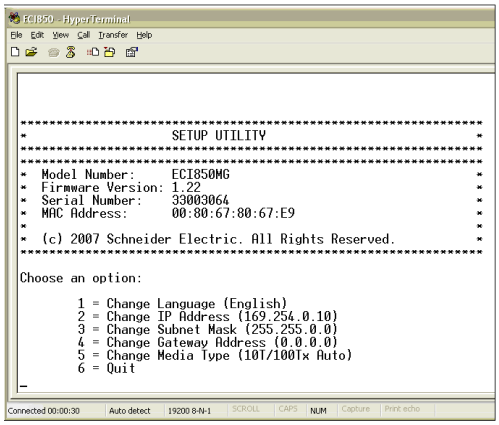
Note: *If the IP address is changed through a remote connection of SFT2841, the connection is then lost and needs to be restored using the new address.*

Network configuration on ECI850

This configuration is done through the web interface of the ECI850. If the default IP address cannot be used, the initial configuration can be done through the serial interface.
The default Ethernet configuration, which enables greater flexibility and better performance, should be kept whenever possible.

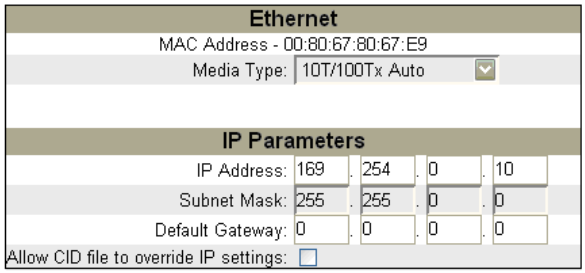
***Note:** If the IP address is changed through the web interface, the connection with ECI850 is lost and needs to be re-established using the new address.*

DE80705



ECI850 serial interface for setup.

DE80707



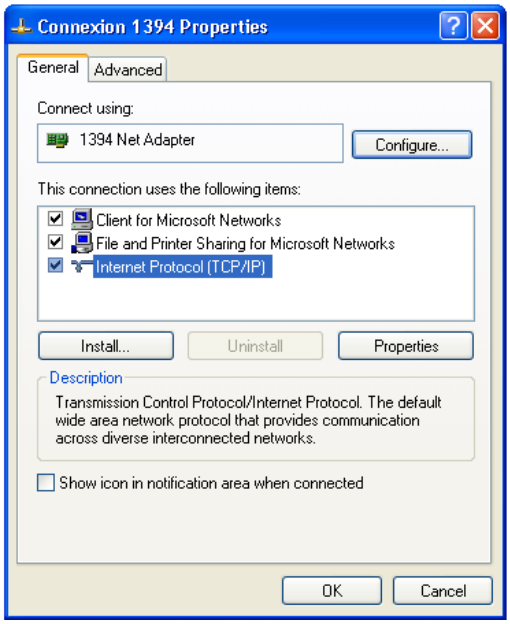
ECI850 web interface - Ethernet and IP parameters.

Network configuration on a PC

Unless a DHCP server is present on the network, the Ethernet connection uses static IP parameters. To set up this Ethernet connection:
1. From the **Network Connections** window, select the desired network interface and select **Properties** from the contextual menu.
2. In the **Connection Properties** window displayed, select the **Internet Protocol (TCP/IP)** item from the item list and click **Properties**.
3. In the **Internet Protocol (TCP/IP) Properties** window displayed, configure the IP parameters values in the relevant fields. DNS servers are not required and the fields can be left empty.
4. Close all the windows by successively clicking **OK**.

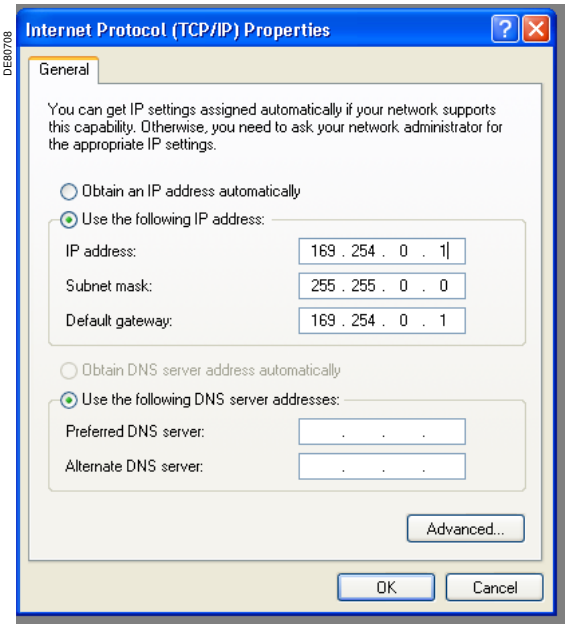
There are many types and versions of operating systems on PCs. The examples shown in this guide are based on Windows XP SP2.

DE80706



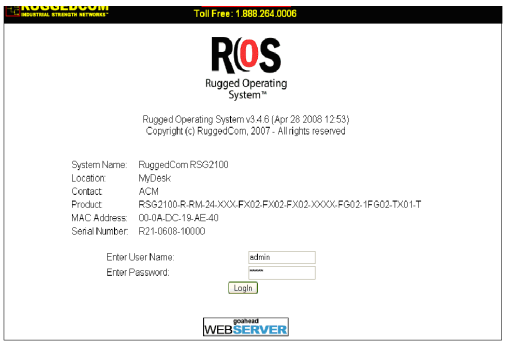
Connection Properties window.

DE80708



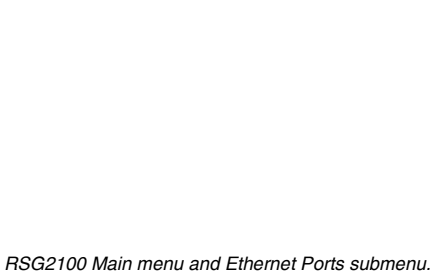
Internet Protocol (TCP/IP) Properties window.

DE80709



RSG2100 Home page.

DE80710



RSG2100 Main menu and Ethernet Ports submenu.

Network configuration on RuggedCom™ switches

Connecting to RuggedCom™ switches

RuggedCom™ switches configuration and diagnostic can be performed through the console serial link or through the embedded web interface.
The switch default parameters are:

- default IP address: **192.168.0.1**
- default account: **admin**
- default password: **admin**

Configuring switch ports

The switch ports default configuration, which enables greater flexibility and better performance, should be kept whenever possible. Therefore, the switch ports do not require initial configuration for network operation. If for some reason you need to modify the default configuration, proceed as follows.

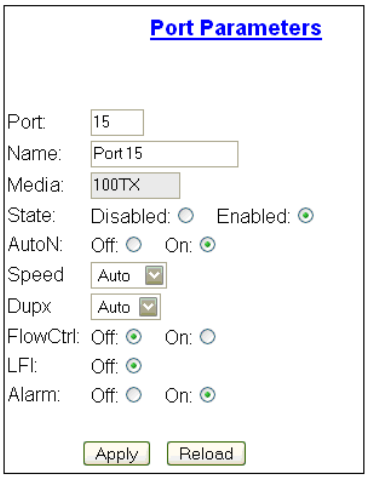
1. From the **Ethernet Ports** submenu, select the **Configure Port Parameters** to display the **Port Parameters** summary.
2. Select the desired port by clicking the port number to display the **Port Parameters** window. 2 examples of **Port Parameters** are provided below. One applies to copper-type ports, the other to fiber-type ports.

DE80711

Port	Name	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm
1	Port 1	100FX	Enabled	Off	100M	Full	Off	Off	On
2	Port 2	100FX	Enabled	Off	100M	Full	Off	Off	On
3	Port 3	100FX	Enabled	Off	100M	Full	Off	Off	On
4	Port 4	100FX	Enabled	Off	100M	Full	Off	Off	On
5	Port 5	100FX	Enabled	Off	100M	Full	Off	Off	On
7	Port 7	100FX	Enabled	Off	100M	Full	Off	Off	On
9	Port 9	1000X	Enabled	On	1G	Full	Off	Off	On
10	Port 10	1000X	Enabled	On	1G	Full	Off	Off	On
11	Port 11	1000X	Enabled	On	1G	Full	Off	Off	On
13	Port 13	100TX	Enabled	On	Auto	Auto	Off	Off	On
14	Port 14	100TX	Enabled	On	Auto	Auto	Off	Off	On
15	Port 15	100TX	Enabled	On	Auto	Auto	Off	Off	On
16	Port 16	100TX	Enabled	On	Auto	Auto	Off	Off	On

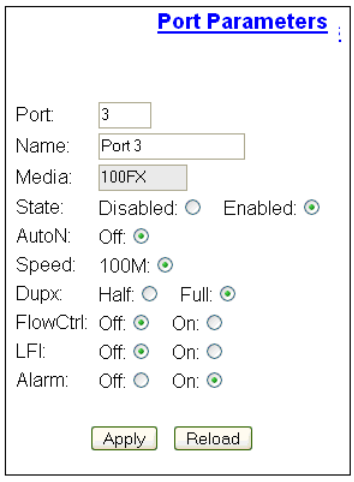
Port parameters summary.

DE80712



Port parameters for copper ports.

DE80713



Port parameters for fiber ports.

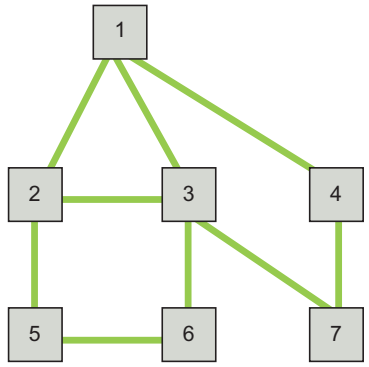
Network operation
The Spanning Tree Protocol

Loops and storms

Ring and mesh topologies create physical network loops. Such loops are prone to a phenomenon called broadcast storm: multicasted and broadcasted frames are forwarded by switches out of every port, they propagate endlessly on these loops and rapidly flood the network, inhibiting its normal operation.
Several solutions exist to overcome this situation. The most common and standardized one is the Spanning Tree Protocol.

Note: *Most of the other solutions available apply only to ring topologies and not to meshed ones.*

DE80714



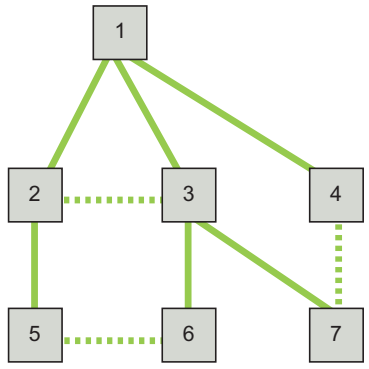
A meshed network.

Spanning tree protocol versions

There are several versions of the Spanning Tree Protocol (STP):
- The original version of STP is contained in IEEE 802.1D 1990. This protocol is relatively slow and takes several minutes to reconfigure a network.
- A faster version known as the Rapid Spanning Tree Protocol (RSTP) was issued in 802.1w 1998.
- An improved version of RSTP, with the original STP removed, was introduced in 802.1D 2004.
- eRSTP is a RuggedCom ® proprietary improved implementation of 802.1w with performance similar to 802.1D 2004.

All these versions are compatible and devices compliant to different versions can be mixed. However, the high level of performance required for a substation is only obtained by using the 802.1D 2004 version of RSTP that is implemented in Sepam relays (ACE850) and RuggedCom ® switches (eRSTP).

DE80715



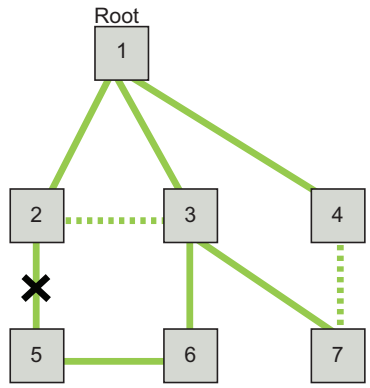
Equivalent spanning tree (blocked links shown as dotted lines).

Spanning tree principles and definitions

The principle is to convert a physically meshed network topology into a logical tree topology by breaking the loops. Bridges collectively compute a spanning tree [(1)], using the Spanning Tree Protocol to exchange the relevant information between them.
This spanning tree is obtained by blocking some of the redundant links. In case of a failure, a new spanning tree is computed and links are blocked or unblocked accordingly.
The resulting spanning tree topology can be adjusted by changing some of the configuration parameters.

[(1)] *In the mathematical field of graph theory, a spanning tree of a connected graph G can be defined as a maximal set of edges of G that contains no cycle, or as a minimal set of edges that connects all vertices.*

DE80716



Spanning tree reconfiguration after the link between nodes 2 and 5 has been broken.

Protocol operation

The spanning-tree calculation occurs when the bridge is powered up and whenever a topology change is detected. It comprises the following steps:

Selecting the root bridge
Every spanning tree must have a root bridge which is the bridge with the lowest Bridge Identifier in the network. The root bridge is selected first for each network reconfiguration, through the exchange of Bridge Protocol Data Units (BPDUs).

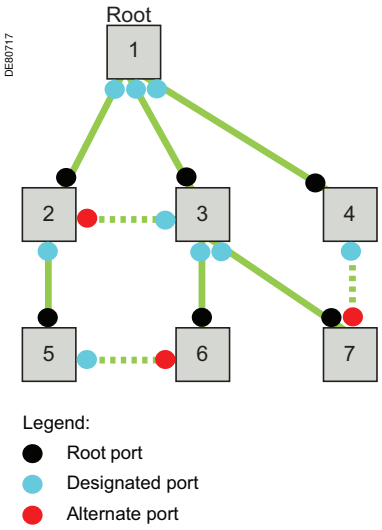
Note: *The bridge identifier is made of the bridge priority (see parameters) and the bridge MAC address.*

Determining the root port
After the root bridge has been chosen, each bridge determines the cost of each possible path from itself to the root. From these, it picks the one with the lowest cost (the least-cost path). The port connecting to that path becomes the root port of the bridge.

Determining the designated ports
The bridges on a network segment collectively determine which bridge has the least-cost path from the network segment to the root. The port connecting this bridge to the network segment becomes the designated port for the segment.

Disabling other ports
Any active port that is not a root port or a designated port is a blocked port.

Network operation
The Spanning Tree Protocol



Ports roles.

Port roles and states

RSTP assigns to every port of a bridge one of the following roles:
- Root port: a port that provides the lowest cost path from that bridge to the root bridge.
- Designated port: a port attached to a segment, that provides the lowest cost path from that segment to the Root.
- Alternate port: a port that offers an alternate path from that bridge to the root bridge, if the current root port is no longer usable.
- Backup port: a port that acts as a backup for the path provided by a Designated Port in the direction of the leaves of the Spanning Tree. Backup ports only exist when 2 bridge ports are connected together in loopback by a point-to-point link, or where the bridge has 2 or more connections to a shared media segment.
- Disabled port: a port that is administratively excluded from the spanning tree.

Alternate Ports and Backup Ports can provide connectivity if other network components fail.

Each port also has states, which for RSTP are:
- Discarding: the port ignores all incoming frames and does not transmit any frames, except BPDUs. Disabled, Alternate, and Backup ports are discarding.
- Learning: the port examines incoming frames to learn their source address but does not transmit any outgoing frames.
- Forwarding: the port transmits normally incoming and outgoing frames.

Note: *STP used additional port states. These states (disabled, blocking, listening, and broken) all correspond to the RSTP discarding port state.*

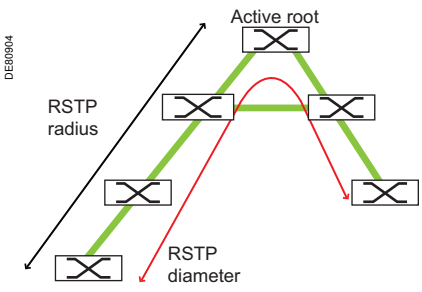
Bridge Protocol Data Units (BPDUs)

The spanning tree protocol makes use of dedicated frames called Bridge Protocol Data Units (BPDUs) to exchange information between bridges.

BPDUs are exchanged regularly (every 2 seconds by default) and when a topology change occurs.

BPDUs are sent with the port's own MAC address as source address and a reserved STP multicast address as the destination address (01:80:C2:00:00:00).
There are 3 kinds of BPDUs:
- Configuration BPDU (CBPDU), used for Spanning Tree computation, when in STP compatibility mode.
- Topology Change Notification (TCN) BPDU, used to announce changes in the network topology when in STP compatibility mode.
- RSTP BPDU used for all purposes in RSTP mode.

BPDUs contain the following information:
- identifier of the bridge that is presumed to be the root (root identifier)
- distance from the sending bridge to the root bridge (root path cost)
- bridge and port identifiers of the sending bridge
- age of information contained in the configuration message.



RSTP radius and diameter.

RSTP radius and diameter

The RSTP radius is the number of bridges from the active root bridge to the bridge that is the farthest away from this active root in the topology, at a given time.
When the network topology changes, the RSTP radius may also change. The RSTP diameter is the maximum value of the RSTP radius among all the possible topologies. As the root bridge can, in theory, be any bridge in the network, the RSTP diameter is sometimes defined as the maximum number of bridges between any 2 points of attachment of end stations.
However, by carefully configuring the bridges, the root bridge location can be restricted to a predefined area, to enable the network to be larger than the RSTP diameter.
For correct RSTP operation, the **Max Age time** parameter must be set to a value greater than the RSTP diameter (see next section).

Spanning tree parameters

Spanning tree protocol parameters

The following parameters are used when configuring the RSTP protocol. Most of them are identical to previous STP parameters, otherwise compatibility means are provided. Depending on the device implementation, some of these parameters can have fixed values and are not shown on configuration interfaces.

- Bridge priority: the bridge with the lowest priority becomes the root bridge. In case of equal priority, the bridge MAC address is also used. Choosing appropriate bridge priorities enables the control of the path of traffic flows under normal and abnormal conditions.
- Port cost: this parameter is used in cost calculations that determine the best path to the root bridge. The port cost is usually obtained automatically from the link speed.
- Port priority: this parameter is used to choose between ports with equal cost that attach to the same segment.
- Hello time: the interval between periodic transmission of configuration messages by the root bridge. This value is normally fixed at 2 seconds. It can be changed to 1 second for STP compatibility.
- Forward delay time: the amount of time a bridge spends learning MAC addresses on a port before it transitions to forwarding. This parameter is only used in STP compatibility mode.
- Max age time: the time during which a configuration message remains valid after being issued by the root bridge. Although expressed as a number of seconds, this value is in fact a number of hops and determines the maximum size of the RSTP network, also called RSTP diameter.
- Max transmit count: maximum number of BPDU messages that can be sent on a port, before the rate is limited to 1 message per second.
- Cost style: RSTP uses 32 bits cost values whereas STP only uses 16 bits values. Use STP style in mixed configurations.

Spanning tree administrative parameters

It is possible to manually define the following parameters in some implementations, which are otherwise determined automatically:

- Edge port: edge ports do not participate in the Spanning Tree. They transition directly to the forwarding state without learning delays.
- Point to Point: point to point links transition quickly to the forwarding state.

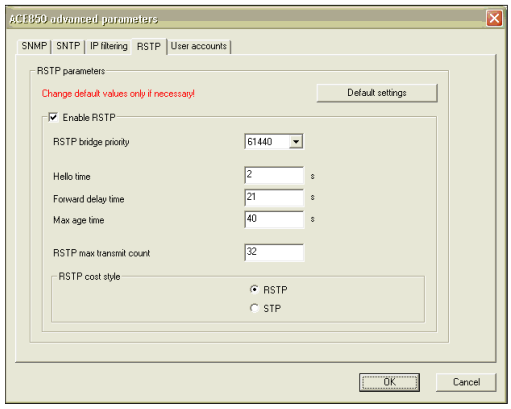
RSTP configuration on ACE850

RSTP parameters on ACE850 have a default configuration which should be kept in normal conditions.

The **RSTP bridge priority** is set higher than the IEEE 802.1 recommended default value to prevent an ACE850 from becoming a root switch, which is not recommended in standard topologies (the root switch should be located on the main ring).

The **Max age time** is set to the maximum allowed value and therefore allows for the largest possible diameter. This parameter can be adjusted to improve performance (see guidelines later in this chapter).

DE80718



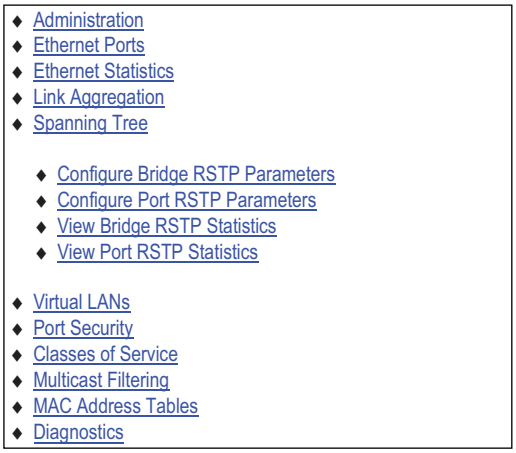
ACE850 advanced parameters - RSTP parameters.

RSTP configuration on RuggedCom™ switches

Bridge RSTP parameters

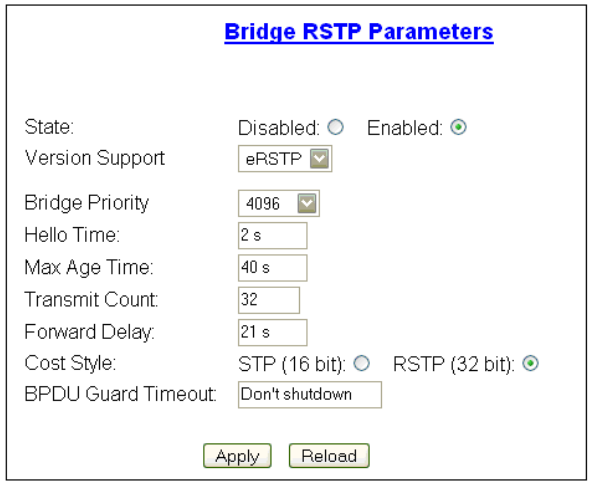
From the **Spanning Tree** submenu, select **Configure Bridge RSTP Parameters** to display the corresponding window.
Unless there are special requirements, the parameters should be set as shown below to ensure that the root switch is located in the main ring and allow for the maximum diameter.

DE80719



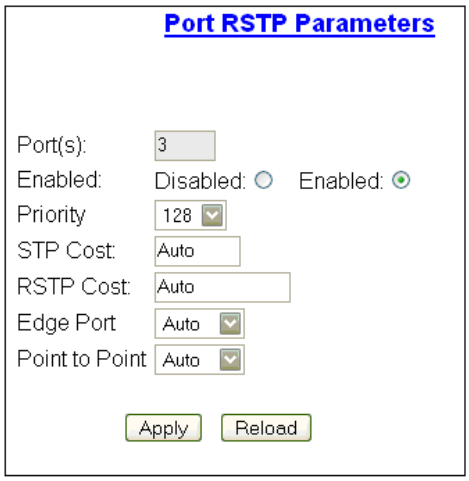
RSG2100 Main menu and Spanning Tree submenu.

DE80720



Bridge RSTP Parameters.

DE80722



Port RSTP Parameters.

Port parameters

From the **Spanning Tree** submenu, select **Configure Port RSTP Parameters** to display the configured **Port RSTP parameters** list. To modify a specific port configuration, click the desired port number. However, it is recommended to keep the default configuration values.

DE80721

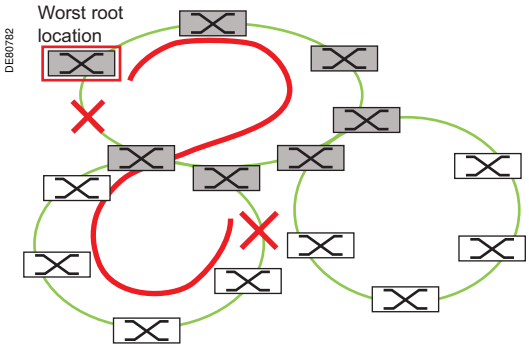
Port(s)	Enabled	Priority	STP Cost	RSTP Cost	Edge Port	Point to Point
1	Enabled	128	Auto	Auto	Auto	Auto
2	Enabled	128	Auto	Auto	Auto	Auto
3	Enabled	128	Auto	Auto	Auto	Auto
4	Enabled	128	Auto	Auto	Auto	Auto
5	Enabled	128	Auto	Auto	Auto	Auto
7	Enabled	128	Auto	Auto	Auto	Auto
9	Enabled	128	Auto	Auto	Auto	Auto
10	Enabled	128	Auto	Auto	Auto	Auto
11	Enabled	128	Auto	Auto	Auto	Auto
13	Enabled	128	Auto	Auto	Auto	Auto
14	Enabled	128	Auto	Auto	Auto	Auto
15	Enabled	128	Auto	Auto	Auto	Auto
16	Enabled	128	Auto	Auto	Auto	Auto

Port RSTP Parameters summary.

Guidelines for using RSTP in ring architectures

Root bridge location

RSTP performance can be dramatically affected by the time required to elect the root bridge. To obtain the best results, the root bridge must be located on the main ring with an alternate root bridge candidate on this same ring in case the root bridge fails. The switch chosen to be the bridge must have its priority set to 4196. The alternate root must be located at the opposite side of the ring and have its priority set to 8192. Other switches on the main ring must keep their default priority of 32768.



RSTP diameter determination.

Maximum number of switches

In a 2 level ring architecture, such as the one shown on the left, the RSTP diameter can be computed as:

DRSTP = Nmain + Nsub_max , DRSTP ⩽ 40

Where:

- DRSTP is the RSTP diameter
- Nmain is the number of switches on the main ring
- Nsub_max is the number of switches on the longer sub-ring

This formula applies only if the root switch is located on the main ring.

By knowing the number of switches on the main ring, the maximum number of switches on any sub-ring can be computed as:

Nsub_max ⩽ 40 - Nmain

It is recommended to keep the number of switches below the maximum value. RSTP performance is better if rings are kept short. For example, it is better to use 3 sub-rings of 10 devices than 2 sub-rings of 15 devices.

Max Age Time parameter

This parameter must be greater than the network diameter. Its maximum value is 40, which is also the default value in the ACE850. The default value in switches is usually 20.

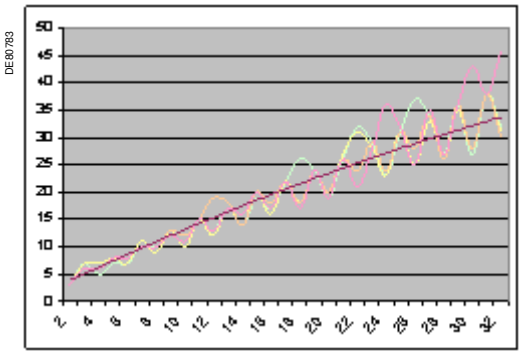
To improve performance, this parameter must be as small as possible by setting it to the value of the RSTP diameter:

DRSTP ⩽ MaxAgeTime ⩽ 40

Special case for RuggedCom™ switches

These switches, when configured for e-RSTP, use a proprietary protocol enhancement that enables a greater number of switches to be used. The formula that applies in this case is:

Nsub_max ⩽ (MaxAgeTime - 1) - [(Nmain - 1) / 4]



RSTP performance example (link failure, single ring).

Example of performance

The graph on the left shows the measured recovery time (Y axis, in ms) related to the number of ACE850 devices (X axis), on a single ring in case of link failure.

The actual performance level depends on the topology, the nature of the event, and the types of the devices on the network.

Other topology management protocols

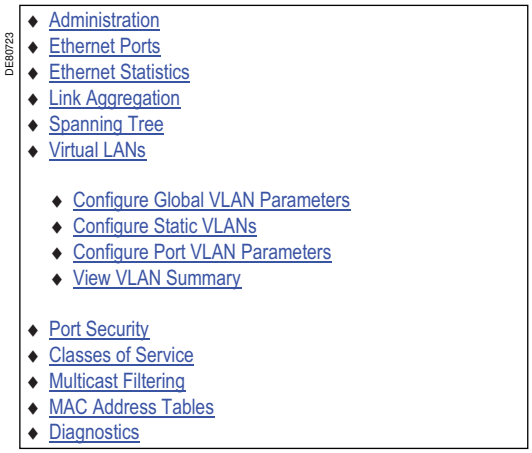
The advantages of RSTP are:
- It is standardized.
- It applies to any topology.

Depending on switch manufacturers, other topology management protocols can be offered, that sometimes have even better healing performance than RSTP. Most of them are however proprietary and apply only to ring topologies.
These protocols can be used for instance on a backbone ring made of switches from the same manufacturer. Conversely, they cannot be used on ACE850 rings. In that case, either the ACE850 are connected in a star configuration or the backbone switches also offer RSTP on the corresponding ports.

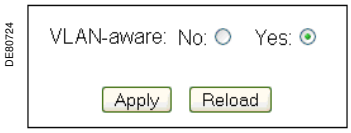
Breaking a storm

When a storm is installed, due to bad configuration or to equipment malfunction, it is almost impossible to establish communication with the devices through the network. The only possibilities to break the storm are usually:
- To connect locally on the devices and change the settings (this way does not work in every case).
- To physically open the loops by removing redundant connections.

When the number of devices in a network increases significantly, it is desirable or even essential for smooth operation to avoid useless propagation of traffic across the whole network. This is mainly true for multicast traffic as unicast traffic is already filtered by switches. Several traffic management possibilities are available.



RSG2100 Main menu and Virtual LANs submenu.



Configure Global VLAN parameters.

Subnets

Dividing a large network into smaller subnets enables the creation of limited broadcast domains. This technique can be used to avoid GOOSE message propagation to non related parts of the network.
On the other hand, routers are then necessary between subnets. These devices add to the infrastructure cost. They also require some time to perform the routing process which must be taken into account in the network design (this can impact SNTP synchronization for instance).
Subnets are generally not the preferred way of managing traffic in industrial networks unless their size is too large.

VLANs

VLANs create separate broadcast domains that can be used to restrict multicast traffic to particular network areas.
VLANs can efficiently manage GOOSE traffic but their usage has certain disadvantages:
- complicated configuration,
- problematic cohabitation with RSTP. The network must be configured so that RSTP never blocks a link that is a unique path for a VLAN. The Multiple Spanning Tree Protocol (MSTP) should be used with VLANs. It implements one spanning tree instance per VLAN and helps prevent the above situation. MSTP is however not available in Sepam devices and some switches.

For these reasons, we do not recommend the use of multiple VLANs in IEC 61850 networks. It is safer to use the default VLAN (usually VID 1) for all the traffic.

VLANs on ACE850

Frames other than GOOSE messages egress ACE850 without the 802.1Q VLAN tag. This tag can be added by intervening network switches, based on their configuration.
GOOSE frames egress ACE850 with a VLAN tag including the VLAN identifier (VID) defined in the CID configuration file. By default, this VID is 0, which is not a valid VID and is usually replaced by the port VID of intervening switches (default is VID 1). It is possible to define a valid VID value in a CID file, which is then left unmodified.

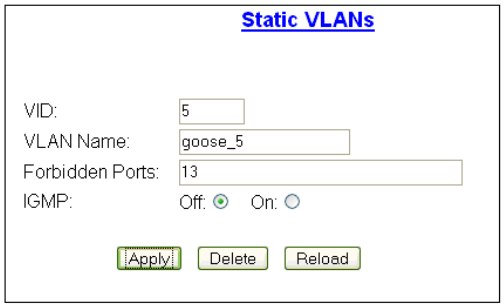
VLANs on RuggedCom™ switches

VLAN-aware mode
From the **Virtual LANs** submenu, select **Configure Global VLAN Parameters** to display the corresponding window.
Switches must be configured in the VLAN-aware mode (default configuration), in order to keep the VLAN tag of GOOSE frames which is also used to assign high priority to GOOSE messages.

Single VLAN
If a single VLAN is used the port default configuration should be kept or restored.

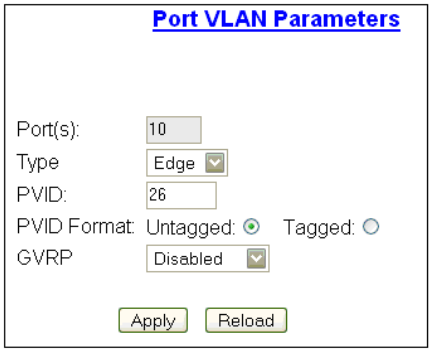
Multiple VLANs
Configuring static VLANs is done in 3 steps:
- declaring **static VLANs**
- configuring the **port VLAN parameters**
- checking the **VLAN configuration**.

DE80726



Static VLANs window.

DE80728



Port VLAN Parameters.

Declaring static VLANs

1. Select **Configure Static VLAN** from the **Virtual LANs** submenu. The list of already configured static VLANs is displayed.
2. To modify or delete a specific VLAN, click the desired VID. To create a new VLAN, click **Insert Record**.The **Static VLANs** window is displayed.

Modify the current values for an existing static VLAN or enter new values when creating a new static VLAN. Press **Apply** to save the configuration.

DE80725

VID	VLAN Name	Forbidden Ports	IGMP
5	goose_5	13	Off
9	MyGoose9	None	Off
26	MyVlan26	None	Off
38	MyVlan26hex	None	Off

Port VLAN parameters.

Configuring the port VLAN parameters

1. Select **Configure Port VLAN parameters** from the **Virtual LANs** submenu. The list of all the configured ports is displayed.
2. To modify the configuration of a specific port, click its port number. The **Port VLAN Parameters** window is displayed.
3. Modify the parameters according to your requirements.

When a port carries trafic for multiple VLANs, the port **Type** must be set to **Trunk**.
When a port carries traffic for a single VLAN only (as defined by the PVID), the port type must be set to **Edge**.
In both cases, untagged frames are assigned to the PVID VLAN.

DE80727

Port(s)	Type	PVID	PVID Format	GVRP
1	Edge	1	Untagged	Disabled
2	Edge	1	Untagged	Disabled
3	Trunk	1	Untagged	Disabled
4	Edge	1	Untagged	Disabled
5	Edge	1	Untagged	Disabled
7	Edge	1	Untagged	Disabled
9	Edge	1	Untagged	Disabled
10	Edge	26	Untagged	Disabled
11	Edge	26	Untagged	Disabled
13	Edge	1	Untagged	Disabled
14	Edge	1	Untagged	Disabled
15	Trunk	1	Untagged	Disabled
16	Edge	1	Untagged	Disabled

Port VLANs parameters.

Checking the VLAN configuration

To check the completed **VLAN configuration**, select **View VLAN summary** from the **Virtual LANs** submenu.

DE80729

VID	Untagged Ports	Tagged Ports
1	1-5,7,9,13-16	None
5	None	3,15
9	None	3,15
26	10-11	3,15
38	None	3,15

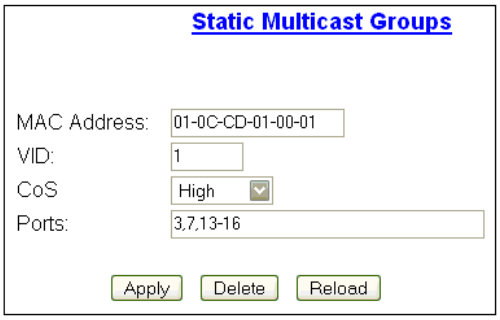
VLAN Summary.

DE80730

- Administration
- Ethernet Ports
- Ethernet Statistics
- Link Aggregation
- Spanning Tree
- Virtual LANs
- Port Security
- Classes of Service
- Multicast Filtering
  - Configure IGMP Parameters
  - Configure Static Multicast Groups
  - View IP Multicast Groups
- MAC Address Tables
- Diagnostics

RSG2100 Main menu and Multicast Filtering submenu.

DE80732



Static Multicast Groups.

Multicast filtering

Multicast frames are usually flooded by switches on all their ports, thus generating heavy and frequently useless traffic. Multicast filtering is a feature that enables the forwarding of multicast frames only to predefined ports of a switch, which decreases the overall traffic and consequently increases the available network bandwidth.

Note: *Two levels of multicasting exist: IP multicast and Ethernet multicast. We are considering only Ethernet multicast as most of the multicasting traffic is generated by GOOSE messages which are not IP frames.*

Multicast filtering on ACE850

The multicast filter of ACE850 is automatically configured to accept only subscribed GOOSE messages. It is not possible to configure it manually, therefore traffic management must be performed by the main switches.

Multicast filtering on RuggedCom™ switches

1. From the **Multicast Filtering** submenu, select **Configure Static Multicast Groups**. The list of already configured **Static Multicast Groups** is displayed. If no multicast group has been defined, the list is empty.
2. To modify a multicast group, click the corresponding **MAC Address**. To create a new group, select **Insert Record**.
3. In the **Static Multicast Groups** window, configure the parameters as required:

- List the ports to which the frames are to be routed.
- Set the **VID** and **CoS** parameters to the same values as those set for the GOOSE messages (default values are **VID=1** and **CoS=High**).

DE80731

MAC Address	VID	CoS	Ports
01-0C-CD-01-00-01	1	High	3,7,13-16
01-0C-CD-01-00-02	5	High	7,9

Static Multicast Groups summary.

DE80733

RSG2100 Main menu and Ethernet Ports submenu.

Port Rate Limiting

Port Rate limiting prevents broadcast storms by limiting the rates of broadcast, multicast, or unicast traffic on each port.

Port Rate Limiting on ACE850

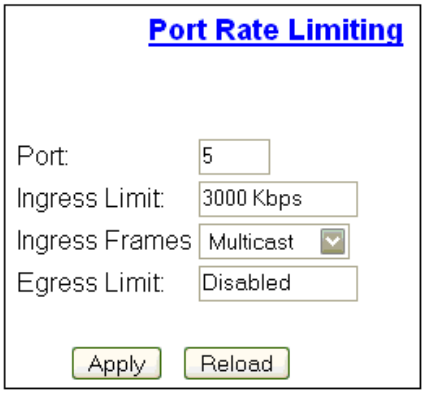
ACE850 has a built-in port rate limiting feature that is not configurable. This feature is mainly provided to protect the ACE850 against overloading and its threshold is defined intentionally high to not disturb traffic on the network. Consequently, this limit is too high to effectively prevent storms which must be achieved by the other network switches.

Port Rate Limiting on RuggedCom™ switches

The port rate limiting feature can be configured on the RuggedCom switches. To do so, proceed as follows:
1. From the **Ethernet Ports** submenu, select **Configure Port rate Limiting**. This displays details of the **Port Rate Limiting** configuration for all configured ports.
2. To configure a specific port, click its port number.
3. Configure the parameters as required.

It is important to select **Multicast** ingress traffic and define the limits according to the forecasted permanent traffic, as explained below.

DE80735



Port Rate LImiting.

DE80734

Port	Ingress Limit	Ingress Frames	Egress Limit
1	1000 Kbps	Broadcast	Disabled
2	1000 Kbps	Broadcast	Disabled
3	1000 Kbps	Broadcast	Disabled
4	1000 Kbps	Broadcast	Disabled
5	1000 Kbps	Broadcast	Disabled
7	1000 Kbps	Broadcast	Disabled
9	1000 Kbps	Broadcast	Disabled
10	1000 Kbps	Broadcast	Disabled
11	1000 Kbps	Broadcast	Disabled
13	1000 Kbps	Broadcast	Disabled
14	10000 Kbps	Multicast	Disabled
15	10000 Kbps	Multicast	Disabled
16	10000 Kbps	Multicast	Disabled

Port Rate Limiting summary.

Rate limiting example

As only multicast traffic is usually limited, the rate limit is based on the GOOSE traffic. Let us consider a site with 250 devices, each sending 2 GOOSE messages of 300 bytes each (2.4 kbits each) with a period of 500 ms in normal conditions. The resulting traffic is:
2.4 kbits x 2 GOOSE x 2 per second x 250 devices = 2.4 Mbps
To allow for increased traffic during event conditions and for other broadcast and multicast frames, the limit should be set to 5 or 10 Mbps.

Network security

Network components such as ACE850, ECI850, and switches offer basic security features such as password protection, IP addresses filtering, disabling of unused ports, which are usually sufficient for industrial networks.
If the network is connected to an unsafe environment such as the Internet or any public WAN, it is recommended to use appropriate protections such as filtering routers or firewalls.
The use of a Virtual Private Network (VPN) may also be considered.
These solutions are outside the scope of this guide.

Network time

Accurate operation of IEC 61850 servers requires that they are properly time synchronized. The IEC standard recommends the use of the SNTP protocol.
Both ACE850 and ECI850 use the NTP or SNTP servers in point to point mode (modes 3 and 4 of NTP). The broadcast mode (NTP mode 0) is not supported.
Both can also be configured with 2 server addresses, to enable the use of a backup time server in case the main one is not available.
If only the Modbus protocol is used with ACE850, it is still possible to synchronize the Sepam unit with SNTP. In that case, Modbus based synchronization must not be used.

Synchronizing RuggedCom™ switches

Although not always required, it is also possible to synchronize the switches from the same SNTP server. This is done from the **Configure Time and Date** item in the **Administration** menu.

Using a PC as time server

Microsoft Windows includes a NTP time server that can conveniently be used as the time source for testing. However, it is not stable enough for normal operation and its usage should be avoided.

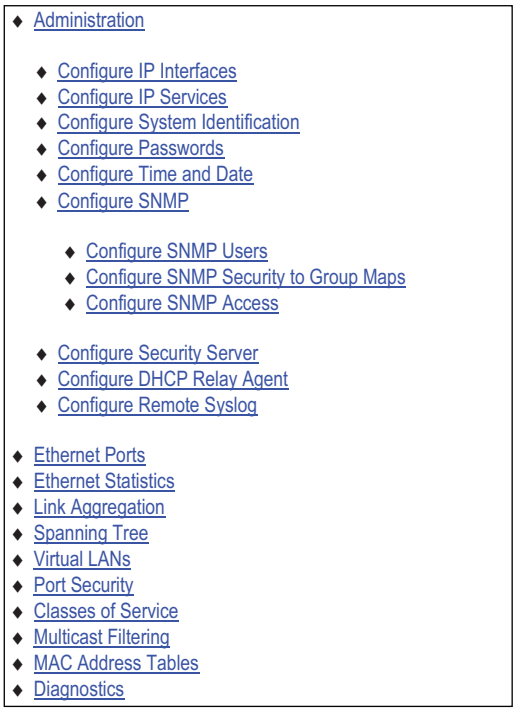
Network management

Usually SCADA systems indicate communication failures only when they have occurred (when communication with devices is no longer possible). To keep the redundant paths of the network available in case of failure, it is important to continuously monitor the overall state of the network including the backup links.
Various network management software are available on the market including ConneXview by Schneider Electric. They provide powerful active monitoring of the network using ICMP, SNMP, and various other means.
A passive, thus less powerful, monitoring can be performed using a simple SNMP trap receiver. Some can be freely downloaded from the Internet. Despite being better than no monitoring at all, we do not encourage this solution.

SNMP on ACE850 and ECI850

ACE850 and ECI850 are SNMP V1 compatible, their configuration is straightforward (refer to the associated manuals). ACE850 provides link up and link down SNMP traps.

DE80736

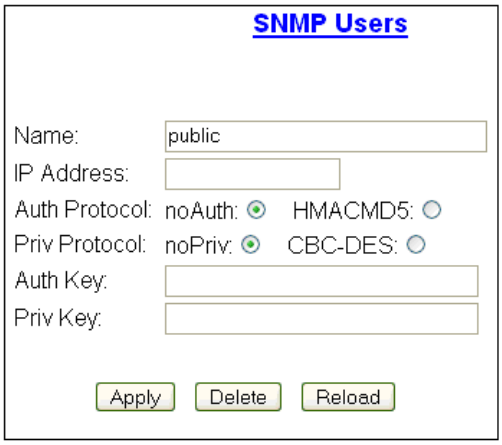


RSG2100 Main menu and Configure SNMP submenu.

SNMP on RuggedCom™ switches

Configuring the SNMP agent
Configuring the SNMP agent on a RuggedCom switch is done in 3 steps:
- Creating the SNMP user.
- Configuring security aspects.
- Specifying rights for the users.

DE80738



SNMP user creation page.

Creating the SNMP User
For monitoring purposes, this user is named public by default (this is the community name of SNMP V1 or V2).
1. From the **Configure SNMP** submenu, select **Configure SNMP Users**. This displays the **SNMP users summary** window.
2. Click **public** to modify the details of the public SNMP user.

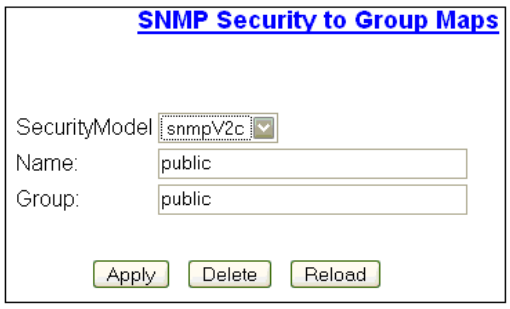
DE80737

Name	IP Address	Auth Protocol	Priv Protocol	Auth Key
public		noAuth	noPriv	

SNMP users summary.

If control capabilities are required, a corresponding user must also be created (its default name is **private**).

DE80740



SNMP Security to Group mapping page.

Configuring security aspects

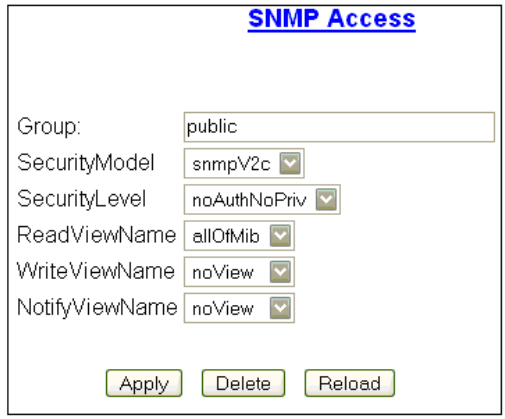
1. From the **Configure SNMP** submenu, select **Configure SNMP Security to Group Maps**. This displays the SNMP security groups summary window.
2. To modify the security group details, click the **SecurityModel Name**. Configure the parameters as requested by assigning the SNMP user to a security group.

DE80739

SecurityModel	Name	Group
snmpV2c	public	public

SNMP security groups summary.

DE80742



SNMP access rights page.

Specifying rights for the SNMP user

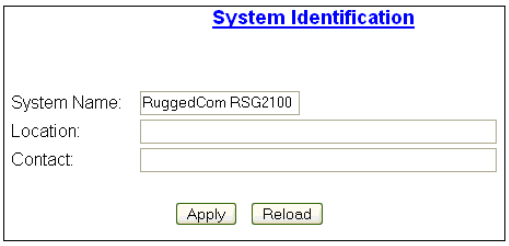
1. From the **Configure SNMP** submenu, select **Configure SNMP Access**. The **SNMP group rights summary** window is displayed.
2. Click the group name to modify the rights of a configured group.

DE80741

Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
public	snmpV2c	noAuthNoPriv	allOfMib	noView	noView

SNMP group rights summary.

DE80743



System identification page.

System identification

Complete the system identification fields which appear on the SNMP manager screen. From the **Administration** submenu, select **Configure System Identification**.

When all the network devices are connected together, powered on, and configured, it is necessary to check network operation. Various methods and tools are available to test the correct operation of the network. The way described here is an example of what can be done. We suggest to test network operation in 2 or 3 steps:

- *check basic operation*
- *check for abnormal conditions*
- *check GOOSE traffic, when applicable.*

Checking basic network operation

The simplest way to test a network is to try to address each equipment connected to it. This can be done by connecting a personal computer to the network and sending a **`ping`** command to every device on it.
If this test is successful, this does not mean that network operation is optimal but that the network is operating.

If a device does not answer to the **`ping`** request, check the following:

- Check that the ability to answer to ping requests function is not disabled as can be the case for PCs. Enable if necessary.
- Check links and connections by using the LEDs on the devices.
  - The link up LEDs must be on and the speed LED must match at both ends.
  - Check cables and link parameters at both ends of the link.
  - For fiber optic cables, check that transmit and receive fibers are not inverted.
- Check IP addresses and parameters:
  - If 2 devices are configured with the same address, only the first to connect can be reached.
  - If the device does not belong to the same subnet, there must be a valid path to it. Check the subnet mask and default gateway at both ends.
- Check the switch configuration (V-LANs).

Checking for abnormal conditions

Even if the devices respond to **ping** requests, there may exist abnormal conditions that disturb network operation.

Loops

Check the amount of traffic as an excess of traffic, especially broadcast and multicast, can indicate the presence of logical loops in the network. To do so, select **View Ethernet Port Statistics** from the **Ethernet Statistics** submenu to display the corresponding window.

DE80744

- Administration
- Ethernet Ports
- Ethernet Statistics
  - View Ethernet Statistics
  - View Ethernet Port Statistics
  - Clear Ethernet Port Statistics
  - Configure RMON History Controls
  - Configure RMON Alarms
  - Configure RMON Events
- Link Aggregation
- Spanning Tree
- Virtual LANs
- Port Security
- Classes of Service
- Multicast Filtering
- MAC Address Tables
- Diagnostics

RSG2100 Main menu and Ethernet Statistics submenu.

DE80745

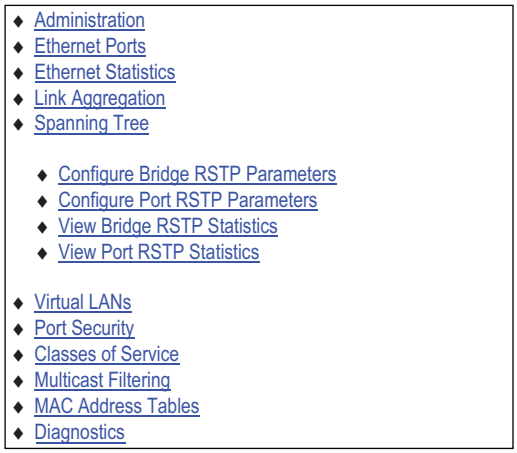
Port	InOctets	OutOctets	InPkts	OutPkts	TotalInOctets	TotalInPkts	InBroadcasts	InMulticasts	CRCA
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	6646357	127662831	24211	1315591	6646357	24211	52	12	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
7	124250991	768	1275245	12	124250991	1275245	80231	1195014	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
13	0	832	0	13	0	0	0	0	0
14	0	19277	0	194	0	0	0	0	0
15	3443073	6757279	40600	25952	3443073	40600	211	11	0
16	67905511	39763556	374609	605252	67905511	374609	80011	292901	0

Ethernet Port Statistics.

If the counters increase by an excessive rate, check that RSTP is enabled on every device (this page is not automatically refreshed: use the refresh button of the web browser to see the changes in the counters).
If in doubt, open the ring and check that the traffic returns to a lower value.

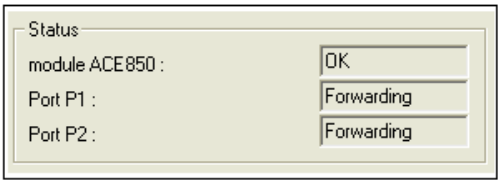
***Note:** The **Wireshark** tool (see next section) can also be used for this check.*

DE80746



RSG2100 Main menu and Spanning Tree submenu.

DE80747



SFT2841 Diagnostic screen (extract).

Backup links

If rings are used, check that backup links are operational and able to take over in case of failure. From the **Spanning Tree** menu, select **View Port RSTP Statistics** to display the corresponding window.

DE80769

Port(s)	Status	Role	Cost	RX RSTs	TX RSTs	RX Co
1	Link Down		0	0	0	0
2	Link Down		0	0	0	0
3	Forwarding	Designated	200000	12	902053	0
4	Link Down		0	0	0	0
5	Link Down		0	0	0	0
7	Discarding	Backup	200000	902043	12	0
9	Link Down		0	0	0	0
10	Link Down		0	0	0	0
11	Link Down		0	0	0	0
13	Link Down		0	0	13	0
14	Link Down		0	0	98	0
15	Link Down		0	0	1795	0
16	Forwarding	Designated	200000	62	602711	0

Port RSTP statistics.

For the ACE850, the link status can be checked either from the **SFT2841 diagnostic** screen or from the web interface.

Checking GOOSE traffic

Due to their nature and the use of VLAN tags, the flow of GOOSE messages is different from other traffic and so their circulation in the network must be checked. The GOOSE messaging statistics web page of ACE850 is provided for this purpose.

■ The first section shows all the published messages with the associated transmit counter. Check that messages are transmitted.

DE80748

GOOSE Produced

Index	GOOSE ID DataSet	Destination @ Vlan ID / Priority	Test	Enabled AppID	Min / Max (ms)	Tx Msgs
1	appGOTX IED01LD0/LLN0$GoDsA	01:0C:CD:01:00:01 0 / 4	☐	✓ 289	1024 / 4096	17318

ACE850 web interface: GOOSE messaging statistics page, transmit section.

■ The second section shows the subscribed GOOSE messages with the associated receive counter. Check that messages are received. If not, check that:
- ☐ A producer exists for these messages and that they are transmitted.
- ☐ Messages are not blocked by improper multicast filtering configuration.
- ☐ The receiver's VLAN membership is compatible with the message.
- ☐ A VLAN path exists between the producer and the receiver.

DE80749

GOOSE Subscribed

Index	GOOSE ID DataSet	Source @ Destination @	Test	Validity AppID	Quality Status QD / QR	Rx Msgs
1	appGOTX IED01LD0/LLN0$GoDsA	00:00:54:90:60:02 01:0C:CD:01:00:01		✓ 289	✓ ✓	17318
2	appGOTX IED02LD0/LLN0$GoDsA	00:00:00:00:00:00 01:0C:CD:01:00:02		✓ 289	⚠	0

ACE850 web interface: GOOSE messaging statistics page, receive section.

The following paragraphs describe diagnostic tools commonly used in troubleshooting communication problems.

Standard PC tools

The following tools are always provided with any personal computer.

Ping

The ping tool can be used to test if a device with a given IP address is connected to the network. It runs in a command interface window. The simplest form is:

```
> ping aaa.bbb.ccc.ddd
```

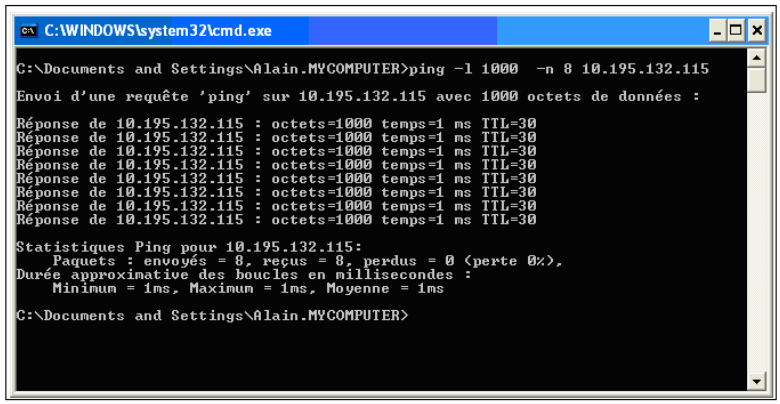
where `aaa.bbb.ccc.ddd` is the address to test.

Additional parameters (switches) can be provided before the IP address:

- `-l nnn`: instructs `ping` to use a nnn bytes long frame instead of the default frame.
- `-n nnn`: instructs `ping` to perform nnn consecutive tries.
- `-t`: instructs `ping` to run continuously until it is stopped by hitting **Ctrl**/**C**.

`Ping` makes use of an ICMP echo request. It cannot work correctly if ICMP traffic is blocked by some network nodes. More sophisticated versions of `ping` also exist, either commercial or freeware.

DE80750



Ping command and response.

Tracert

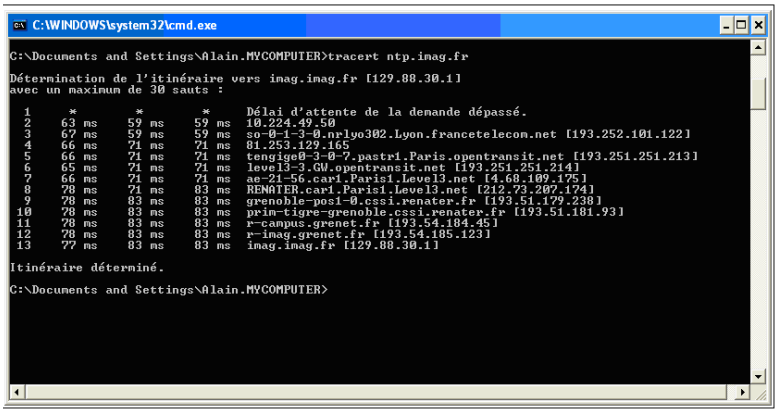
The `tracert` (trace route) tool is used to follow the successive routing path used by a frame along the network. It is therefore useless inside a single subnet. The simplest form is:

```
> tracert aaa.bbb.ccc.ddd
```

where `aaa.bbb.ccc.ddd` is the address to test.

Similarly to `ping`, `tracert` makes use of an ICMP echo request. It cannot work correctly if ICMP traffic is blocked by some network nodes.

DE80751



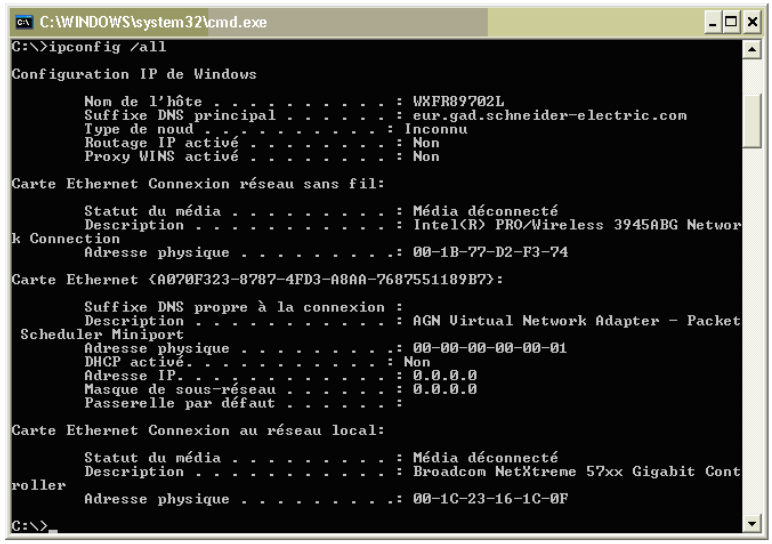
Tracert command and response.

Ipconfig

The Ipconfig tool is used to check the host PC configuration when it cannot establish communication with the network. The command line is:

```
> ipconfig /all
```

DE80752



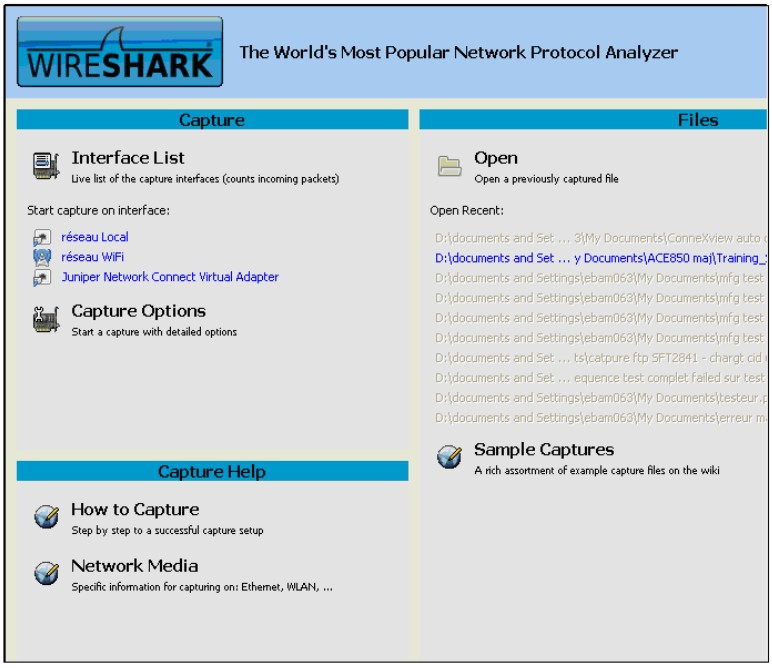
Ipconfig dialog box.

Wireshark

Wireshark (previously known as Ethereal) is a powerful network protocol analyzer that can be freely obtained from www.wireshark.org.
Simple analyses are straightforward even without previous knowledge of the tool, whereas deeper ones can be complex and require a good mastery of the tool.
Main uses of Wireshark are:
- Checking frames source and destination addresses (both at Ethernet and IP levels).
- Checking if particular protocol frames are transmitted (for instance, to be sure that a server receives, and is answering to, requests).
- Checking response times.
- Checking unexpected traffic origin.

Before using Wireshark, the basic communication problems must have been solved.

DE80753

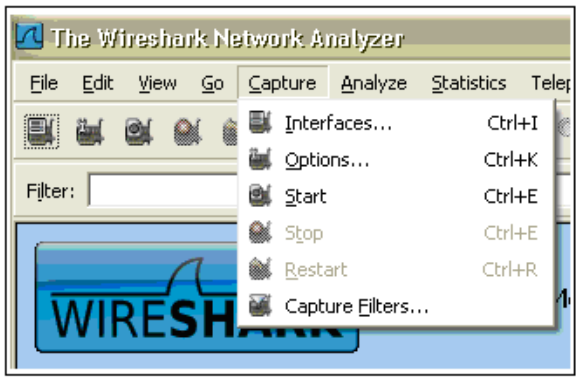


Wireshark: start page.

Capturing with Wireshark

The Wireshark start page lists the different network interfaces found on the computer. Capture can be launched by clicking on the corresponding interface. Default capture options are generally adequate but can be modified by clicking on **Capture options**.
The **Capture** menu item also provides a way to start and stop a capture and to change options.

DE80754

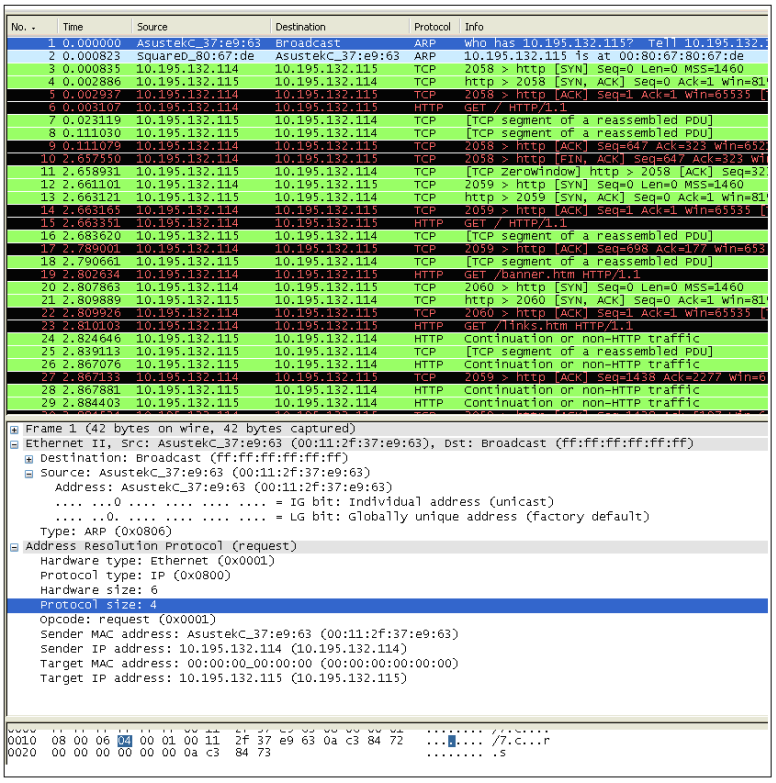


Capture menu.

Two capture options are of special interest:
- **Capture packets in promiscuous mode**: option used to capture all the frames present on the wire, even if they are not addressed to the computer.
- **Update list of packets in real time**: option used to display packets as soon as they are captured instead of waiting for the capture to be stopped.

The packets screen is divided in to 3 areas:
- Packets summary: lists all the captured packets in a synthesized way.
- Packet details: provides details of the selected packet with protocol interpretation.
- Packet dump: presents the raw content of the selected packet, expressed in hexadecimal and ASCII forms.

DE80755



Packets screen.

A display filter can be used to restrict the frames displayed according to specific criteria. It must be entered in the **filter** window and is activated by clicking **Apply**. A green background indicates a valid filter ; a red background indicates incomplete or incorrect expressions.

DE80756

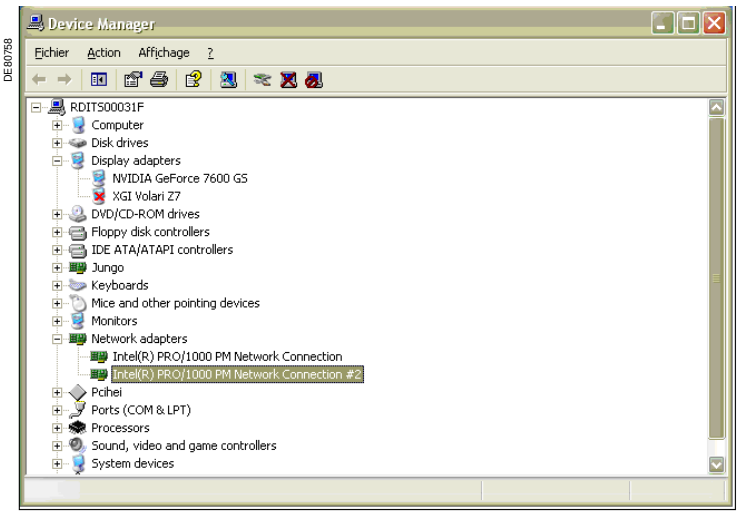
Display filter.

Commonly used filters are:
- IP address filters: `ip.addr == 169.254.0.10`
- Protocol filters: `tcp, snmp, arp`...

Complex filters can also be built, please refer to the Help for display filter syntax.

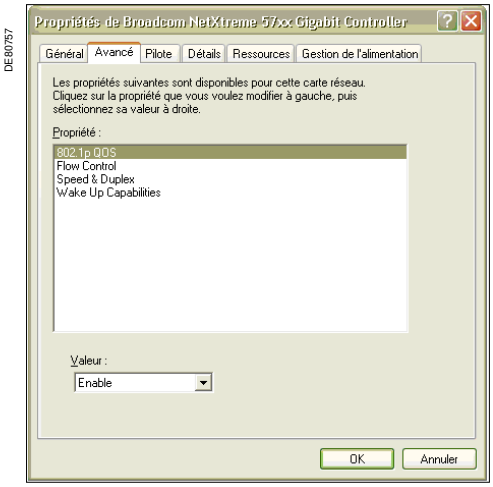
Capturing VLAN tags

VLAN tags are frequently removed by the computer network interface and are therefore not present on Wireshark capture. It is possible to request the interface to keep the tag in order to display it in Wireshark. To do this, go to the **Device Manager** and double-click the network interface.

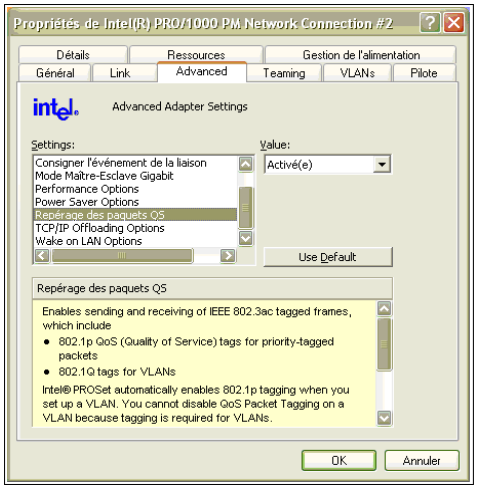


Device Manager window.

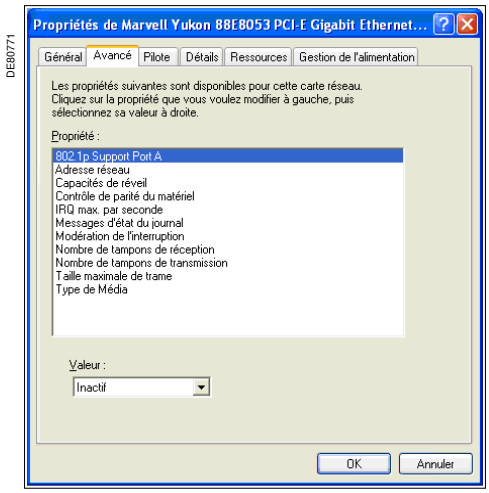
The screen displayed is device dependent. Select the **Advanced** tab (configuration of special features). Look for a parameter related to quality of service or 802.1p or 802.1q and enable it. Some examples are given below.



Example of network interface special features.



Example of network interface special features.



Example of network interface special features.

DE80710

RSG2100 Main menu and Ethernet Ports submenu.

Capturing the right traffic

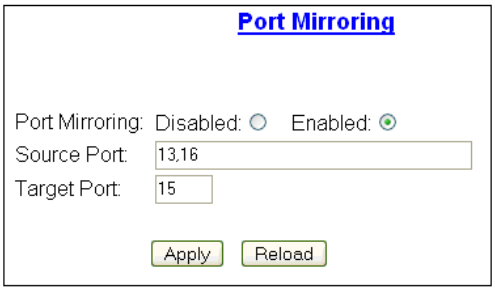
Wireshark can only capture traffic that arrives on the computer's network interface. In a switched network, this is usually only unfiltered multicast traffic and unicast traffic corresponding to the computer's MAC address.To monitor other traffic, use the following solutions:

- Insert a hub in the network and connect the computer to this hub.
- Use the port mirroring capability offered by many switches. This feature can be used to redirect a copy of the traffic flowing through one or several switch ports to a dedicated port to which Wireshark is connected.

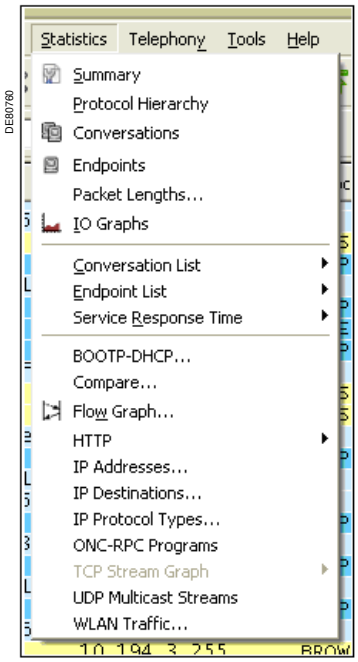
Port mirroring on RuggedCom™ switches

1. From the **Ethernet Ports** submenu, select **Configure Port Mirroring**.
2. Enumerate the port(s) to be mirrored.
3. Enter the mirror port number.

DE80761



Port Mirroring.



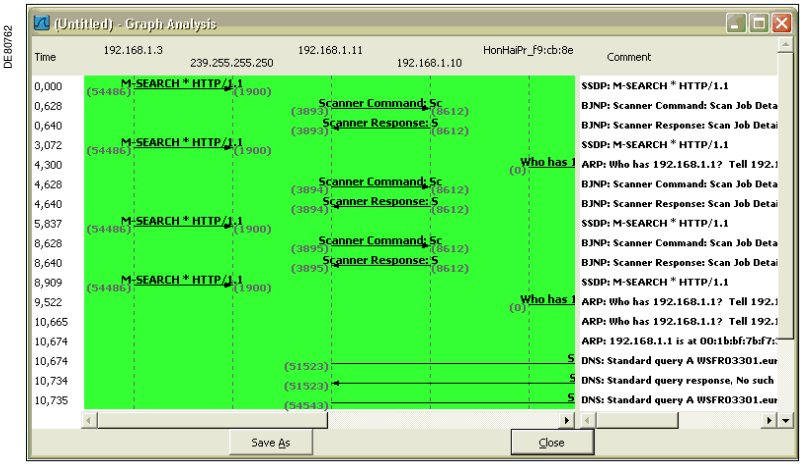
Wireshark Statistics menu item.

Additional analysis tools

Analyzing traffic flow using the Wireshark packets list can be cumbersome. However, the tool provides some helpful features that are accessible from the **Statistics** menu item.

Flow graphs

Flow graphs show the flow of exchange between nodes. They can be used to find unexpected traffic or exchange anomalies.

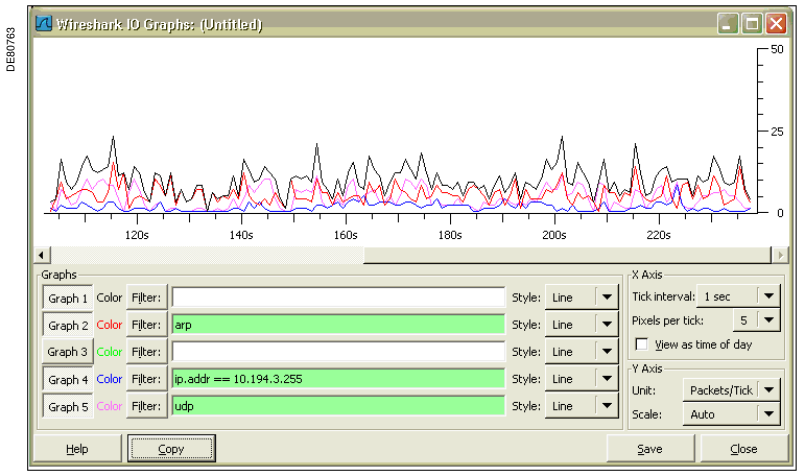


Wireshark flow graph.

IO graphs

IO graphs show the traffic profile against time. Filters can be applied to isolate specific traffic.

This graph can be used to check for storms.



Wireshark IO graph.

The following paragraphs describe some common problems encountered when building Ethernet Networks.
They do not replace the troubleshooting instructions contained in product manuals, which should be followed first, but provide additional tips and recommendations.

Incorrect wiring or physical setup

Always use link status indications to ensure the links are properly established. In case they are not:
- For copper links:
  - Check that the proper type of cables between the device and the switch (direct cable) or between switches (crossover cables is used). This applies only if the devices do not have the auto-MDIX capability.
  - Check that the cable category matches the speed that is used.
- For fiber links:
  - Check that the correct fiber type (monomode or multimode is used).
  - Check that the fibers are not inverted (Tx1 on Tx2 instead of Tx1 on Rx2).
- Check that both end of the link have the same speed.
- Check that the declared type for ACE850 (TP or FO) is correct, as this changes the default settings.
- Check that the switches ports are enabled.

Duplex mismatch

In Ethernet, a duplex mismatch is a condition where 2 connected devices operate in different duplex modes, that is, one operates in half-duplex while the other one operates in full-duplex. A duplex mismatch results in a network that works but is often much slower than its nominal speed.A duplex mismatch can be the result of manually setting 2 connected network interfaces to different duplex modes. It can also be the result of connecting a device that performs auto negotiation to one that is manually set to a full-duplex mode. When a device set to auto negotiation is connected to a device that does not use auto negotiation, the auto negotiation process fails. The standard requires the use of half-duplex in these conditions. Therefore, the auto negotiating end of the connection uses half-duplex while its peer is locked at full-duplex.
A duplex mismatch causes problems when both ends of the connection attempt to transfer data at the same time. In such conditions, the full-duplex end of the connection sends its packets while receiving other packets: the purpose of a full-duplex connection. Meanwhile, the half-duplex end cannot accept the incoming data while it is sending and interprets it as a collision. As a result, almost all of the packets sent by the full-duplex end are lost because the half-duplex end is streaming either data packets or acknowledgments at the same time. The end result is a connection that works (no errors are usually reported from a ping command) but performs extremely poorly.
Ethernet statistics can help diagnose this problem:
- The effective data transfer rate is asymmetrical, performing much worse in one direction than the other.
- The collisions seen on the half-duplex side of the link are late collisions, which do not occur in normal half-duplex operations.
- The full-duplex side usually registers frame check sequence (fcs) errors.

Actual duplex for ACE850 and ECI850 links can be checked on the web interface.

IP setup issues

Common errors for the IP parameters are:
- The same IP address is assigned to several devices.
- The subnet mask is not properly defined and some devices are considered outside of the subnet to which they belong.
- The gateway is not on the same subnet as the device.
- IP filtering is enabled on ECI850 or ACE850 but not set up with the correct addresses.

Firewalls

If firewalls (or routers) are installed on the network, ensure that they do not block useful traffic. The following IP ports are required for normal system operation:

- Ports 20 and 21: FTP traffic
- Port 80: HTTP traffic (web)
- Port 102: IEC 61850 traffic
- Port 123: NTP/SNTP traffic
- Ports 161 and 162: SNMP traffic
- Port 502: Modbus traffic

FTP transfer issues

ACE850 and ECI850 devices use the File Transfer Protocol (FTP) for loading/unloading CID configuration files and for firmware updates.
The FTP protocol is probably one of the most popular application protocols of the Internet suite but also the most misunderstood.

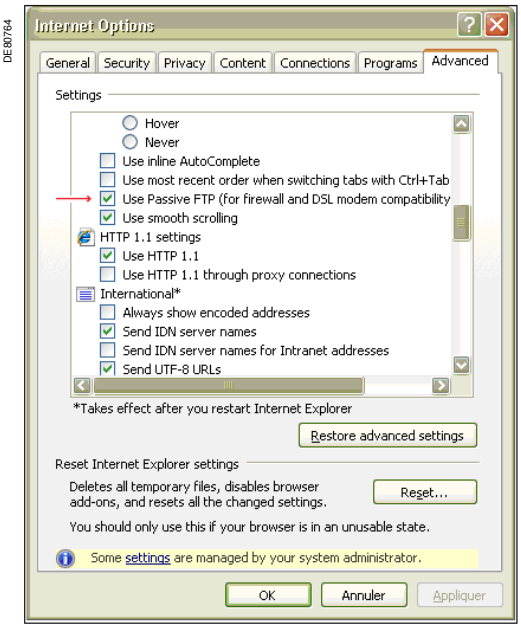
Active and passive modes

The usual (implicit) way of using FTP is the active mode (sometimes called Port mode). This mode requires the server to open a connection on the client, usually a PC. This opening can be blocked by the computer's firewall.
If you can login to a FTP server but your directory listings and data transfers time-out, you are most likely in this situation. To overcome this issue, there are 2 possibilities:

- Use the passive mode, if available on the FTP client (passive mode is available on both ACE850 and ECI850).
- Disable the firewall or configure it to allow FTP traffic.

Using FTP passive mode

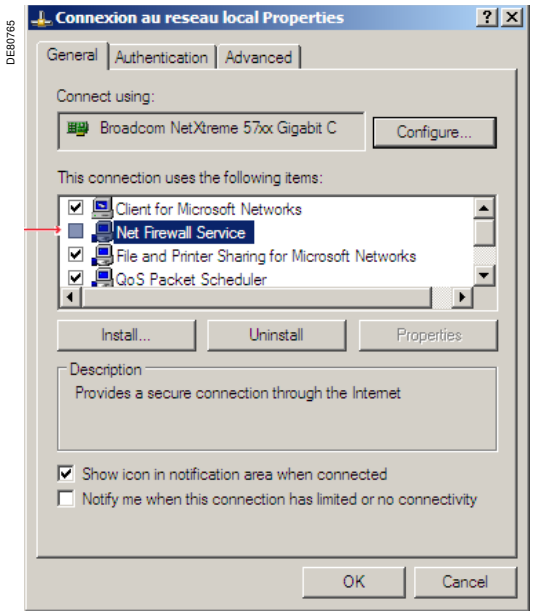
Not every client is capable of working in passive mode. Internet Explorer can be configured in this mode. To do so, from the **Tools** menu, select the **Internet Options**, and then select the **Advanced** tab. Check the **Use Passive FTP** option in the list.



Advanced Internet Options in Internet Explorer.

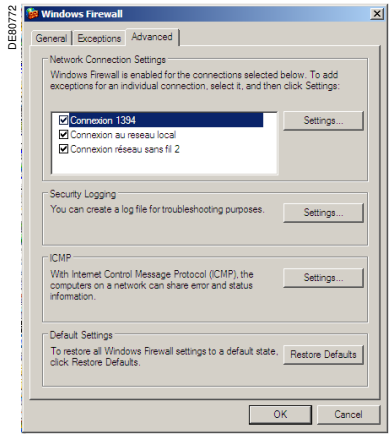
Disabling the firewall

The standard Windows firewall can be disabled on a specific network connection by unchecking the **Net firewall Service** in the **Network connection** properties dialog box for that connection, as shown on the left.
If this option does not appear in the list or if disabling it is not efficient, double click **Windows firewall** option in the control panel. Check that the firewall is disabled globally (**General** tab) or at least on the network connection that you use (**Advanced** tab).



Disabling firewall in network connection properties.

Windows firewall general tab.



Windows firewall advanced tab.

As several versions of native Windows firewall exist as well as firewalls from third party editors, it is impossible to give explanations for all of them. Please refer to the manuals or to your network administrator.

Issues with FTP clients

The design of the FTP protocol is intended for use by a human operator from a command line interface at the client level. This implies that different FTP implementations can:

- use different subsets of FTP commands,
- present the command results in different ways.

FTP clients with graphical user interfaces have been developed, which assume results are presented in a given way and use a predefined set of FTP commands. These clients are therefore not ensured to work with every FTP server on the network.

At the time of writing, we recommend the use of the following FTP clients:

- ECI850: Windows command line interface, Internet Explorer 6.0, or Windows Explorer.
- ACE850: Windows command line interface.

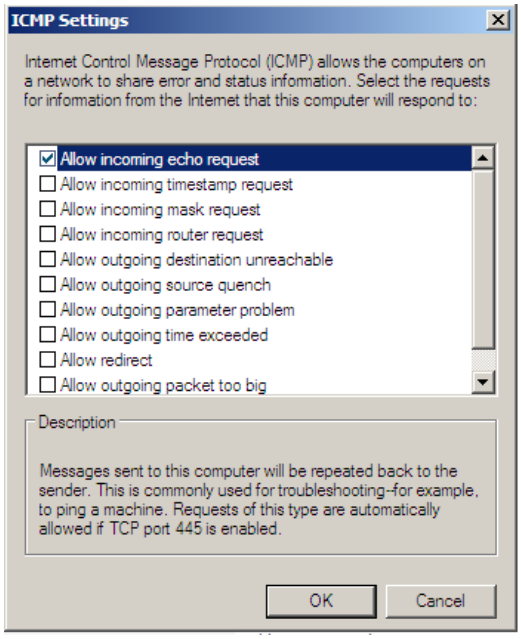
Note: *The Windows command line interface does not feature passive mode.*

ICMP does not work on a PC

If a PC does not reply to ping commands, this is probably because ICMP echo requests are disabled.

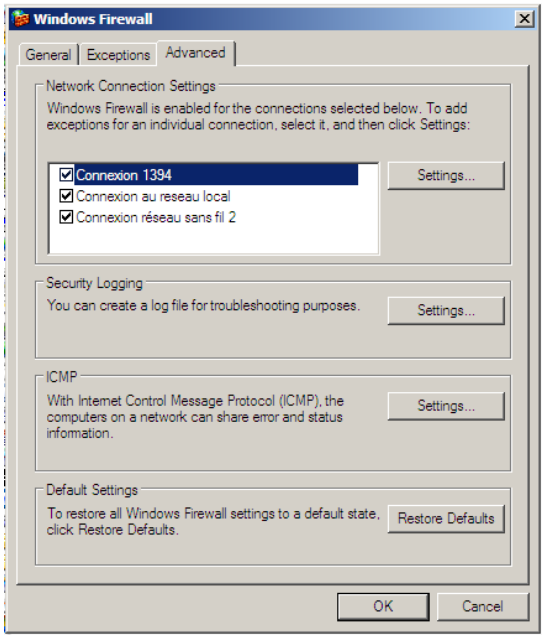
To enable ping commands, open the Windows firewall configuration panel, go to the **Advanced** tab and click the **ICMP parameters** button. In the new panel, authorize ICMP echo request by checking the corresponding box and validate by clicking **OK**.

DE80785



ICMP parameters window.

DE80772



Windows firewall advanced tab.

References and bibliography

Additional information can be found in the following documents or sources which have been used for the writing of this guide:

- Fiber optical networks revealed - RuggedCom Inc. (www.ruggedcom.com).
- A comparison of dispersed topologies for Ethernet by Roger Moore - RuggedCom Inc.
- Implementing robust ring networks using RSTP and e-RSTP, Application note - RuggedCom Inc.
- Transparent Ready User Guide, ref. 31006929 - Schneider Electric (www.schneider-electric.com).
- Wikipedia, The Free Encyclopedia (www.wikipedia.org).
- Internet standards (RFCs) - The Internet Engineering Task Force (IETF) (www.ietf.org).
- IEEE 802 standards - Institute of Electrical and Electronics Engineers, Inc (www.ieee802.org).
- Modbus specifications - Modbus Organization, Inc (www.modbus.org).
- IEC 61850 standard - International Electrotechnical Commission (www.iec.ch).

Schneider Electric Industries SAS

35, rue Joseph Monier
CS 30323
F - 92506 Rueil-Malmaison Cedex
RCS Nanterre 954 503 439
Share capital 896 313 776 €

www.schneider-electric.com

Printed on recycled paper

Production : Assystem France
Publication / Publishing : Schneider Electric

SEPED310018EN

10/2010