460

The use of Ethernet Technology in the Power Utility Environment

Working Group

D2.23

April 2011

The use of Ethernet Technology in the Power Utility Environment

Members

Carlos Samitier (Convenor) Spain, Mehrdad Mesbah (Secretary) France,
Jorge Fonseca-Portugal,Pat Cooney-Ireland, Anders Runesson-Sweden,
Andres Cadenas-Spain, Aitor Arzuaga-Spain, Emiliano Marquesini-UK,
Paul Schwyter-Switzerland, Sampo Yliraasakka-Finland,
Ray Elliott-South Africa, Oyvind Finnekaasa-Norway, Chris Huntley-Canada

Corresponding Members

Rodolfo Pellizzoni-Argentina,Dugald Bell-Australia, Jan Piotrowski-Poland,
Claudio Trigo-Brazil,Masami Inoue-Japan, Mrs. Jovanka Gajica-Serbia, Wan Azlan-Malaysia

ISBN: 978- 2- 85873- 149-7

1 INTRODUCTION 6
1.1 Scope of Work 8
1.2 What is Ethernet? 8
1.3 Service Provision Model 10
1.4 Benefits 11
1.5 Business Implications 13
1.6 Cost Considerations 14
2 UTILITY INDUSTRY CONTEXT AND APPLICATIONS FOR ETHERNET 15
2.1 Introduction 15
2.2 Utility Applications 15
2.2.1 Substation Control 15
2.2.2 Substation Data Analysis 15
2.2.3 Real Time Protection and Automation 16
2.2.4 Substation Automation Platform Management 16
2.2.5 Commercial Applications 16
2.2.6 Substation Management 17
2.2.7 Site Working 17
2.2.8 Security Applications 17
2.2.9 Substation Operational Voice System 18
2.2.10 Collaborative Multi-media Communications 18
2.3 Substation Automation Process – IEC61850 19
2.3.1 Introduction to IEC61850 19
2.3.2 Model & Mechanisms of IEC61850 19
2.3.3 Time synchronisation for substation automation 22
2.3.4 Further Extensions 22
2.4 SCADA and ICCP related Utility communication characteristics 23
2.4.1 Overview of EMS/SCADA Communications 23
2.4.2 SCADA RTU to Control Centre Communications 24
2.4.3 Inter-Control Centre Communications 26
2.4.4 SCADA System Security 27
3 NETWORK TECHNOLOGY DESCRIPTION 29
3.1 Concepts and Definitions 29
3.1.1 Topology: LAN, MAN and WAN 29
3.1.2 Layer 2 networking 29
3.1.3 Differences with Layer 3 IP network 30
3.2 Networking architecture 30
3.2.1 Bridging 30
3.2.2 Switching 30
3.2.3 Virtual Networking 31
3.2.4 RPR – Resilient Packet Ring 33
3.2.5 Provider Backbone Bridging 34
3.2.6 MPLS-TP 35
3.3 Protection Mechanisms 36
3.3.1 Spanning Tree 36
3.3.2 Ethernet Ring Protection 37
3.3.3 IEC 62439 Parallel Redundancy Protocol (PRP) 37
3.4 Existing relevant Ethernet standards 38

3.5 Authentication & Security services over Ethernet 40
3.5.1 Physical port protection 40
3.5.2 Authentication & Encryption (RADIUS) 41
4 ETHERNET TRANSMISSION TECHNOLOGIES 42
4.1 Introduction 42
4.2 Copper interfaces 43
4.3 Fibre interfaces 43
4.3.1 Optical Gigabit Ethernet Interfaces 43
4.3.2 10 Gigabit Ethernet interfaces 44
4.4 Optical Networks - Wavelength division multiplexing 45
4.4.1 CWDM (Coarse Wavelength Division Multiplexing) 45
4.4.2 DWDM (Dense Wavelength Division Multiplexing) 46
5 TRANSPORT OF ETHERNET OVER SDH 47
5.1 Introduction 47
5.2 Modern SDH Data Capabilities 47
5.2.1 Virtual concatenation 49
5.2.2 Dynamic Bandwidth Allocation 49
5.2.3 Generic Framing Procedure (GFP) 49
5.2.4 Combining TDM and LAN Services 52
6 ETHERNET ACCESS TECHNOLOGIES 54
6.1 Ethernet over xDSL 54
6.2 PDH sub-E1 mapping 55
6.3 Inverse Multiplexing 55
6.4 Microwave Radio 56
6.4.1 Microwave Backbone Ethernet 56
6.4.2 Microwave Access Systems 56
6.5 DPLC Bridge 57
6.6 GPRS and UMTS 59
6.7 VSAT 60
6.8 Broadband Power Line Communication 62
6.9 Passive Optical Networks (EPON) 63
6.10 Free Space Optical links 65
7 WIRELESS ETHERNET NETWORKS 66
7.1 Introduction 66
7.2 Wireless LAN or WiFi (IEEE 802.11) 67
7.3 Wireless MAN or WiMAX (IEEE 802.16) 69
7.4 Wireless PAN, Wireless Sensor Networks (IEEE 802.15) 70
8 EMULATED LAN SERVICE 71
8.1 Ethernet Emulation 71
8.2 Ethernet over MPLS – VPLS 72
8.2.1 Multi-Protocol Label Switching (MPLS) 72
8.2.2 Transporting Ethernet over an IP/MPLS network 72
8.2.3 Virtual Private LAN Service (VPLS) 74
8.3 Ethernet over ATM – LANE 75
8.3.1 LAN Emulation Components 76
8.3.2 Location of LAN Emulation Service Components 76
9 APPLICATION REQUIREMENTS 77

9.1 IEC-61850 Performance Requirements 77
9.2 Service Availability Issues 79
9.3 Applications Performance Requirements 80
10 ARCHITECTURAL DESIGN GUIDELINES 84
10.1 Performance 84
10.1.1 Network Throughput and Full Duplex Operation 84
10.1.2 Network Availability 85
10.1.3 Quality of Service (QoS) 86
10.1.4 Ethernet Broadcast Control 88
10.2 Topology 90
10.2.1 Cascade 90
10.2.2 Star Topology 90
10.2.3 Ring 91
10.2.4 Hybrid Architecture 92
10.2.5 Mesh Topology 93
10.3 Scalability 94
10.4 Management 95
10.4.1 Fault-management 96
10.4.2 Performance monitoring 96
10.4.3 Traffic monitoring 97
10.4.4 Traffic Engineering 97
10.4.5 Configuration management 97
10.5 Ethernet Security 98
10.5.1 Practices and policies 98
10.5.2 Remote Access 100
10.6 Resiliency 101
10.6.1 Service Availability and Fault Tolerance Objectives 101
10.6.2 Fault-tolerance and Redundancy Design 102
10.6.3 Topology 103
10.6.4 Restoration Mechanisms and Recovery Time 103
10.7 Service isolation and VLAN Mapping 104
10.7.1 Segregating and Prioritizing Data 104
10.7.2 Isolating Device Failures 105
10.7.3 Limiting Network Outages with MSTP 105
10.7.4 Service, VLAN and Priority mapping 105
10.8 Switch Requirements for Operational Ethernet 107
10.9 Internetworking 109
10.9.1 Layering architecture 109
10.9.2 Implementation of distributed LAN 109
10.10 Physical packaging of network functions 110
10.11 Transport technology design 111
10.12 Migration & Legacy Integration 112
10.12.1 Migration with legacy systems 112
10.12.2 Integration of Legacy devices 113
10.12.3 Integration of existing SCADA RTUs 113
11 ENVIRONMENTAL & MECHANICAL ISSUES 115
11.1 Fibre types 115

11.1.1 Multimode fibre (MM) 115
11.1.2 Single Mode fibre (SM) 116
11.1.3 Optical connectors 117
11.2 Copper cables 119
11.3 Electromagnetic Compatibility (EMC) 120
11.3.1 RF interference 121
11.3.2 Shielding and Grounding 121
11.4 Power over Ethernet (PoE) 123
12 CASE STUDY – REN Portugal 124
12.1 Introduction 124
12.2 Network topology, technology and design issues 124
12.3 Network architecture 126
12.4 Management and central services of Ethernet network 127
12.5 Conclusions 128
13 APPENDICES 129
Appendix 1 – Ethernet Related Standards 130
ITU-T G.7041 130
ITU-T G.7042 130
ITU-T G.7043 130
ITU-T G.8040 130
ITU-T Y.1730 130
ITU-T Y.1731 130
Appendix 2 – Abbreviations 131
Appendix 3 – References 134

1 INTRODUCTION

In order to run reliably their core business, utilities must maintain a complex, geographically distributed infrastructure covering generation facilities, remote substations or other components such as pipelines and railways. To ensure public safety, equipment at these infrastructure locations must function reliably and predictably and the telecommunication service provided has to fulfil the requirements of every service integrated in the network. The consequences of malfunction and failure are generally severe and operationally unacceptable, leading to a rather conservative position in adopting newer technologies. Deterministic (e.g. TDM) solutions are perceived to be the most reliable. Meanwhile Ethernet technology has gained wide acceptance for many operational utility services.

The advances in broadband technologies together with the need for simplification of access interfaces are introducing the Ethernet interface as the standard access interface for any type of data device. Furthermore, the Ethernet interface can accommodate virtually any type of protocol thus becoming a straightforward solution for legacy and new protocol integration over a common telecommunication infrastructure.

The main objective of this technical Brochure is to explore the new opportunities, advantages and disadvantages introduced by the use of Ethernet technology, especially for the Power System Protection and Control applications.

Although Ethernet was primarily developed as a local area network interface, broadband backbones allow the transport and distribution of information so now Ethernet has become a technology that can also be used in Wide Area Network (WAN) applications. In fact, Ethernet is now a service offered by the latest generation of broadband WAN networks.

This aspect is developed by the technical brochure exploring interoperability and interaction with other technologies, whether transmission or networking.

Consequently, to run a utility network with the appropriate availability and safety requires highly reliable communication systems for local as well as for wide area interconnectivity.

This Technical Brochure covers those critical design and implementation aspects that may have a direct impact on the network and service reliability. The structure and content of the document is as follows:

- Chapter 2 defines Power Utility context and applications for Ethernet. It develops how different applications can use Ethernet and the key aspects to be considered.

- Chapters 3 to 8 describe Ethernet technology, associated transmission, transport and emulation. Covering all the possibilities that may be of interest to the Power Utility environment both, as an access interface, as well as a service provided by a network.

- Chapter 9 defines applications requirements with special interest in the IEC 61850 requirements since they are the most critical application of Ethernet technology.

- Chapter 10 and 11 develop design and implementation issues. These are the most critical aspects to be considered in order to achieve a reliable network.

One should consider not only the technical aspects and performance of Ethernet but also the organizational issues. Behind each Utility communication network is a team with a high responsibility and a certain history. Introducing Ethernet may need a completely new mind-set. The past was dominated by ‘point to point’ thinking and dedicated ‘wires’ for a specific application or equipment. Suddenly, mission critical signals are expected to find their way through a network cloud. Combining the advantages of traditional- and Ethernet-technologies provides a solution to this issue. The operational team of the Utility needs substantial training and experience to trust in, and to implement and to operate the new Ethernet-technology. It’s much more than “plug & play”!

The brochure is complemented with a case study and the appendix that includes further information and references for those readers interested in developing some technical aspects.

1.1 Scope of Work

The objective of the present brochure is to assist utilities to plan, specify, design and implement Ethernet infrastructures necessary for the IP-based operational applications of the electrical power delivery system.

The document covers operational applications relative to the power delivery process in the HV substation and in the Control Centre, as well as the associated Operation Support applications connecting the Utility office to the HV substation or to the Control platforms.

Corporate enterprise data networking in the Utility office, being very similar to other office LAN cabling and infrastructure, is already covered extensively in the networking literature and is therefore excluded from the present brochure.

Similarly, the brochure is limited to the Ethernet layer and does not describe or discuss the IP network (or any other network) overlaying the Ethernet infrastructure. Multi-service operational IP networks and the use of Virtual Private Networks (VPN) for implementing Operational services are already covered in other Cigre D2 Brochures as presented in the Bibliography and References section.

Finally, the present brochure presents concepts, standards, network technologies, architectures and practical guidelines for implementing Ethernet in the power delivery system, but limits its description of the underlying transmission and transport technologies (Fibre, SDH, Radio, etc.) to the issues and aspects which are directly related to carrying Ethernet traffic.

1.2 What is Ethernet?

Ethernet was originally a local computer network developed by Xerox in the 1970s based on the idea of sharing a coaxial cable as a broadcast transmission medium. The analogy with packet radio systems operating in a similar manner over the “ether” gave birth to the name “Ethernet”. Robert Metcalfe and David Boggs paper “Ethernet: Distributed Packet-Switching for Local Computer Networks” published in 1976, can be considered as the starting point for Ethernet.

Sharing of the coaxial cable broadcast medium was performed through a “Medium Access Control” protocol called Carrier Sense Multiple Access (CSMA): Any computer desiring to transmit would “sense” the shared medium to check if there was no other on-going activity (Carrier Sensing). In the event of a collision with another communication, the system had mechanisms for collision detection (CD) and each colliding station would restart after a pre-determined (or random) lapse of time.

This rather simple operation mode was adopted as an IEEE standard in 1983 and used widely in the computing world. The physical characteristics associated to this network were noted as 10BASE5 (10 Mbps, Baseband modulation, 500 meters span). In the following years many other versions and physical layers were added to the IEEE standard constituting a whole range of network technologies and components.

The principle of using one broadcast cable medium for all connected stations required however a means of preventing service interruptions when stations were being added or removed. The

well-known particularity of Ethernet technology in the 1980s was the “vampire tap” Cable Attachment Unit biting the Yellow Ethernet Coax to connect with the cable core and shield. This highly sensitive, error-prone and costly mode of cable attachment was overcome through the replacement of the semi-rigid coaxial cable with point-to-point links over unshielded twisted-pairs connected together by hubs as defined in StarLAN (1BASE–5 and later 10BASE–T). The advent of hub-based twisted-pair wiring enabled Ethernet to become a commercial success due to reduced installation costs, increased reliability, and point-to-point management and troubleshooting.

Also, through the use of the electronic hub, Ethernet topology evolved from a simple bus into a great number of hybrid topologies and structures adapting to the requirements of any environment. Optical repeater sections, different cable types and technologies could be mixed according to the requirements of each section of the network.

Finally, the evolution from Hub-based networks to Bridged and Switched Ethernet in the early 1990s removed the constraint of uniform bit rate and the paradigm of packet collision over the network, replacing the CSMA/CD scheme by a switched full duplex system.

Moving to point-to-point full duplex links separated by switches also allowed the move to ever higher speeds using the progress in switching technology: from 10 Mbps to Fast Ethernet at 100Mbps, and further to Gigabit Ethernet and 10 Gigabit Ethernet. At present IEEE is preparing for 40 and 100 Gigabit Ethernet for Access and Core network technologies.

Historically, Ethernet was considered as a non-deterministic network, which excluded it largely from being applied for real-time applications. Early industrial networks, such as IEC PROWAY and different types of FIELDBUS, were based on Token passing protocols rather than Ethernet. Collision probability in the CSMA/CD protocol could be kept low only by limiting severely the traffic and therefore network throughput. Switched Ethernet in the early 1990s coupled with careful traffic engineering have significantly narrowed the deterministic versus non-deterministic debate.

Ethernet standards and technologies, which were already in extensive use in the office computer networking, were adopted for services that required rather tight real-time performance. In order to meet the environmental constraints and the availability and performance requirements of the industrial process, more robust and environmentally resistant network switches have been developed integrating leaner and faster service restoration and fault tolerance.

Ethernet allows only the exchange of data frames between connected machines. It was initially supported by the vendor’s proprietary operating systems which did not allow integration across dissimilar vendor platforms or across multiple networks. Over time protocols were introduced that did allow mixed vendor support over Ethernet. At present, TCP/IP is the predominant transport and network protocol being used over Ethernet in the Office system architecture.

In the Electrical Power Utility environment, TCP/IP transport is also omni-present and shall concern the majority, but not all, of the operational and operation support traffic over the Utility Ethernet infrastructure:

- ⇨ operation support communications (file transfer, document exchange, data base access, remote server access and mail),
- ⇨ SCADA RTU communications (IEC 60870-5-104),

- ⇨ inter-Control Centre communications (TASE2, ICCP),
- ⇨ digital substation automation applications (IEC 61850 MMS)

TCP transport resides in the end stations, however the IP internetworking can be in every intermediate node, or if lower delay is required, only in the end stations without internetworking.

Utility applications such as voice and video-surveillance are carried over Ethernet through an IP network without using TCP transmission control. Other applications use Ethernet end-to-end without IP (e.g. protection relay tripping).

1.3 Service Provision Model

An Ethernet connection can be provided between two or multiple access points in different manners. Complex networks as those of Electrical Power Utilities are often a hybrid combining two or three levels of connectivity using the following techniques.

An Ethernet LAN with local or limited coverage can be implemented over copper wire, optical fibres or a wireless medium depending on the distance, required throughput and environmental constraints. In this case, the network is implemented simply through the appropriate Ethernet Transceivers incorporated into the Ethernet LAN switches and connected into the required topology. Optical Ethernet interfaces and in particular GigaEthernet can be implemented over a wavelength, sharing in this way the fibre capacity with other traffic through wavelength division multiplexing (WDM).

The Ethernet network can also be implemented over an SDH or PDH transport layer which allocates some bandwidth for the transport of Ethernet data frames mapped into the workload of the multiplex system. This approach allows the transmission over larger distances than the previous case and shares the same transmission resource (e.g. STM-4 or STM-16) for Ethernet and TDM traffic.

Ethernet connectivity is increasingly available through Service Providers as a replacement of previously available “leased line” (LL) managed services. Telecom Service Providers have started to include Emulated Ethernet services known as Metro Ethernet in their offer. This has been made possible by using VPN (Virtual Private Network) capabilities of their MPLS infrastructure as described in the following sections.

Metro Ethernet consists of providing Ethernet services directly to customer sites dispersed across a Metropolitan domain and hence allowing them to operate as if multiple networks are connected to the a single LAN. In this case, the Service Provider Network is transparent to customer’s LAN segments.

The Metro Ethernet Forum (MEF) is an association of Service Providers and technology suppliers that has worked towards the promotion and standardization of Metro Ethernet solutions, defining the following Ethernet connectivity services:

	Point-to-point **E-Line**	**Multipoint-to-Multipoint** **E-LAN**
Port Based Service	Ethernet Private Line	Ethernet Private LAN

No Service Multiplexing Dedicated Bandwidth	EPL Most widely deployed, simplest to deliver, can be offered with strong SLA	EPLAN
VLAN Based Service Service Multiplexing Shared Bandwidth	Ethernet Virtual Private Line EVPL	Ethernet Virtual Private LAN EVPLAN

Figure 1.1 – Ethernet Connectivity Services as defined by MEF

Electrical Power Utilities employ all the described provisioning modes for Ethernet connectivity:

Local Area Ethernet in HV substations and in Control Centres is typically implemented through copper wire and optical fibres. The intrinsic EMC immunity of the optical fibre and its galvanic isolation render this medium particularly attractive for local networking in the substation, leaving the copper wire essentially for cabinet backplane connections.

Similarly, when short spans are to be covered, between different voltage level substation control buildings, or between the Control building of the substation and annex buildings, optical fibre is the preferred medium.

Ethernet over SDH is the most common provisioning method for SCADA and IP voice connectivity, requiring the establishment of Ethernet connections for inter substation communication as well as from the HV substation to a Central platform (Load Dispatch Centre, etc.).

Emulated Ethernet is mainly a way to replace previous “Leased lines”. The migration of operator infrastructures to IP/MPLS, is an example of this replacement strategy. However, it should be noted that Emulated Ethernet is generally not suitable for the time-sensitive operational applications due to poor latency and jitter performance.

It is therefore normal to find the three provisioning modes, local area Ethernet, Ethernet over SDH and emulated Ethernet, at different parts of the Power delivery system.

1.4 Benefits

Replacing Legacy Data interfaces in the substation by Ethernet ports presents the following benefits:

- ⇨ Single interface replacing many different functional, electrical and mechanical interfaces for data and voice circuits used in the electrical power environment (RS-232, RS-422/V.11, RS-423/V.10, RS-485, X.21, G.703, etc). This interface standardization results in reduced engineering and coordination effort, reduced documentation requirements, reduced spare parts, and no interface converters.
- ⇨ Low cost of connection point – RJ45 is the most economical connection point well below any other data interface (connector, patch cord, port hardware, network hardware).

- Bit rate flexibility – All interfaces are at the same bit rate. The throughput at the interface and across the network is soft controlled and can be modified without changing any physical boards or channel reprogramming across the network.
- Fibre isolation – Spans of cable that require galvanic isolation or electromagnetic immunity can be implemented in optical fibre without any external electro-optical converters.
- No Protocol conversion and transcoding – Knowing that at the central node, generally it is required to connect into a platform on an Ethernet LAN, direct Ethernet interfacing at the substation end avoids protocol conversions.
- Easy implementation of Back-up control centre routing – No junction splitters required for broadcasting data to two different destinations.
- Stable and standard protocol – Ethernet is the most dominant standard in the networking industry. Its widespread use guarantees its availability for a very long time.
- Transmission span – Ethernet allows much longer separation between the application equipment and the network equipment than any of the legacy data interfaces that it replaces.
- Strong industry support – Ethernet technology is available from a large number of suppliers with continuous development (switching, speed, fibre, wireless, ...) both at the supplier end and at the standardization end.
- Extensive topological flexibility – Through the use of Ethernet switches it is possible to adapt to any topology and environment constraint.

Replacing Leased Lines by Metro Ethernet service is mainly driven by the abandonment of transparent leased line services, as the Telecom Service Provider infrastructure moves from Time Division Multiplexing to IP.

Despite certain issues concerning its performance for critical services it presents the following benefits:

- Ethernet service constitutes a “less expensive” alternative than Leased Lines
- More efficient use of resources – The packet nature of the Ethernet service as compared to the permanent circuit nature of the Leased Lines allows the use of the network’s available capacity in a more efficient manner.
- More efficient bandwidth procurement – The procured capacity corresponds to the immediate requirements of the customer application. As the upgrade process is extremely simple and immediate, the customer does not have to dimension his connection according to future requirements.
- Ability to upgrade bandwidth quickly – the bandwidth allocated to each user is independent of the physical interface. Bandwidth upgrade does not therefore require a technician’s visit to change the physical interface at the customer premises. It can

be performed by the service provider through soft configuration upgrade increasing the allowed throughput for the customer. The time for change is therefore minimal.

- Fast and easy deployment of new applications – Ethernet is the standard interconnection mode for almost all new applications. Providing Ethernet service instead of several different data interfaces previously used on Leased Lines allows the elimination of functional, mechanical and electrical incompatibilities, time consuming interface coordination and the requirement for interface converters.

1.5 Business Implications

- The large majority of existing substation equipment is still "Serial Data" interfaced. The change of equipment in the substation with Ethernet /IP connectivity is a major business decision with time and cost implications.
- The Migration into Ethernet connectivity necessitates long-term planning with coexistence of legacy and new technologies across the network and in some substations.
- Knowledge & Expertise management – The type of required expertise changes radically when migrating the system to Ethernet. From the traditional interface engineering efforts of the non-networked system leading to a great number of different interface types and interface conversion devices, the effort and expertise evolve towards Traffic capability coordination and Performance Engineering. This new knowledge is generally absent in Electrical Power Utilities and requires investment in staff training.
- Increased Security issues – Network connectivity in the substation introduces security risks which were non-existent before the introduction of wide area network access. Therefore introducing Ethernet connectivity to the substation must be accompanied by appropriate Security barriers and intrusion detection.
- Qualitative change regarding communications with the HV substation – Ethernet connectivity shall facilitate the addition of new services in the substation without hardware modifications. This will enable a greater flexibility of new service implementation without much input from telecom providing entities, in particular those in relation to the "operation support" activities (e.g. On-line Asset monitoring, etc.)
- Business / Operational uniformity – The convergence of technologies, expertise, and maintenance know-how across the different activities of the Electrical Power Utility may be a factor of organizational convergence between IT and telecom and/or operational and corporate sections of the utility.
- Technology Lifecycle – The much faster rate of evolution of the concerned technology may lead to a shorter time period for substation refurbishment projects and new types of refurbishment contracts with a more continuous upgrade process (switching, speed, fibre, wireless, ...)
- Unity between Local and Wide Area Networking – The uniformity of technologies and expertise may lead to organizational change in the Electrical Power Utility.

1.6 Cost Considerations

It is commonly agreed that at present 98% of all data traffic in all enterprise starts and ends on an Ethernet port. The extensive use of Ethernet in general data and voice communications has drastically reduced the cost of connection and network components and has made its use extremely cost effective.

The generalization of IP networking in the office and the arrival of High speed Internet at home mainly through existing copper wires and ADSL technology, as well as the migration over IP of fixed line telephony and more recently the TV have lead to the introduction of Ethernet connections into almost any piece of modern electronic equipment and the movement is still in progress. From a connection cost of a few thousand dollars in the past, the present day Ethernet PC card represents an extra cost of a few tens of dollars. Today it is actually more costly to use serial communications adapters than Ethernet adapters and Ethernet is typically 100 times faster.

Cost advantage is not however limited to the cost of hardware, connector, patch cord and communication port. The main item of cost saving is related to the cabling, installation design, and interface coordination and conversion.

Moreover, the simplified cabling and interfacing, and in particular the standardization of network interfaces, lead to a reduced cost of network operation & maintenance.

Finally, when data connection is to be performed between one central site (e.g. Load Dispatch Centre) and a great number of outstations (e.g. HV substations), the data aggregation capability of Ethernet allows to arrive in the central site with one network interface rather than individual data ports and associated equipment (modem and transceiver banks). This allows important cost saving in equipment, cabling, and installation effort.

2 UTILITY INDUSTRY CONTEXT AND APPLICATIONS FOR ETHERNET

2.1 Introduction

This chapter presents a brief description of existing and potential data communication applications in the electrical power utility which may use Ethernet.

In the present chapter only a description of applications is given, whereas more details relative to their required data volumes and performance is presented in chapter 9.

Only operational applications relative to the power delivery process have been covered. This includes applications in the HV substation and in the Control Centre, as well as the associated Operation Support applications connecting the Utility office to the HV substation or to the Control Platforms.

Corporate enterprise data networking applications in the Utility office, being very similar to any other large enterprise corporate IT, have not been treated in this document beyond the Operation Support applications of the Utility.

Two important drivers for the migration from point-to-point multiplexed circuits to the network-oriented Ethernet are the TCP/IP SCADA and the new substation automation process through IEC 61850 standard. The concepts and underlying principles are given in the sections 2.3 and 2.4 hereafter.

2.2 Utility Applications

2.2.1 Substation Control

Substation control refers to all information exchange, within the substation or external to the substation, that provides access to substation “real time” operational data, time-stamped or non-time-stamped indications relative to status changes, alarms, measurements of electrical quantities, and commands sent to alter the state of operational equipment. The important applications related to substation control are:

Local Substation Control

Energy Management SCADA

Remote Substation Control

Networking requirements related to these applications are covered through IEC61850 and TCP/IP SCADA and therefore through Ethernet as described in the following parts of the chapter.

2.2.2 Substation Data Analysis

This is data collected and used (generally off-line) either to evaluate events at the substation or to provide confirmation of device configuration.

Event Reports – typically log files and reports generated by an event recorder or historical system which provide information on the change of state of operational equipment

Oscillography File Transfer – typically event triggered fault records generated by a protection device or fault recorder. These may contain digital events and analogue waveforms.

Confirmation of Parameters/ Upload of Setting – data files uploaded to provide information on the actual configuration of a device.

Networking requirements related to these applications are covered through IEC61850 and therefore through Ethernet as described in the following parts of the chapter.

2.2.3 Real Time Protection and Automation

This is data which is transferred between devices in real time to ensure correct protection, operation and substation automation.

Protection and Protection initiated automation – Data and signals used to initiate Circuit Breaker Tripping and high speed reclosure, operating in a timeframe of less than 100ms.

Teleprotection – Data and signals sent to remote substations to accelerate release or block Circuit Breaker tripping. Usually covers the exchange of monitoring and command information to protect operational equipment.

Zone Protection and Wide Area Control schemes – Data and signals required by automation systems that operate across zones of the transmission system on a wide area inter-substation basis.

Low Speed Substation Automation – Data and signals used to initiate intra substation applications, which operate in a timeframe of more than 100ms. Management of outages on distribution networks in real time.

Networking requirements related to these applications are covered through IEC61850 and its future extensions to cover teleprotection and therefore through Ethernet as described in the following parts of the chapter.

2.2.4 Substation Automation Platform Management

This is data required to manage the configuration and performance of the SAS itself. The data types identified are:

Substation Automation System Monitoring Data – Supervision data relating to the operational performance, health and condition of the SAS

Configuration downloading – File transfer of site specific application configuration data files or parameter settings

Networking requirements related to these applications are covered through IEC61850 and therefore through Ethernet as described in the following parts of the chapter.

2.2.5 Commercial Applications

This is data collected for the purpose of energy trading and billing or has an impact on the commercial operation of the utility business.

Revenue Metering – This is time integrated Energy Data at a commercial interface or boundary used for energy charging and billing. Introducing meters as rather inexpensive IP units in a well distributed computer network will give the possibility to increase the precision (density and frequency) of metering resulting in accurate payment for delivered services.

Energy Quality Monitoring – This is data related to agreed quality of service criteria, where energy is transferred at commercial interfaces or boundaries, which could be subject to financial penalties.
The use of Ethernet in these applications is emerging.

2.2.6 Substation Management

This is data collected to monitor plant and equipment condition or relates to environmental factors.

HV Apparatus Health and Performance Monitoring – data relating to plant condition and performance, generally used to indicate maintenance requirements, its duty cycle, capability and loading ability
Weather and environment Monitoring – data relating to substation environmental factors such as temperature and pollution etc., which may be used to influence utility business decisions.
A great amount of this data is at present remaining in the HV substation. Their transfer out of the substation shall necessarily be through Ethernet connection of the substation.

2.2.7 Site Working

This is data required by site personnel in the execution of site related duties.

Safety Information – data used by site personnel to ensure that plant and equipment to be maintained is isolated, secured and earthed. (Tagging)

Online Documentation – data used by site personnel to carry out their tasks at the substation (e.g. maintenance manuals and schedules, drawings and plans). Documentation is an essential base for efficient management of utility infrastructure. Pictures and video add particularly useful information in the dispersed environment of the power delivery system. These applications require a broadband network in order to meet an acceptable time performance. The introduction of inexpensive GPS equipment and commercial mapping applications makes Geographical Information Systems (GIS) an important tool for field based maintenance personnel. Connecting to maintenance applications in the substations and downloading accurate maps, pictures and work orders may effectively economize time.
However, the use of GIS and increasingly automation of data acquisition of power line infrastructure (e.g. laser scanning) leads to heavily growing data volumes and the need for scaleable ICT infrastructure.
If Security Tagging is not yet accepted to be “virtual”, the requirement for on-line documentation is very well identified. The use of networking is to be coordinated through the Security policy of the Power Utility.

2.2.8 Security Applications

Data required to visualize and to prevent threats to the physical substation and unauthorized access.

Video-surveillance – Surveillance of unmanned substations and even manned stations during the night have become increasingly important due to danger from sabotage and the possibility of damage from high voltage installations to the public (authorities demand). Traditional video surveillance equipment based on proprietary solutions has been, and still is, rather expensive. Introducing rather inexpensive, semi intelligent IP based cameras opens a new road to better control of the exterior border of substations.
Surveillance cameras using Video over IP are widely being used. Ideally High Definition video would be necessary in order to provide the necessary resolution, however, the traffic volume makes these systems very difficult to implement in a generalized manner.
Video-surveillance can also be used for remote "visual" verification of grounding for work in the substation or on the power line as required by safety regulations and infra-red camera systems may be employed as a means of condition monitoring for certain substation assets.

Access Control – data relating to potential threats to the substation communication systems and general configuration data which must be prevented from disclosure, modification or destruction.
IP networking is the appropriate way to deal with these applications.

2.2.9 Substation Operational Voice System

The implementation of the Operational hotline telephone in the HV substation is evolving into IP telephony and therefore it becomes an Ethernet transported data service.
Switched Telephone networks incorporate IP telephony as a consequence of switch technology change, network change and also in the objective of cost reduction and new features (e.g. connection to mail systems and calendar systems). QoS control and VPN techniques (or even physical separation) mechanisms may be employed in order to ensure separation from other communication services.

2.2.10 Collaborative Multi-media Communications

The possibility to distribute office applications like mail, word processing etc and ERP solutions like project control and time registration will increase the efficiency in local branch offices. IT-support may be effectively administered from a corporate central site or even be part of the decentralized organization.

Presence of Ethernet and IP in substations and given sufficient capacity and efficient compression technology the network will serve as useful video conference system. The increased focus on energy saving and CO2 reduction is encouraging the reduction in travelling thus supporting solutions for remote administration.

2.3 Substation Automation Process – IEC61850

2.3.1 Introduction to IEC61850

The *scope* of the standard IEC 61850 is to support the communication for all process oriented functions being performed in a substation. The *goal* of the standard is *interoperability*, i.e. the ability for IEDs from one or several manufacturers to exchange information and use the information for their own functions.

The standard IEC 61850 supports the *free allocation of functions* to Intelligent Electronic Devices (IEDs) and, therefore, supports any kind of system philosophy covering different approaches in function integration, function distribution, and Substation Automation architecture.

The standard contains an object-oriented *data model* that groups all data according the common user functions in objects called Logical Nodes (LN). All related data attributes are contained and defined in these Logical Nodes. The access to all the data is provided in a well defined way by the *services* of the standard, which aim to fulfil the performance requirements.

The data model and services of the standard are mapped to a *mainstream communication stack* consisting of MMS (Manufacturing Messaging Specification), TCP/IP and Ethernet with priority tagging. These services cover the needs of IEC61850 in terms of Intra-station communication.

With the ongoing extension of the IEC61850 standards for *Inter*-Station communication (between two or several Sub-stations) and communication towards the Network Control Centre, WAN networks are being developed. LAN traffic with time critical IEC61850 content can be transported, in most cases, over the already existing utility SDH-network (→ Ethernet over SDH). This approach allows running traditional services in parallel with IEC61850 traffic while benefiting from technical as well as commercial (→ investment protection) aspects.

The following paragraphs describe the model and mechanisms of IEC61850 as well as the time synchronization issues related to the real-time nature of these applications.

An overview of the performance requirements of the underlying Ethernet infrastructure for the substation communication applications through IEC61850 is presented in section 9.1.

2.3.2 Model & Mechanisms of IEC61850

IEC61850 is currently mainly related to Substation Automation Systems (SAS). A Substation Automation System is a set of inter-connected devices aiming at protecting, supervising and operating the electrical network (e.g., a busbar, a transformer, or a line). In almost all cases, this is associated with a breaker. SAS have been traditionally implemented as either centralised or distributed architectures. Centralised systems are generally electrically hardwired or use serial communications to connect the data acquisition units. More recent SAS are implemented with dispersed IEDs which are connected using either a proprietary communication network or a network based on an industry standard. The current recommendation for SAS communications is IEC 61850. One of the main drivers for this suite of standards is to have a unified SAS-architecture and interoperability of IEDs of different brands.

The IEC 61850 standard was focused on the SAS topology, which considers the interconnection between IEDs at substation level, using standardised local area networks

(LANs) and defines object models for substations and feeder equipment. This allows the standardisation of different devices and equipment at the substation, defining a new automation architecture.

The IEC 61850 standard supports the substation automation functions by the communication of sampled values (SV), fast exchange of I/O data for protection and control, control and trip signals, engineering and configuration, monitoring and supervision, control-centre communication, time-synchronisation, etc.

The IEC 61850-7-xx parts explain how the abstract services and models are mapped to concrete communication protocols as defined in IEC 61850-8-1 and as is shown in figure 2.1 The data transmission between IEDs are accomplished through different types of messages, such as GOOSE (Generic Object Oriented Substation Event) which are used for transmission of critical events in real time (such as tripping, commands to operate) and sampled values (SV), which are encapsulated and transmitted over Ethernet. All other information within the substation is transmitted by means of communication messages between the logical nodes that constitute the functions. The messages are based on simple communication services provided by the MMS (Manufacturing Messaging Specification) protocol. Underlying the application level with MMS the model uses TCP/IP as transport and network protocols.

Figure 2.1 shows in a simplified way the 7 – layer OSI reference model for the Ethernet / IP based application. GOOSE and SV messages go directly to layer 2 (Ethernet link layer) to avoid time consuming TCP/IP processing.

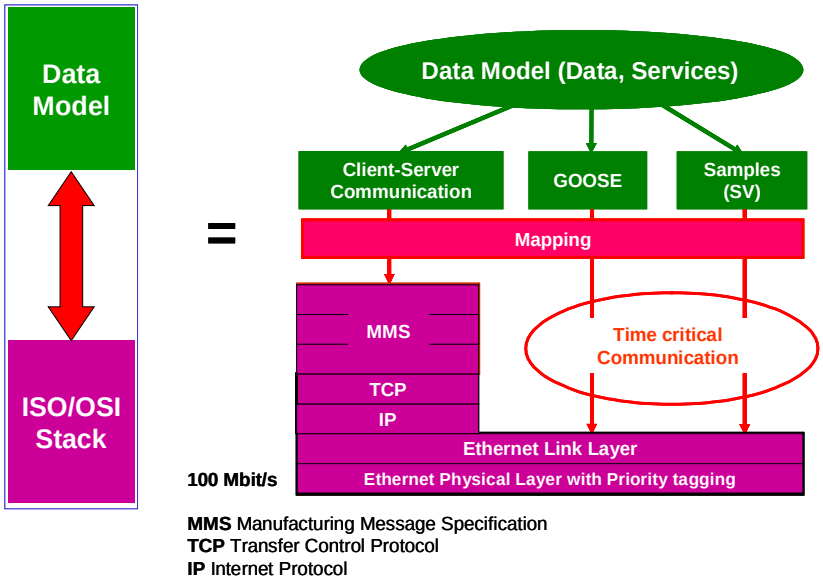


Figure 2.1 – IEC 61850 Communication model

The IEC61850 communication services can be grouped into two general kinds of communication (see figure 2.2): Vertical and horizontal communication. Vertical communication in Substation automation is that which takes place between station and bay level devices. Vertical communication services are designated by IEC61850 for reading or writing data, for control and monitoring applications, including file transfer. These are mapped

on MMS (ISO9506) over TCP/IP. Control services are using acknowledged services on application level. Monitoring services rely on TCP/IP data integrity.

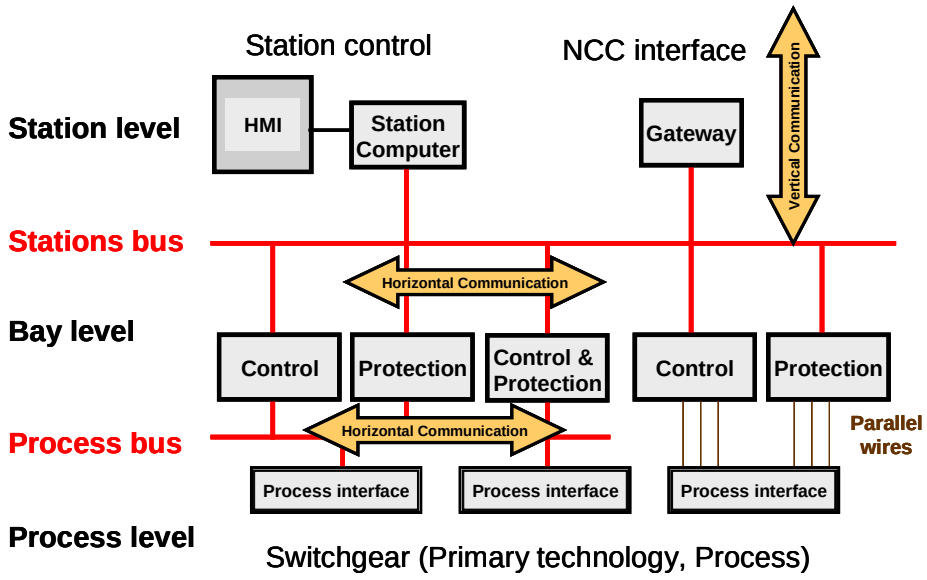


Figure 2.2 - Horizontal versus vertical communication

With “Horizontal communication” in IEC61850 we are talking mainly about the Generic Substation Event (GSE) model for exchanging time critical data (messages) between two or more IEDs using Ethernet multicast (see Fig.2.2, on bay level). The GSE service model of 61850- 7-2 details fast and reliable system-wide distribution of input and output data values. This GSE service uses a specific scheme of retransmission to achieve the appropriate level of reliability.

Sampling and digitisation voltage and current measurement is defined in the standard to replace traditional I/O wiring. Protection IEDs base their decisions on current and voltage samples, measured by current and voltage transformer IEDs. A loss, or even a delay, bigger than 4ms between two consecutive samples prevents IEDs from functioning correctly.

Sample exchange can be basically seen as vertical communication. However, these samples are sometimes also distributed horizontally within the substation. An example would be the so-called bus bar voltage used to trigger protection relays. These samples have to be measured with a frequency of typically 4 kHz and have to be transmitted cyclically with a frequency of 1kHz. Since typically more then one IED requires the measured values, MAC layer multicast addressing is used. Within a substation typically 30 to 60 IEDs are transmitting these samples leading to a high rate of multicast load in case of just a single common network.

2.3.3 Time synchronisation for substation automation

The IEC61850 standard specifies Simple Network Time Protocol (SNTP, RFC 2030) for time synchronisation, considering the inclusion of IEEE 1588 in a future revision. There are different performance classes, which are used for different Substation Automation functional requirements on time tagging as shown in Figure 9.3 in section 9.

Traditional SNTP implementations are mostly based on time stamping of incoming and outgoing SNTP time packets in the SNTP application layer (which is above UDP layer). The accuracy that can be achieved adhering to such a time stamping scheme is not very good (~1ms). To meet the substation automation requirements (IEC class 2 or better) it is possible to do time stamping at low level in both the SNTP client and server. Note that this is considered to be an implementation issue and therefore is not in conflict with SNTP as such.

SNTP specifies time distribution based on both unicast and broadcast methods. However, IEC61850 proposes that only unicast time synchronisation will be used, i.e. the “time client” controls the interval between two time requests. Since the accuracy is decreased by differing transmission times the accuracy is improved if the number of hops between the time server and the IED is as small as possible. In contrast to SNTP, according to IEEE 1588 the timeserver initiates the time update. In principle both approaches promise to reach the same level of accuracy.

2.3.4 Further Extensions

IEC61850 is introduced at substation level, but is being extended for communication between substations and between substation and control-centre.

Whereas the timing requirements under normal operating conditions can be achieved within a substation, much more care has to be taken when designing WANs. Considering messages like GOOSE to be transmitted for distant protection purposes, one has to be able to guarantee QoS including deterministic timing for such services, even under adverse network conditions. An available technology for WAN applications is therefore Ethernet over SDH, which can provide the needed QoS characteristics (see also chapter 5).

In future synchronisation of IEDs will be governed by IEEE1588v2 which will improve the precision of clocking when compared to the existing SNTP protocol. This will necessitate the addition of specific synchronization hardware.

2.4 SCADA and ICCP related Utility communication characteristics

2.4.1 Overview of EMS/SCADA Communications

Electrical power system SCADA and the Load Dispatch Centre's Energy Management platform are some of the most important and well established applications of Ethernet communications in the operational environment of the Electrical Power Utility.

EMS/SCADA protocols have been the subject of dedicated CIGRE Technical brochures and their brief coverage here is only for the purpose of better understanding of the context of use, and the related constraints of the underlying Ethernet infrastructure.

Several levels of local and wide area Ethernet connections can be distinguished across the network, as presented in figure 2.3, with different inter-networking strategies related to security and data exchange constraints. It should be noted that depending upon the adopted architectures and technologies, some of the described levels can be merged together.

- **Substation RTU to the SCADA Platform** – A first level which is developing quite fast is related to TCP/IP based connection of the substation RTU to the SCADA platform in the Control Centre. The RTU may be natively operating with a TCP/IP protocol stack and interfaced to the network through an Ethernet connection (IEC60870-5-104) or through a Terminal Server encapsulating Serial data from legacy RTU as further discussed in section 10.12.
- **Front-end LAN** – This level allows the connection of all substation RTU communication channels to communication front-end servers. It is generally a local network confined into the Control Centre but can also be distributed among a number of SCADA access points, in particular when a back-up Control Centre exists in the network.
- **SCADA LAN** – This level allows the EMS servers to access to the different substations through the communication front-end machines and the dedicated workstations to access the servers. It is generally localized in the Control Centre but can also be extended to a back-up Control Centre or to a remote workstation across the network.
- **Inter-Control Centre interconnections** – Individual Servers in the Control Centre or the platform as a whole require direct high speed connections to back-up facilities (e.g. for database synchronization), to other Control Centres (e.g. for dispatch coordination), or to other platforms (e.g. for market management applications). These Ethernet based links are generally used to carry traffic through the Inter-Control Centre Protocol (ICCP) standardized as IEC 60870-6 and Telecontrol Application Service Element (TASE-2) protocol. TASE-2 is used internationally for communications between control centres and often for communications between SCADA systems and other engineering systems within control centres.
- **Control Centre Office LAN** – This level concerns non-real-time traffic such as the access of engineering workstations to synthetic data generated or processed in the EMS/SCADA platform. It carries normal office environment data exchange protocols.
- **Public Zone (DMZ)** – This level concerns the processed data which is made available to the outside world by the Control Centre through web-service and must therefore be well

separated from the critical operational world. The data traffic across this network is exchanged using web-oriented protocols.

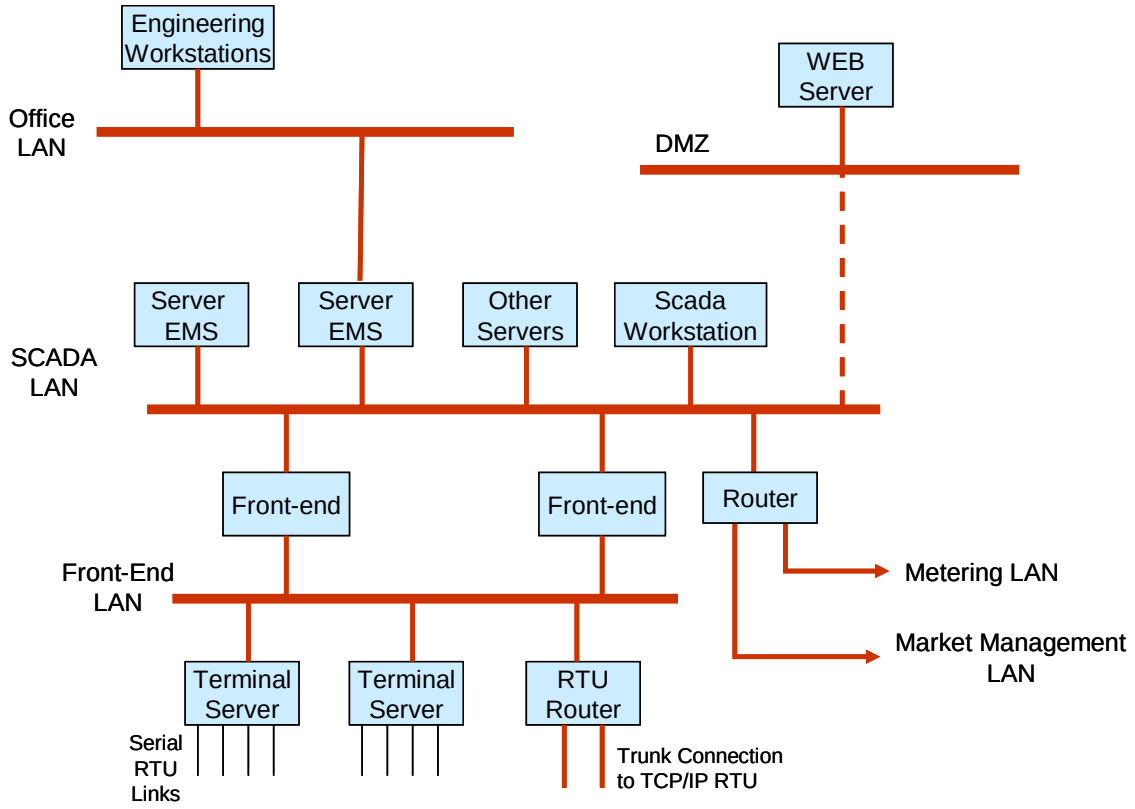


Figure 2.3 – Control Centre Platform Communications

2.4.2 SCADA RTU to Control Centre Communications

Still today, the widest employed communication mode for the substation RTU remains the Asynchronous Serial link through an RS-232 interface. The communication protocol associated to this mode has been standardized as IEC 60870-5-101 (IEC101), although many other protocols are still in use in legacy systems. It is suitable for multiple configurations such as point-to-point, star, multi-drop, etc. The great advantage of Serial link SCADA is its conceptual simplicity when associated to a circuit-based communication system: RTUs have independent circuits and can be backed-up by another circuit with fully separate routing across the network. The major drawback to serial communication for SCADA is indeed its lack of flexibility and the large quantity of independent serial circuits which must be terminated and connected to a Front-end in the Control Centre. This implicates hundreds of RS-232 interface points, associated interface hardware and a great amount of cabling and connectors. Moreover, any change in the organization of the SCADA system, such as the transfer of the Control Centre to a new geographical location or the implementation of a Back-up Control Centre,

shall require tremendous change and a great number of ancillary equipment such as fall-back switches, interface splitters, etc., reducing considerably the overall reliability of the system.

In the late 80s, packet switching protocols were applied to SCADA services essentially to save leased bandwidth in the aggregate links to the Control Centre and also to enhance the flexibility of the system. RTU information was assembled into ITU-T X.25 packets at designated switching nodes using a PAD (Packet Assembler Disassembler) and routed to the Control platform through Virtual Circuits established across multiple packet switches. Similar implementations were made in early 90s using Frame Relay systems.

The principle of replacing end-to-end serial SCADA circuits by packet communication received considerable support with the advent of IP networking leading to TCP/IP based SCADA protocol IEC 60870-5-104, generally called IEC104. The high capacity optical network with modern SDH transmission provides the adequate infrastructure to deploy the required wide area Ethernet connections.

The IEC104 protocol was developed as an extension of IEC101, adapted for use in a TCP/IP environment through an Ethernet LAN interface at 10 or 100Mbps, although the bandwidth allocated to each RTU communications remains often around 10kbps.

The application layer remaining largely unchanged, the amount of process-oriented data to be exchanged does not significantly increase through the use of IEC 104, even if new applications such as RTU-management and SW-updates may momentarily consume more bandwidth than in IEC101.

Moving from Serial link to TCP/IP SCADA communications raises a number of issues that must be taken into account:

- **Latency** – RTU communication is time sensitive and high latency can degrade the overall performance of the SCADA system or even render the protocol completely inoperable through the time-out of the communication servers. Latency problems due to switching and routing infrastructure may be avoided through an appropriate design. It should be noted that the “real-time” requirements of RTU-cycles are generally in the range of seconds, as compared to order of magnitude smaller transmission times across a thoroughly designed SCADA Ethernet/IP infrastructure. The main issue here is therefore the number of intermediate nodes in the routing of SCADA information as well as the time for any encapsulation and concatenation.
- **Path Redundancy and Resilience** – SCADA RTU communications generally require independent normal and back-up communication routes. In an Ethernet/IP network environment, the problem of resilience is generally overcome through inherent IP routing mechanisms (e.g. OSPF routing), and/or through the protection mechanisms of the underlying SDH network (e.g. SDH ring protection). Adequate planning of OSPF-routing areas (to avoid unwanted management traffic and increased re-routing times), and appropriate predefined alternative routes in the SDH infrastructure, allow to keep high reliability and limited transmission times. Duplicated RTU routing independently from the network resilience is indeed possible but should be performed keeping in mind the independence of normal and back-up routes and no common point of failure.
- **Restoration time** – Restoration times in case of failure may be higher than with serial transmission, depending on the selected protection schemes. The original restoration

mechanism of Ethernet, the Spanning Tree Protocol (STP) has a convergence time which depends upon the complexity of the Ethernet mesh and which may be too long for a SCADA system. More elaborate options such as Rapid Spanning Tree (RSTP) reduce this time, and as a general rule, the restoration time must be taken into consideration in the design of the SCADA Ethernet infrastructure. This subject is further discussed in the relevant section of the document.

- **Multi-service integration** – IP networking is generally considered as a multi-service network technology. However, it should be noted that migrating SCADA to TCP/IP does not necessarily allow the integration of additional services (office communications or IP voice services) within the same IP network. To provide the required QoS for a TCP/IP SCADA system, it is recommended to implement specific VLANs with dedicated bandwidth-allocation.

The use of TCP/IP in SCADA RTU communications allows to aggregate bandwidth from groups of RTU, increasing gradually towards the Control Centre, in such a way that only a few Ethernet interfaces are required at the Control Centre rather than the cabling of hundreds of modem-connections towards the front-end processor. Instead of uncounted wires, only few (redundant) LAN-connections are needed and the RTUs are addressed via their IP-address.

Moreover, the use of TCP/IP enhances considerably the flexibility of the SCADA communication system, facilitating the relocation of an RTU or a complete Front-end.

The migration process for a large installed base from existing serial communications to TCP/IP is a major concern in many SCADA systems. This process may be extended over many years, and does not necessarily cover at the same time the replacement of the RTU, its communication interface, the telecommunication infrastructure and the Control Centre Front-end facilities. Moreover, new RTUs dispersed across the network may be TCP/IP while the existing may remain serial linked, up to their programmed end-of-life.

Different implementation strategies generally using Terminal Servers across the network allow to mix serial and TCP/IP SCADA in the same network and to provide for a gradual migration scheme as addressed in detail in Section 10.12.

2.4.3 Inter-Control Centre Communications

Communications between Control Centres is necessary for connection to back-up facilities (e.g. for database synchronization), to other Control Centres (e.g. for dispatch coordination), or to other platforms (e.g. for market management applications). These interconnections have been assured through the Inter-Control Centre Protocol (ICCP) standardized as IEC 60870-6 and Telecontrol Application Service Element (TASE-2) protocol, although earlier protocols such as ELCOM-90 and its multiple adaptations may still be in use in certain older systems.

The primary purpose of Telecontrol Application Service Element (TASE.2) is to transfer data between control systems and to initiate control actions. Data is represented by object instances. The object models and services which are specific to Control Centre operation and applications are found in the IEC 870-6-503. Additional models and services may be defined according to particular requirements.

ICCP uses an underlying transport-service, normally TCP/IP over Ethernet. The required bandwidth for an ICCP link is generally around 2Mbps (E1) provisioned over an SDH network, although lower capacity links (64-128 kbps or even lower) have been in use in implementations where no fibre and SDH capacity is available.

The time constraint for an ICCP connection is of the order of hundreds of milliseconds which rarely constitute a constraint in an Ethernet/IP infrastructure over a digital communication network.

Security is the fundamental issue in implementing ICCP connections. An inadequately protected ICCP connection may form an open door to the control of the nation-wide energy network. Although an in-depth discussion of IT-security is not within the scope of this document, few important standards and their relationship are mentioned in the following paragraph.

2.4.4 SCADA System Security

Even if Security is a topic treated in dedicated Cigre brochures (Ref [6]) and that the specific Ethernet LAN related security aspects are treated further in the document (sections 3.5 and 10.5), it is useful here to make a particular note concerning SCADA system security.

The IEC TC_57 / WG15 has undertaken the development of security standards for various communication protocols such as IEC 60870-5, its derivative DNP, IEC 60870-6 (ICCP), and IEC 61850. These security standards must meet different security objectives for the different protocols, which vary depending upon how they are used. Some of the security standards can be used across a few of the protocols, while others are very specific to a particular profile. The different security objectives include authentication of entities through digital signatures, ensuring only authorized access, prevention of eavesdropping, prevention of playback and spoofing, and some degree of intrusion detection. For some profiles, all of these objectives are important; for others, only some are feasible given the computation constraints of certain field devices, the media speed constraints, the rapid response requirements for protective relaying, and the need to allow both secure and non-secured devices on the same network.

This work is published by the IEC as IEC 62351, Parts 3-6, titled:

- **IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP** (these security standards cover those profiles used by ICCP, IEC 60870-5 Part 104, DNP 3.0 over TCP/IP, and IEC 61850 over TCP/IP)
- **IEC 62351-4: Data and Communication Security – Profiles Including MMS** (these security standards cover those profiles used by ICCP and IEC 61850)
- **IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0)** (these security standards cover both serial and networked profiles used by IEC 60870-5 and DNP)
- **IEC 62351-6: Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles** (these security standards cover those profiles in IEC 61850 that are not based on TCP/IP – GOOSE, GSSE, and SMV)

The interrelationship of these security standards and the protocols are illustrated in Figure 2.4.

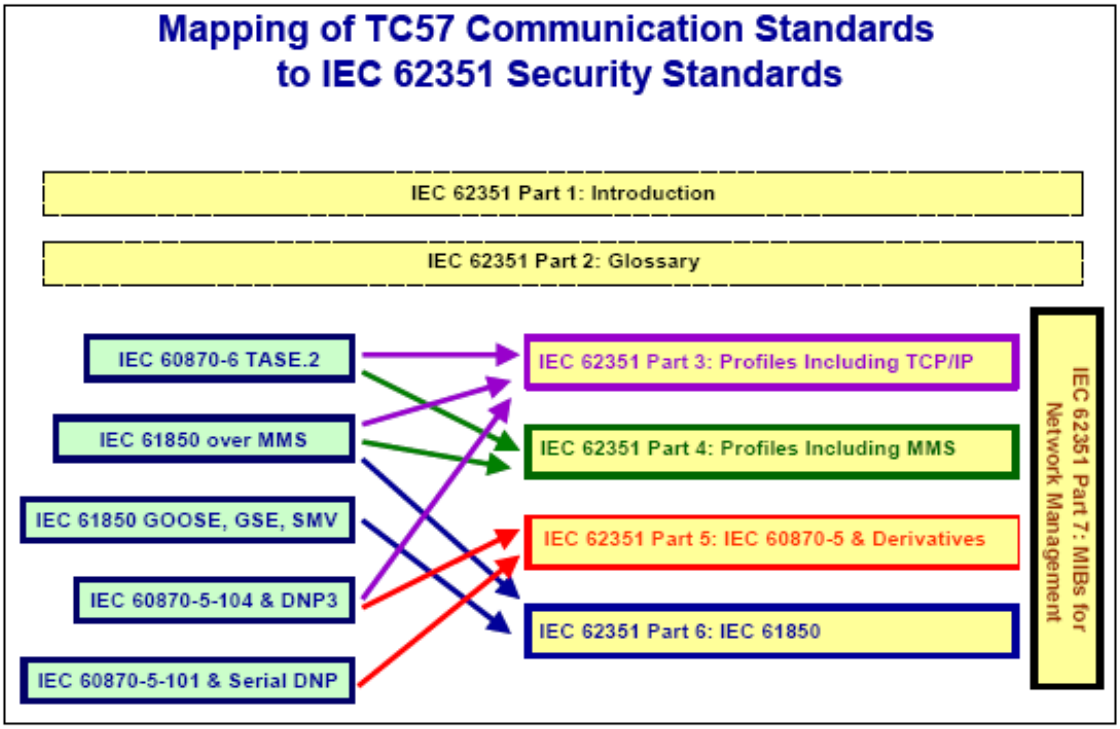


Fig 2.4 - Mapping of communication standards to IEC 62351-xx

3 NETWORK TECHNOLOGY DESCRIPTION

3.1 Concepts and Definitions

3.1.1 Topology: LAN, MAN and WAN

A Local Area Network (LAN) is a network covering a room or a building. Modern optical transmission interfaces allow LAN to be extended to a group of buildings.

The transmission of information amongst host devices, computers, Intelligent Electronic Devices (IED), etc. is carried out using a shared communication point-to-multipoint media which provides intrinsic broadcast of information. Every terminal connected to a LAN requires a unique address identifier in order to maintain point-to-point communication in a shared medium.

A Metropolitan Area Network (MAN) is a network spanning a city. MANs are typically based on Fibre Optical links forming a ring topology. A MAN is used to interconnect several LANs.

A Wide Area Network (WAN) is a network covering a broad area which may include a region, one or several countries or even the whole planet like the Internet.

A WAN normally has a large number of nodes connected with a variety of transmission technologies forming a complex topology. In most cases, it is necessary to have a network layer (normally IP) to manage the topology. Large WANs are generally implemented using a hierarchical architecture which combines several technologies in order to optimise cost and performance.

3.1.2 Layer 2 networking

A layer 2 network is network formed by a limited number of physical devices connected by means of a communication medium able to provide full connectivity. The communication media can be formed by a bus implemented by physical wires, a point-to-multipoint radio, a satellite system, or an Ethernet LAN.

A layer 2 network based on Ethernet technology is a network formed by Ethernet switches and bridges able to forward Ethernet frames to its destination host thus providing Ethernet service in all of its access ports. This working principle is not following the classical ISO 7-layers model which states that layer 2 is responsible for the link transmission of information, that is to say, its scope is the control of the links between network nodes whereas layer 3 is the responsible for finding the route to the final destination port and deliver the information throughout the network.

Layer 2 networks do not have routing procedures. There is no need since Layer 2 networks provide broadcast to all its members. Nevertheless, Ethernet switches provide mechanisms to find where every host is connected and therefore deliver the frames to its right destination without using broadcast forwarding. This mechanism is not based on the routing principles but on dynamic Address Resolution Protocol (ARP) table built from the switched traffic. Those frames addressed to unknown destinations are broadcasted to all the destinations. Every time an Ethernet switch receives a frame with a new address, this address is automatically added to the ARP table so that, as traffic is forwarded, spontaneous broadcast decreases.

Layer 2 addresses are randomly assigned. Unlike layer 3 addresses, they do not identify the location where the host is connected. They are just used to identify the Host. Due to the random distribution of Ethernet addresses, the address of every host has to be stored in every Ethernet switch and therefore, it is not possible to implement a routing procedure like in layer3.

Layer 2 networking is a cost-effective approach that presents some scalability limitations mainly due to the random address allocation and the lack of routing procedure. Due to this reason, a large WAN usually requires a backbone and more scalable assignment capability.

3.1.3 Differences with Layer 3 IP network

Traditional network layer packet forwarding relies on the information provided by network layer routing protocols (for example, Open Shortest Path First [OSPF]), or static routing, to make an independent forwarding decision at each hop (router) within the network. The forwarding decision is based solely on the destination unicast IP address. All packets for the same destination follow the same path across the network if no other equal-cost paths exist.

Routers perform the decision process that selects what path a packet takes. These network layer devices participate in the collection and distribution of network-layer information, and perform Layer 3 forwarding based on the contents of the network layer header of each packet.

Layer 2 (LAN or WAN) switches cannot be involved in the Layer 3 packet forwarding decision process. In the case of the WAN environment, the network designer has to establish Layer 2 paths manually across the WAN network. These paths then forward Layer 3 packets between the routers that are connected physically to the Layer 2 network.

3.2 Networking architecture

3.2.1 Bridging

Bridges operate by examining MAC layer addresses, using the destination and source addresses within a frame as a decision criterion to make their forwarding decisions. Operating at the MAC layer, bridges are not addressed, and must therefore examine all frames that flow on a network. Because bridges operate at the MAC layer, they in effect terminate a collision domain. That is, if a collision is detected upon one port of a bridge, it is not propagated onto any output port. This means that a bridge can be used to extend the span of a LAN.

3.2.2 Switching

To put microprocessor technology into hubs can be considered as the first step in the development of switching hubs, which are now more commonly referred to as LAN switches.

There are several basic types of LAN switches, with the major difference between each type resulting from the layer in the OSI Reference Model where switching occurs. A layer 2 switch looks into each frame to determine the destination MAC address while a layer 3 switch looks further into the frame to determine the destination network address. Similarly, a layer 4 switch looks even further into each frame to focus upon the transport layer header.

Depending upon the software that supports switch operations a layer 4 switch may be programmed to make switching decisions based upon two or more criteria, such as destination IP address and port number. Thus, a layer 2 switch operates at the MAC layer and can be

considered to represent a sophisticated bridge while a layer 3 switch resembles a router. In comparison, a layer 4 switch that uses multiple metrics in determining where to forward frames could function as a traffic load balancer.

3.2.3 Virtual Networking

Virtual Networking allows network connections to share common physical media with other data while remaining logically isolated to and from other users. Virtual Networking can be set up at different levels in the OSI layer model, from layer 1 to layer 3 or higher.

Virtual LANs or VLANs (IEEE 802.1Q) are the most common mechanism used over layer 2 (Ethernet is a layer 2 technology). Upper layer technology Virtual Private Networks (VPN) such as IPSec and TLS/SSL can also be implemented.

The main advantages are the following:

- Scalability – Once the network is in place, it can be easily expanded to other sites or higher capacities by just contracting new capacity from public network operators.
- Lower cost compared to private or leased communication services, because infrastructure maintenance costs are much smaller.
- Simplified network topology – Virtually connected LANs can be seen as a single network from the end user / application perspective.

In order to guarantee the security in the virtual networks, there are two concepts that must be taken into account:

- Authentication, to validate that only authorized and trusted users can gain access.
- Encryption, in order to make the traffic secure for any potential eavesdropper in the public section of the network.

In the present brochure, the focus being Ethernet technology, only Virtual LAN (VLAN) shall be described further.

A VLAN is a logically separate Ethernet network that shares cabling and equipment infrastructure with other VLANs. Each VLAN on a network has its own broadcast domain, meaning that Ethernet frames from one VLAN will not be transmitted onto another VLAN. This restricted broadcast domain provides a powerful security mechanism; users and IEDs on one VLAN cannot communicate with other VLANs unless a router is deployed to route between the VLANs. The router then becomes a central location for administering security policies for inter-VLAN communications.

The IEEE 802.1Q standard defines a 4-byte extension to the Ethernet frame header that allows traffic from one VLAN to be distinguished from another VLAN as shown in the following figure 3.1.

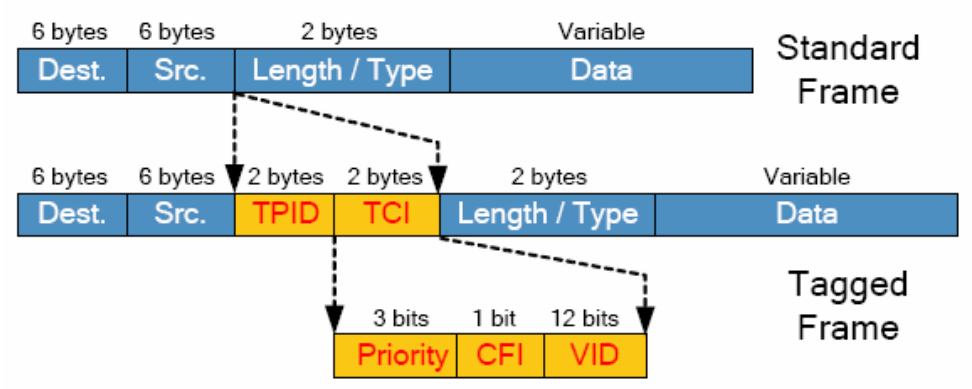


Figure 3.1 – VLAN identification through tagging

The VLAN Identifier (VID) is a 12-bit field that allows 4096 different VLANs to exist on a single LAN. Frames in a VLAN-enabled network will have both tagged and untagged traffic present. Trunk ports that interconnect switches have all frames tagged. Edge ports that connect IEDs and PCs to the network have untagged frames or frames assigned to its VLAN. The exceptions to the latter are Generic Object-Oriented Substation Event (GOOSE) and Sampled Measured Value (SMV) frames issued by IEC 61850 IEDs.

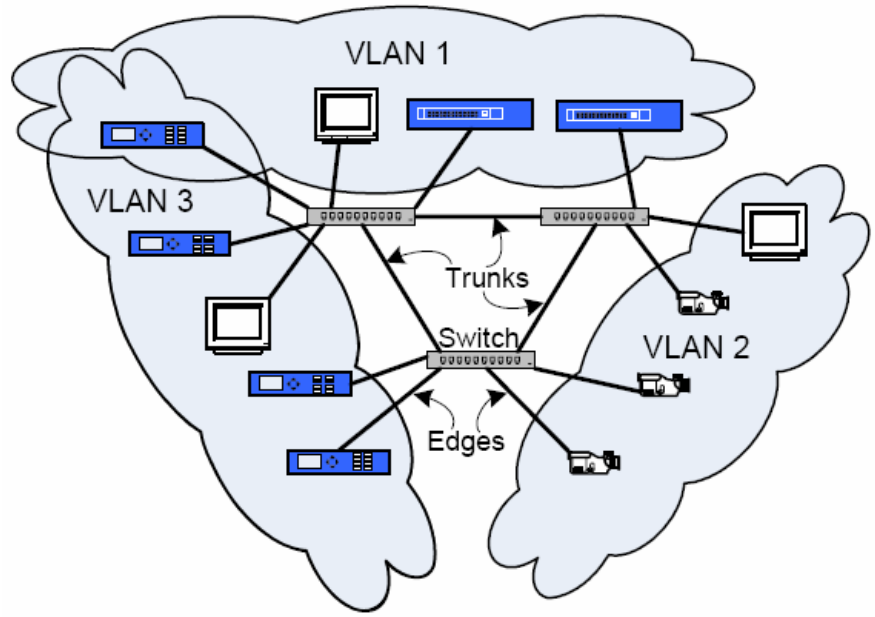


Figure 3.2 – Ethernet network architecture with multiple VLANs

Q-in-Q Functionality

The original IEEE 802.1Q VLAN definition allows only 4096 VLANs to be created (12 bits). To expand the VLAN space 802.1Q-in-Q consists on stacking the VLANs. In this way, every tagged Ethernet frame can be tagged again. This technology enables the possibility to perform

advanced traffic management policies, such as fine QoS classification, while maintaining all the security and integrity associated with VLANs using inexpensive equipment.

The figure 3.3 compares a normal Ethernet frame with a tagged frame and a double-tagged one (Q-in-Q).

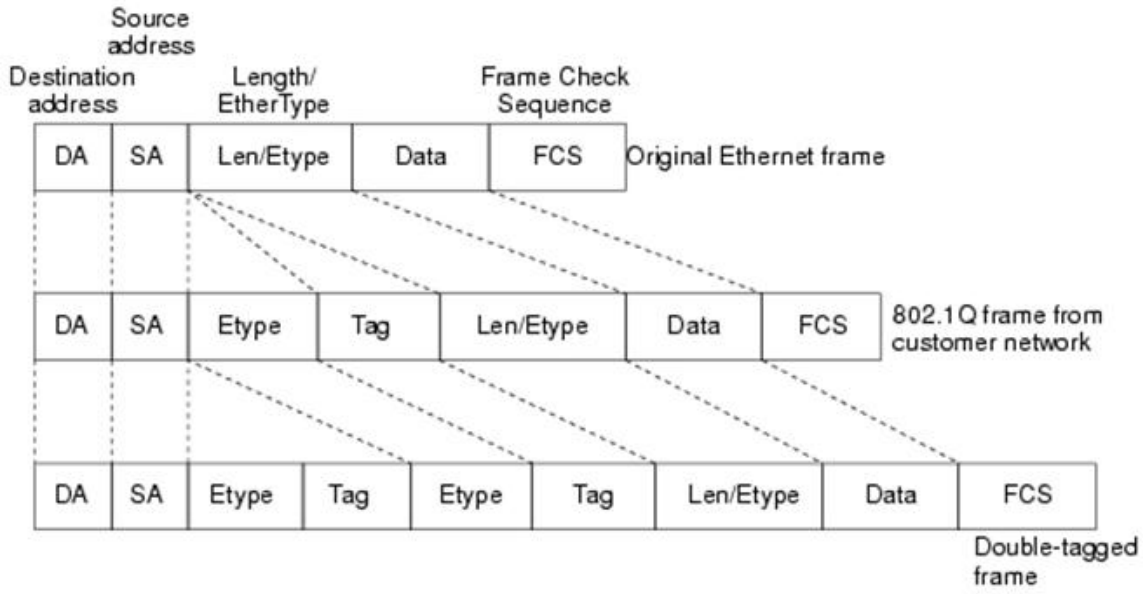


Figure 3.3 – Normal and double tagged Ethernet frames

This feature is widely used and has many applications for the utilities. For instance, the first (outermost) VLAN tag may identify traffic coming from different locations (e.g. a substation A, substation B…), and the inner tag may identify traffic from different services present at each location (telecontrol, timestamping, corporate data access, IP telephony), each one having a different VLAN id and different policies regarding priority, bandwidth assignment, etc.

3.2.4 RPR – Resilient Packet Ring

RPR is a technology optimised to transport Ethernet frames using optical rings. It is a MAC layer technology independent from the physical layer which could be Gigabit Ethernet or SDH, optionally enhanced with Wavelength Division Multiplexing. Unlike Ethernet switches that queue and schedule traffic at every intermediate node, RPR switches introduce the concept of the transit path. Traffic not addressed to the local node passes through automatically without being queued or scheduled. Thanks to this, RPR processes traffic coming in from the ring at line rate. This functionality is based on three basic functions:

- The Add function that insert local traffic into the ring
- The Drop function that removes traffic addressed to local ports
- The Pass function that allows traffic not addressed to the node to pass through it.

This functionality makes the ring behave as a single and continuous medium shared by all the nodes thus providing the functionality of a single Ethernet switch.

Rings have an intrinsic redundancy. RPR technology is being designed to take all the advantages brought by rings including recovery mechanisms that reduce failover periods to less than 50 msec, similar to SDH. The service recovery time is not affected by the number of nodes in the ring.

Ring topology simplifies the implementation of a bandwidth fairness algorithm. RPR takes advantage of the ring continuity to implement a ring-level fairness algorithm that allocates the ring bandwidth as a single global resource. This algorithm dynamically adapts to the changing pattern of the traffic. The MAC entity of every node monitors the use of its links and makes this information available to the other nodes of the ring. Each node can then decide if all the offered traffic can be carried by the ring or some of the traffic sources have to be slowed down to prevent congestion.

A Packet ring presents a natural competence to support Broadcast and Multicast traffic. Every node can receive the packet and forward it around the ring until the packet reaches the source node where it will be removed. Owing to this mechanism, it is possible to broadcast a packet by sending only one copy around the ring.

The advantage of RPR in comparison with a Gbit Ethernet ring is that the RPR ring behaves like a single Ethernet switch providing QoS and fast time-bounded outage recovery.

It can be summarized that the main characteristics of RPR are:

- Ethernet transport provision with full compatibility with IEEE 802 architecture.
- Resiliency by implementing ring recovery mechanisms.
- Adoption of existing physical layers.
- Service classes with QoS provision.

Intrinsic resiliency and guaranteed QoS make this technology especially attractive for Mission-Critical applications like most of the ones used in Power System Control

3.2.5 Provider Backbone Bridging

Provider Backbone Bridges (PBB, according to IEEE 802.1ah, also called Mac-in-Mac) overcome the service scaling limitations based on the QinQ (IEEE 802.1ad or stacked VLANs) implementation in Ethernet networks.

Provider Backbone Bridge has a greater scalability (up to millions of service instances per metro) by physically providing more addressing space in the Ethernet frame.

A PBB device re-encapsulates the QinQ traffic with an outer Ethernet header that includes source and destination MAC addresses of the PBB devices. This will protect provider Ethernet switches from having to learn a large number of end-user MAC addresses. Only the MAC addresses of the PBBs need to be learned. The service scalability is increased by mapping Provider Services inside a 24-bit Service ID (I-SID).

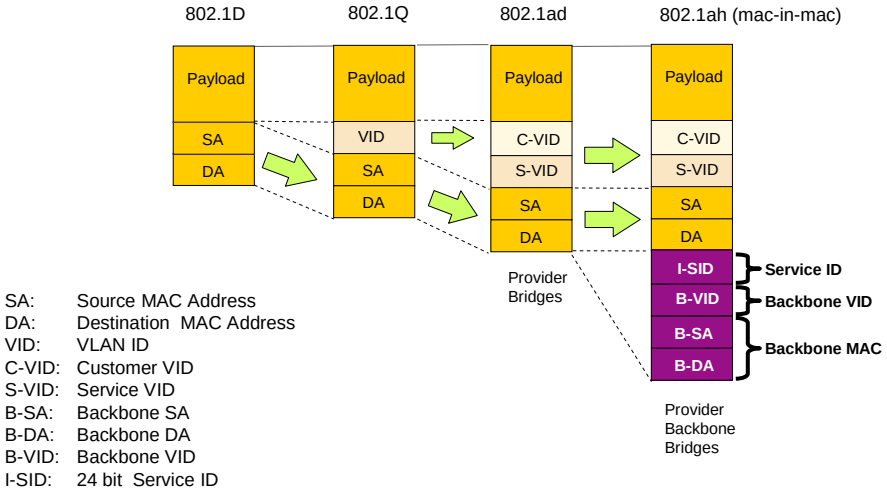
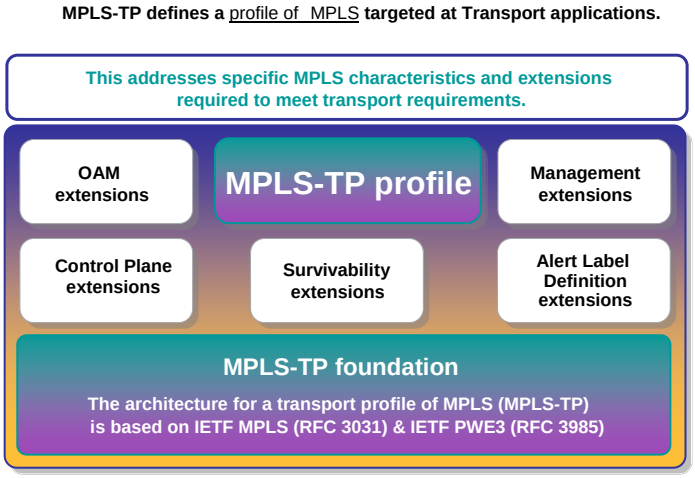


Figure 3.4 Shows Ethernet frame format used in Provider Backbone Bridging

3.2.6 MPLS-TP

MPLS-TP or MPLS – Transport Profile is a profile of Multiprotocol Label Switching (MPLS) defined by a Joint Work Team (JWT) of IETF and ITU-T, designed for use as a network layer technology in transport networks.

The objective is to bring transport requirements into IETF MPLS and extend IETF MPLS forwarding, OAM, network management, protection and control plane protocols. MPLS-TP is based on the same architectural principles of layered networking that are used in longstanding transport network technologies like SDH, SONET and OTN.



3.3 Protection Mechanisms

3.3.1 Spanning Tree

To achieve network redundancy one requires more than one path from source to destination which implies physical loops in the network. However, if a true loop were to occur in an Ethernet network, the first broadcast frame would circulate endlessly, consuming all available bandwidth resulting in a 'broadcast storm'.

The IEEE 802.1D Spanning Tree Protocol (STP) was developed to allow the construction of robust networks that incorporate redundancy while preventing loops. Certain links in the network are put into a backup state so that no traffic may flow across them. The backup links are re-enabled as needed when network problems occur, to restore connectivity of all devices. In this way, the Spanning Tree Protocol forms a logical tree structure spanning all switches out of the mesh or ring topology of the physical interconnection network. At the base of the tree is found the 'root bridge' which is elected by all the switches.

While STP is effective, any link outage causes the halt of all frame transfers until all bridges in the network are aware of the new topology. Using the 802.1D recommended values, this period lasts 30 seconds.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) was a further evolution of the 802.1D Spanning Tree Protocol. It replaced the settling period with an active handshake between bridges that guarantees topology information to be rapidly propagated through the network. In this way, it allows for the creation of fault tolerant ring network architectures that can reconfigure in milliseconds.

RSTP also offers a number of other significant innovations, including:

- ⇨ Topology changes in RSTP can be originated from and acted upon by any designated bridge, leading to more rapid propagation of address information unlike topology changes in STP which must be passed to the root bridge before they can be propagated to the network.
- ⇨ RSTP explicitly recognizes two blocking roles, alternate and backup port roles, including them in computations of when to learn and forward while STP recognizes one state, blocking, for ports that should not forward.
- ⇨ RSTP bridges generate their own configuration messages, even if they fail to receive one from the root bridge. This leads to quicker failure detection but STP relays configuration messages received on the root port out its designated ports. If an STP Bridge fails to receive a message from its neighbour it cannot be sure where along the path to the root a failure occurred.
- ⇨ RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation while at the same time protecting them against loops.

While providing a much better performance than the STP, the IEEE 802.1w RSTP still requires up to a few seconds to restore network connectivity when a topology change occurs. A revised and highly optimized RSTP version is defined in the IEEE standard 802.1D-2004 edition. The IEEE 802.1D-2004 RSTP reduces network recovery times to just milliseconds and optimizes

RSTP operation for various scenarios. Performance of a good RSTP implementation can yield worst case failover and recovery times of the order of 5 ms per switch in the network.

3.3.2 Ethernet Ring Protection

Proprietary ring protection mechanisms have been implemented by manufacturers in order to improve the performance that could be attained by the Spanning Tree and hence to meet the constraints of the industrial automation (50 ms reconfiguration time).

The **Ethernet ring protection** ERP is a protocol to manage Ethernet ring topologies, offering SDH/SONET like protection. It has been pre-published by ITU-T as G.8032/Y.1344 Ethernet Ring Protection Switching.

The main characteristics of the ERP are as follows:

- ⇨ It requires no additional underlying protection mechanism within the ring configuration, the complete functionality is implemented on the line cards of the system and does not require additional dedicated hardware which may raise network complexity and costs
- ⇨ It is a unique robustness functionality which runs on every network element involved in the ring configurations. It means each system is active part of the ring protection mechanism. Therefore it guarantees a maximum of 50 ms to switch over towards a new configuration after link or system failures.

3.3.3 IEC 62439 Parallel Redundancy Protocol (PRP)

The choice of protection mechanisms depends upon the maximum acceptable recovery time (also called the “grace time”) which is indeed application-dependent. IEC SC65C has produced a standard for implementing redundancy in switched Ethernet networks applicable to a variety of industrial local networks, with different solutions depending on the grace time of the plant and on the level of redundancy desired. For the most demanding applications IEC 62439 defines the Parallel Redundancy Protocol (PRP), which is a redundancy method applicable to hard real time systems, based on full duplication and parallel operation of two redundant networks. PRP nodes send on both networks at the same time, and receive from both, providing “bumpless recovery”. In this way, recovery times below 2ms can be achieved using PRP. Duplicate discarding and management functions complement the standard. Details concerning this protocol can be found in reference 4.

3.4 Existing relevant Ethernet standards

The main organization involved in the definition of Ethernet standards is the IEEE 802 LAN/MAN Standards Committee. The purely Ethernet standards, including the Medium Access Control layer (MAC layer) and the different Physical layers are titled IEEE 802.3 followed by one or two alphabet characters, sometimes referred to as the "alphabet soup".

Another group of relevant IEEE 802 specified standards are the IEEE802.1 series which globally define the associated Bridging and Switching facilities (Resilience, Virtual Networking, etc.).

The International Telecommunication Union, ITU-T as the worldwide authority on telecommunication networks has adopted the majority of IEEE standards and a number of new recommendations under the G-series of standards. In general ITU-T recommendations relate to the projection of Ethernet LAN principles to the Metropolitan and Wide Area Networks (e.g. Ethernet over SDH, Ethernet over DSL, etc.).

The Internet Engineering Task Force (IETF) produces documents titled RFC (Request for Comments) which are related to the implementation of IP and MPLS networks and their management. A number of these are relevant to the implementation of Ethernet infrastructures, primarily because the Ethernet infrastructure is used for carrying IP traffic, but also due to the fact that the management of Ethernet infrastructures employs mechanisms defined by IETF (e.g. Simple Network Management Protocol SNMP). Finally, Emulated Ethernet over an IP/MPLS network as used by the Metro Ethernet technology is originally an IETF defined system.

Industrial Ethernet and its constituents, including their electromagnetic and environmental specifications, have been defined by the International Electromechanical Commission (IEC). The Technical Committee TC57 of the IEC has further defined the TCP/IP based SCADA standard IEC 60870-5-104, the Substation Communication standards IEC61850-x and the related Data and Communication Security standards 62351-x, which are based on the usage of Ethernet as the common transport technology. The major performance requirements of an Ethernet infrastructure for Power Utility operational applications must therefore be extracted from these standards.

A Practical guideline has been produced by IEEE PES/PSRC (Power and Energy Society, Power System Relay Committee) focusing on the local usage of Ethernet in the Substation for Protection and Control (reference [5]).

Hereafter is presented a short list of the most important standards related to Ethernet devices. A more detailed description is given in Appendix 1:

- ⇨ Electrical interfaces over twisted copper wire(100Mbps and 1Gbps)
    - IEEE 802.3u 100BASE-TX Fast Ethernet
    - IEEE 802.3ab 1000BASE-T Gigabit Ethernet
    - IEEE 802.3x Full-duplex Flow Control
- ⇨ Network resilience protocols allowing to reconstitute connectivity after a fault
    - IEEE 802.1D Spanning Tree
    - IEEE 802.1w Rapid Spanning Tree

- IEEE 802.1s Multiple Spanning Tree
- IEEE 802.3ad Link Aggregation Control
- ITU-T G.8031/Y.1720 Ethernet Protection switch
- ITU-T G 8032/Y.1344 Ethernet Rings Protection Switching

⇨ Virtual Network definition protocols and their related priority assignments

- IEEE 802.1 P/Q VLAN
- IEEE 802.1p Priority Queues
- IEEE 802.1ad Provider Bridge

⇨ Security solutions at Ethernet layer

- IEEE 802.1x Port and MAC Based Access Control

⇨ Time distribution across an Ethernet network

- ITU-T G.8261 Synchronisation of packet networks

3.5 Authentication & Security services over Ethernet

Connecting the utility corporate network to the substation has its obvious business advantages: access to real-time data; ability to troubleshoot and remedy problems remotely; integration of physical security measures like access control and video surveillance. However, these benefits come at the cost of potentially exposing critical cyber assets to the corporate users at large.

Security is not a set of techniques and devices but rather a process issue and a matter of policy. Implementing a Security Policy must cover such issues as passwords and physical access to equipment. A description of Practices and policies are given as design guidelines in section 10.5. The Electronic Security Perimeter is "The logical border surrounding a network to which Critical Network Assets are connected, and for which access is controlled".

Ethernet on its own provides minimum security from malicious intruders from a larger corporate network perspective. A cyber-security appliance with IP routing, firewall, VPN, and IDS/ IPS (Intrusion Detection/Protection System) functionality is needed to create an "Electronic Security Perimeter" around the critical cyber assets of the substation and/or power system.

3.5.1 Physical port protection

The first level of security is indeed to shut down unused ports. For used ports, there are two main types of physical port protection,

- MAC Based Port Security – It refers to the ability to secure ports on a switch so only specific Devices / MAC addresses can communicate via that port.
- By the standard 802.1x (Port Based Network Access Control) - the ability to lock down ports on a switch so that only authorized clients can communicate via this port.

IEEE 802.1x is the standard for port-based network access control. The standard framework empowers the secure exchange of user and/or device credentials, and prevents any unauthorized network access since authentication is complete before a network IP address has been assigned. IEEE 802.1x operates at Layer 2 or the Data Link layer.

An 802.1x network requires three components to operate:

- A Supplicant – software that implements the client side of the 802.1x standard. The Supplicant is loaded onto the user's device (like PC) and is used to request network access.
- An Authenticator – a component that sits between the external user device that needs to be authenticated and the infrastructure used to perform authentication. Example of Authenticator is a network switch.
- An Authentication Server – a server which receives remote authentication service (RADIUS) messages and uses that information to check the user's or device's authentication credentials.

3.5.2 Authentication & Encryption (RADIUS)

This important functionality provides centralized password management to allow or restrict users to access devices via a particular port. It provides the ability to configure parameters for authorized and authenticated access to the device services (HMI via Serial Console, Telnet, SSH, RSH, Web Server). The access to the switch can be authorized and authenticated via RADIUS server (Remote Authentication Dial In User Service), or using locally configured passwords, that are always related to the username and access level.

4 ETHERNET TRANSMISSION TECHNOLOGIES

4.1 Introduction

The simplest way to constitute Ethernet connectivity with local or limited coverage is to use Unshielded Twisted Pair (UTP) copper wire or optical fibres through the appropriate Ethernet Transceivers incorporated into the Ethernet LAN switches. This is widely used for the Local Area Ethernet in HV substations and in Control Centres, as well as for the connection of Application devices to the communication network.

Currently Ethernet has many varieties that vary both in speed and physical medium used. Perhaps the most common forms used are 10BASE-T, 100BASE-TX, and 1000BASE-T. All three utilize twisted pair cables and 8P8C modular connectors (often incorrectly called RJ45). They run at 10 Mbps, 100 Mbps, and 1 Gbps, respectively. However each version has become steadily more selective about the cable it runs on and some installers have avoided 1000BASE-T for everything except short connections to servers.

The distance to be covered, the required throughput and the environmental constraints are some of the defining factors for the interface type and copper/fibre type. Optical Ethernet interfaces and in particular GigaEthernet can be implemented over a wavelength, sharing in this way the fibre capacity with other traffic through wavelength division multiplexing (WDM).

Fiber optic variants of Ethernet are commonly found connecting buildings or network cabinets in different parts of a building. Their advantages lie in performance, electrical isolation and distance, up to tens of kilometers with some versions. Fiber versions of a new speed almost invariably come out before copper. 10 G Ethernet is becoming more popular in both enterprise and carrier networks, with development starting on 40 and 100 G Ethernet.

Although the currently recommended RF wireless networking standards, 802.11 and 802.16, are not strictly speaking Ethernet, (they do not use the Ethernet link-layer header, use non-Ethernet control and management packets), these wireless systems are also described in section 7. It must be noted that it would not be simply a matter of modulation to transmit Ethernet packets on an 802.11 or 802.16 network, or to transmit 802.11 or 802.16 packets on an Ethernet network

The enhancement in optical transmission technologies have also been incorporated to Ethernet technology. Thanks to this, Ethernet links can work over distances that meet MAN or WAN typical requirements thus becoming another player for the implementation of Metropolitan Area Networks (MAN).

The implementation of a MAN using Ethernet is simply the interconnection of Ethernet switches using medium and long-range optical interfaces. Furthermore, the increased capacity of new Ethernet standards ranging up to 10Gbit/s allows the capacity of the optical fibre to be used thus providing a simpler alternative to other transport technologies. Nevertheless, despite its broadband performance, these new Ethernet standards maintain the same working principle which means that they also suffer from the same technical limitations. In particular, the lack of native Quality of Service support, routing limitations and lack of traffic engineering control.

This section covers the usage of copper wire and fibre interfaces as well the wavelength division multiplexing of Ethernet with other networks over the same fibre. Wireless Ethernet has been covered separately in chapter7.

4.2 Copper interfaces

Copper (or Electrical) interface remains the most used connection point between the Application and the Network, mainly due to low cost, simplicity and remote power (Power over Ethernet POE) capability.

Electrical baseband communication over copper wire is strongly limited in speed (data rate) and distance limiting their potential use. Moreover, electromagnetic induction and coupling problems in copper wire communications necessitate extensive protection requirements and inherent EMC constraints in the harsh electromagnetic environment of power stations and substations. The application of high-speed copper technologies in the power environment requires most careful engineering, in particular when such systems are expected to operate during faults in the primary system as might be the case for protection applications.

Electrical copper wire Ethernet interfaces which are still widely used are as follows:

10Base-T	Basic Ethernet
100Base-T	Fast Ethernet
1000Base-T	Long haul copper UTP (Unshielded Twisted Pair) CAT 5e cable (75m)
1000Base-TX	Long haul copper based on CAT 6 cable (75m)
1000Base-CX	Short-haul copper "twin-axial" STP (Shielded Twisted Pair) cable (25m)

4.3 Fibre interfaces

The intrinsic EMC immunity of the optical fibre and its galvanic isolation render this medium particularly attractive for local networking in the substation, leaving the copper wire essentially for cabinet backplane connections.

Similarly, when short spans are to be covered, between different voltage level substation control buildings, or between the Control building of the substation and annex buildings, optical fibre is the preferred medium.

Gigabit Ethernet is considered as directly usable on optical fibres connecting substations as long as all communication requirements can be covered through Ethernet.

Coloured optical interfaces are available allowing wavelength division multiplexing of Ethernet services with other networks based on other technologies (e.g. SDH).

4.3.1 Optical Gigabit Ethernet Interfaces

Gigabit Ethernet is an extension of the IEEE 802.3 Ethernet standard. Based on the Ethernet and Fibre Channel technology, it increases the speed up to 10Gbps.

Gigabit Ethernet supports various media types. These are defined in 802.3z (1000Base-X) and 802.3ab (1000Base-T).

1000Base-SX	850 nm laser on multimode fibre; ranging up to 500m.
1000Base-LX	1300 nm laser on single mode (5 km range) and multimode fibre (500m range)
1000Base-ZX/-LH	Industry defined SFP interfaces ranging up to 80km. (1550nm laser on single mode fibre)

4.3.2 10 Gigabit Ethernet interfaces

The 10Gigabit Ethernet standard has been driven by the increase in data traffic and the proliferation of new, bandwidth intensive applications, including motion video.

The 10Gbit Ethernet standard is similar to the former Ethernet versions including the same working principles, frame format, etc. The only difference is that it operates only in full-duplex mode. 10 Gigabit standard supports both single-mode and multi-mode fibre transmission media.

Optical 10GbE with XFPs reaches following typical values:

10GBase-SR	850 nm on multimode fibre up to 300m.
10GBase-LR	1310 nm on single mode fibre up to 25km.
10GBase-ER	1550nm single mode up to 40km.
10GBase-ZR	Based on the STM-64 optical interface up to 80 Km.
10GBase-LX4	Based on CWDM interface. Singlemode up to 10 Km.
10Gbase-SW, LW and EW	WAN version of SR, LR and ER using STM-64 optical interfaces. Normally used to transport 10Gbit Ethernet across a Wavelength Division Multiplexing system or network

At the time of preparation of this brochure, new IEEE standards for 40 and 100 Gbps fibre systems are in progress, although wavelength division multiplexing is more stable and cost-effective for Utility applications.

4.4 Optical Networks - Wavelength division multiplexing

Wavelength division multiplexing is increasingly in use in power utility communication networks. In this case, the objective is not generally to increase the transmission capacity per fibre (as for telecom operators) but rather to provide separation between operational and corporate networks, or to provide separation between an Ethernet-based core network (e.g. interconnection of IP/MPLS nodes) and the existing SDH network (or fibre based protection relay links) across the same fibre infrastructure. This is particularly true where extra fibre is not available or cannot be provisioned economically. Typically, Giga-Ethernet over an independent wavelength can be used for the interconnection of main packet nodes, associated to Ethernet over SDH for the connection of other network sites to the core network.
Wavelength division multiplexing can be used in different network topologies as presented in figure 4.3.

4.4.1 CWDM (Coarse Wavelength Division Multiplexing)

CWDM is the low cost technology for multiplexing up to 16 transmission channels in one fibre. CWDM uses frequencies from 1300 nm to 1610 nm with channel space 20 nm (ITU-T G.694.2 and G.695).

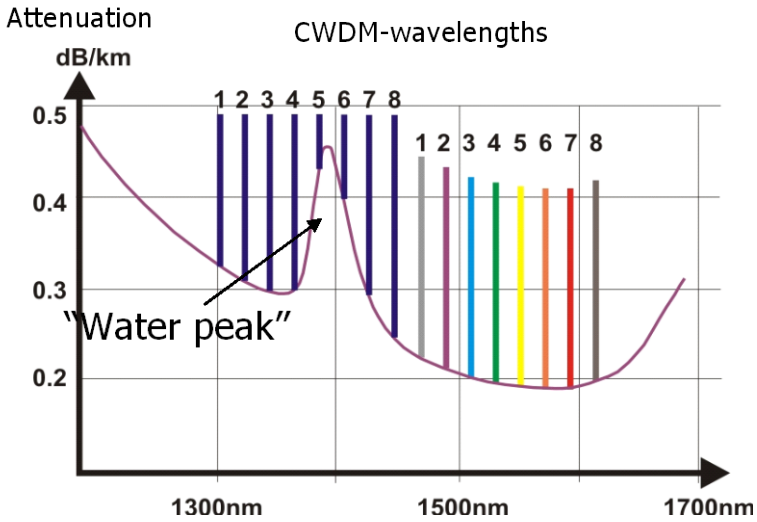


Figure 4.1 - Channel structure for CWDM

CWDM is mainly constructed for cost effective transportation in metro network and can be used in different types of network configurations.

When using all 16 channels, there is a limitation in maximum range of approximately 40 km. Standard fibre type ITU-T G.652 has a high attenuation peak in 1400 nm area. There is a new fibre available on the market that doesn't have this peak in attenuation specified by ITU-T G.656.

Utilizing only 8 channels from 1470 to 1610 nm makes it possible to use transmission lengths up to 100 km without repeaters.

CWDM is available with many electrical and optical interfaces from 100 Mbps Ethernet up to 10 Gbit Ethernet.

4.4.2 DWDM (Dense Wavelength Division Multiplexing)

DWDM is a technology used for multi-channel long distance and/or very high capacity links. A typical DWDM system can be equipped with from 32 channels up to several hundred for one pair of fibres, depending on requirements. DWDM channels are specified by ITU-T G.694.1 ranges from 1530 nm to 1624 nm using 193.10 THz (1552.52 nm) as reference wavelength. At this wavelength the channel space is 12.5 GHz (0,1 nm), 25 GHz (0,2 nm), 50 GHz (0,4 nm), and 100 GHz (0,8 nm) and above.

DWDM is available from several suppliers with different capabilities. Typical DWDM systems transport a minimum of 32 channels, have interfaces up to 10 Gbit/s and span distances ranging from 80 to100 km between repeaters/add drops.

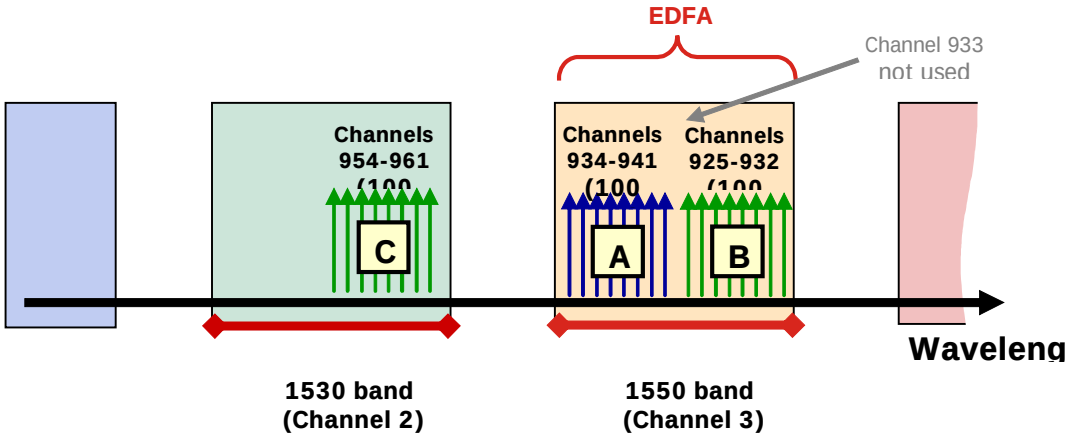


Figure 4.2 - Structure of DWDM channel system

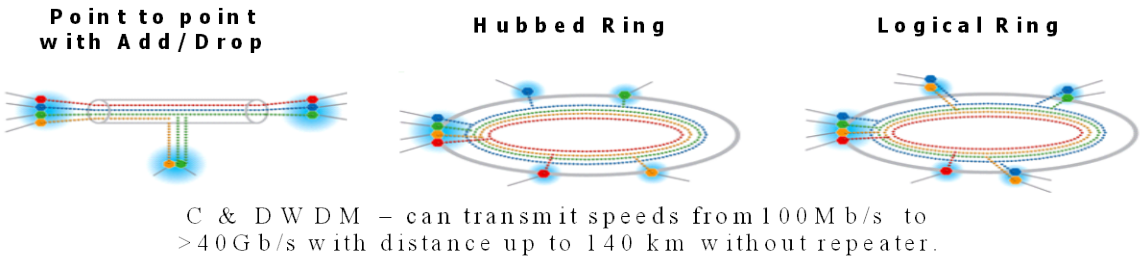


Figure 4.3 - Principles of configuration in a C- and D-WDM network

5 TRANSPORT OF ETHERNET OVER SDH

5.1 Introduction

The SDH as a transport mechanism is a well-proven technology that introduces low delays, and has an efficient, fully standardized multiplexing scheme. Further it provides sophisticated protection-mechanisms and is well suited for a multi-vendor environment. With its ITU-T standardized interfaces, interconnection between metro- / access-networks and backbone for transport over long distances is simple.

But SDH as it was deployed in the 90's with a focus on circuit-switched TDM services did not have mechanisms for sharing efficiently packet oriented traffic in a dynamic way.

Ethernet over SDH (EoS) consists of a set of industry standards that has been developed for more optimized mapping and control of Ethernet traffic over SDH. Collectively these new standards provide a means for utilities to design networks enabling more efficient bandwidth usage through a mechanism for prioritizing traffic, sharing bandwidth and improved bandwidth granularity. This allows easier creation & separation of utility / operational and 3rd party applications transported over the same network in a safe and reliable way.

This section describes a large number of protocols and mechanisms, but not all would be required for implementing an Ethernet connection across an SDH network. During the evaluation process for an EoS solution, it is necessary to survey the TDM and Ethernet services that the SDH network must carry.

For simple LAN-extension for a SCADA or office-network one may simply make use of VLANs. However, if more time-sensitive applications such as IEC61850 with GOOSE over the backbone are considered, then all the described mechanisms including traffic-protection would be required.

When the Ethernet infrastructure to be implemented grows in scale, then other core technologies such as MPLS become more appropriate and allow a more scalable solution for which Ethernet over SDH becomes an appropriate complement. This technology is further described in Chapter 8.

5.2 Modern SDH Data Capabilities

Historically, the answers of equipment manufacturers to the market's requirement for Ethernet-transport over SDH were proprietary mapping schemes of Ethernet/IP – frames into SDH's Virtual Containers. To improve interoperability and flexibility, important standards have emerged. The most important ones for Ethernet encapsulation along with TDM-transport over SDH networks are listed below and their connection is illustrated in Fig. 5.1:

- Generic Framing Procedure (GFP), ITU-T G.7041, provides a generic mechanism to map packet-oriented data-streams (e.g. Ethernet) into SDH and forms the basis for VCAT and LCAS.

- Virtual Concatenation (VCAT) is an extension to G.707 for concatenation of low and high order VCs (VC-12, VC-3, VC-4). VCAT allows multiple individual SDH channels to be combined into a larger channel of appropriate size for a given payload. The figure 5.2 below illustrates the traditional (contiguous) and the virtual concatenation.
- Link Capacity Adjustment scheme (LCAS) for virtual concatenated signals defined in ITU-T G.7042 that basically specifies how link capacity adjustment schemes shall be implemented. LCAS allows hitless changes of allocated bandwidth for Ethernet-services.

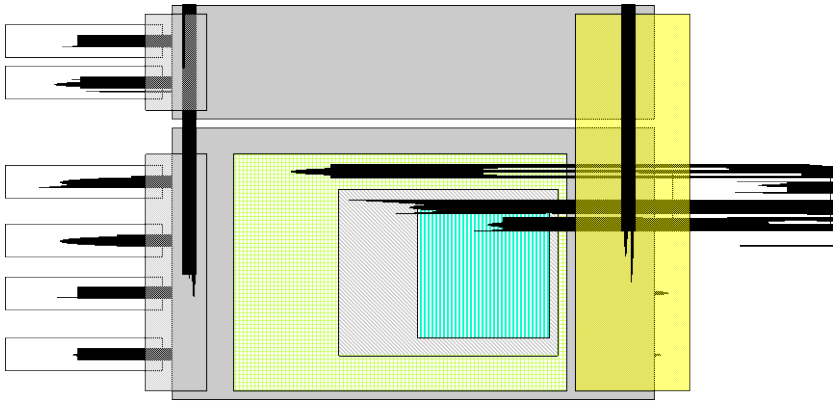


Figure 5.1 - Generic model of SDH-/WDM-equipment offering EoS

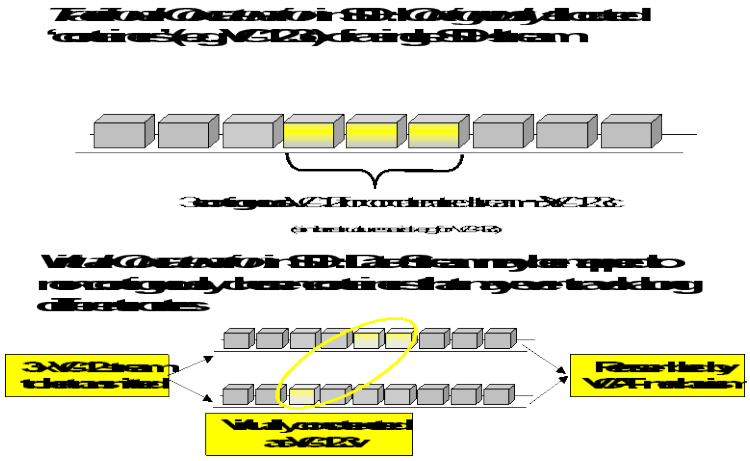


Figure 5.2 - Traditional versus Virtual Concatenation: VCAT provides higher flexibility and reaches, especially in networks with high provisioning rates, a much better capacity efficiency

There are two problems to solve when using Ethernet over SONET/SDH:

- How the SONET/SDH link capacity can be efficiently used for Ethernet traffic
- How to solve interoperability between different vendor equipments.

To help optimize the transport of Ethernet over SONET/SDH links, two new technologies have been standardized.

- ⇨ Virtual Concatenation allows for non-standard SONET/SDH multiplexing in order to address the bandwidth mismatch problem.
- ⇨ Generic Framing Procedure (GFP) provides deterministic encapsulation efficiency and eliminates inter-working problems between different vendor equipments.

5.2.1 Virtual concatenation

Virtual Concatenation is a technique that allows SONET/SDH channels to be multiplexed together in arbitrary arrangements. This permits custom-sized SONET/SDH pipes to be created that are any multiple of the basic rates. Virtual concatenation is valid for STS-1 rates as well as for Virtual Tributary (VT) rates. All the intelligence to handle virtual concatenation is located at the endpoints of the connections, so each SONET/SDH channel may be routed independently through the network without it requiring any knowledge of the virtual concatenation. In this manner, virtually concatenated channels may be deployed on the existing SONET/SDH network with a simple endpoint upgrade. All the equipment currently in the centre of the network need not be aware of the virtual concatenation.

5.2.2 Dynamic Bandwidth Allocation

Along with virtual concatenation, the capability to dynamically change the amount a bandwidth used for a virtual concatenated channel is being developed. This capability is commonly referred to as Link Capacity Adjustment Scheme (LCAS). Signaling messages are exchanged within the SONET/SDH overhead in order to change the number of tributaries being used by a Virtually Concatenated Group (VCG). The number of tributaries may be either reduced or increased, and the resulting bandwidth change may be applied without loss of data in the absence of network errors.

5.2.3 Generic Framing Procedure (GFP)

Generic Framing Procedure (GFP) is protocol for mapping packet data into an octet-synchronous transport such as SONET/SDH. Unlike HDLC-based protocols, GFP does not use any special characters for frame delineation. Instead, it has adapted the cell delineation protocol used by ATM to encapsulate variable length packets. A fixed amount of overhead is required by the GFP encapsulation that is independent of the contents of the packets. In contrast to HDLC whose overhead is data dependent, the fixed amount of overhead per packet allows deterministic matching of bandwidth between the Ethernet stream and the virtually concatenated SONET/SDH stream.

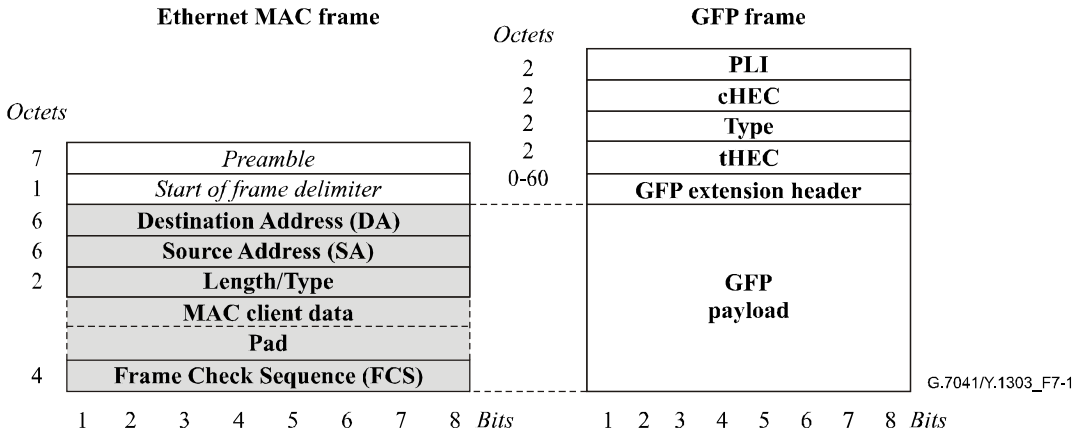


Figure 5.3 - Ethernet and GFP frame relationships

The GFP overhead can consist of up to 3 headers:

- ⇨ Core header containing the packet length and a CRC which is used for packet delineation;
- ⇨ Type header identifying the payload type;
- ⇨ Extension header, which is optional.

Frame delineation is performed on the core header. The core header contains the two byte packet length and a CRC. The receiver would hunt for a correct CRC and then use the received packet length to predict the location of the start of the next packet.

Within GFP, there are two different mapping modes defined: frame based mapping and transparent mapping. Each mode is optimized for providing different services.

Frame based GFP

Frame based GFP is used for connections where efficiency and flexibility are key. In order to support the frame delineation mode utilized within GFP, the frame length must be known and added to the head of the packet. In many protocols, this forces a store-and-forward encapsulation architecture in order to buffer the entire frame and determine its length. This buffering may add undesirable latency. Frame based GFP is good for sub-rate services and statistically multiplexed services as the entire overhead associated with the line coding and inter-packet gap (IPG) are discarded and not transported.

Transparent GFP

Transparent GFP is useful for applications that are sensitive to latency or for unknown physical layers. In this encapsulation, all code words from the physical interface are transmitted. Currently, only physical layers that use 8B/10B encoding are supported. In order to increase efficiency, the 8B/10B line code is coded into a 64B/65B block code and then the block codes are encapsulated into fixed sized GFP packets. This coding method is primarily targeted at Storage Area Networks (SAN) where latency is very important and the delays associated with frame based GFP cannot be tolerated.

GFP uses very simple encapsulation techniques that eliminates the need for termination of customer's Layer 2 frame and re-map it into PPP as required by POS (Packet over SONET/SDH, IETF RFC 2615). GFP is using a deterministic amount of bandwidth relative to the client signal bandwidth. As a result, bandwidth-efficient EoS – connections with a

guaranteed throughput for individual services can be defined (e.g. one for SCADA, a second one for VoIP).

According to SDH, the VC is defined at two levels, high-order and low-order Virtual Containers (VC) and with a virtual concatenation scheme as follows:

- VC-n-Xv is the low-order virtual concatenation of X SDH VCs for n=1, 2, 3.
- VC-4-Xv is the high-order virtual concatenation for X SDH VC-4.

Low-order virtual concatenation allows creation of sub-rate WAN channels with an incremental size between 2 Mbps (VC-12), 34/45 Mbps (VC-3), and high order allow a concatenation of VC-4 channels for users belonging to a Virtual Concatenation Group (VCG). This allows offering services with the appropriate bandwidth granularity and optimizing the network-administration efforts.

LCAS is used as a mechanism for adjusting the bandwidth of a VCAT channel by provisioning and control of the same termination elements. If a provisioning change is required, LCAS will adjust the capacity of the VCAT channel without interrupting the traffic. Thus, LCAS in combination with VCAT provide a tool to adjust the bandwidth in an operator-controlled, dynamic and hitless way.

VCAT/LCAS functionality is only required at the path termination network elements and can work with older equipment (not supporting LCAS&VCAT) in the intermediate network.

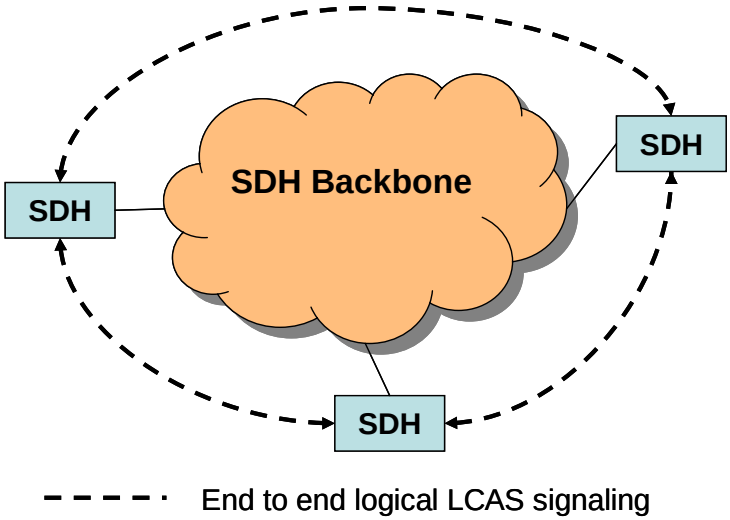


Figure 5.4 - LCAS establishes end-to-end signaling and handshaking between equipment

The enhancements described above have made SDH more flexible regarding the transport of Ethernet, but SDH does not solve the need for packet data traffic handling. Prioritization and load control must be solved before the traffic enters the SDH access network transportation mechanism and therefore it is necessary to look at the IP and Ethernet services that are currently available and/or being standardized.

- VLAN Tag Support (IEEE802.1ad and Q-in-Q). When a Customer Tagged Ethernet frame enters the network operator's edge device, an additional Tag is added to the Ethernet

frame. As a result, the network will maintain the integrity of the traffic and keep one customer's traffic separated from another's traffic. This is commonly known as Q-in-Q tag stacking which has been available for some time as proprietary solution. This feature will also improve significantly the flexibility of Utilities offering SLA-based Ethernet–services to 3rd parties (refer to figures 5.5 and 5.6).

- ⇨ Subscriber Spanning Tree tunnelling (IEEE802.1ad Provider Bridge) provides Customers Spanning Tree Protocol transport through the network giving Ethernet restoration isolation from the operator's protection mechanism.
- ⇨ Rapid Spanning Tree (RSTP), IEEE802.1w, which is an improvement in terms of restoration time
- ⇨ Link Aggregation Control Protocol (LACP) is used by the Service Provider (SP) for aggregation of multiple ports into one logical port. This will enable the SP to offer higher bandwidth between switches in the network adding ports available on that switch with combinations of 10/100Mbps and 1Gbps.
- ⇨ Generic Attribute Registration Protocol (GARP) is used by participants in the GARP group to exchange and register or de-register attribute values within the group. Related protocols like the VLAN Registration Protocol (GVRP) increase the flexibility of user administration.

5.2.4 Combining TDM and LAN Services

The two following figures illustrate the flexibility of EoS combining TDM and LAN-traffic. Common to both schemes is the ability of SDH carrying mission critical TDM-services and LAN-services basically fully isolated, means they will never influence the performance of each other and will always comply with the allocated bandwidth and performance criteria.

For the LAN/VLAN-services, various transport schemes can be implemented:

Fig. 5.5 shows how individual VLAN can be bundled (i.e. tagged VLAN 100 & 200) and finally mapped into a single or group of concatenated VCs. With this set-up, the various LAN-services share the allocated bandwidth according the priorities given to the various VLANs or associated physical ports.

Fig. 5.6 illustrates the case, where a user or user-groups are not ready to share capacity. Here EoS provides the flexibility to allocate e.g. guaranteed bandwidth to VLAN 100 and a different one to VLAN 200. Configured in such a way, neither VLANs nor TDM-services will influence each others performance. A typical application is the separation of e.g. TDM-based teleprotection or voice-traffic from internal and 3rd-party LAN-traffic carried over the backbone.

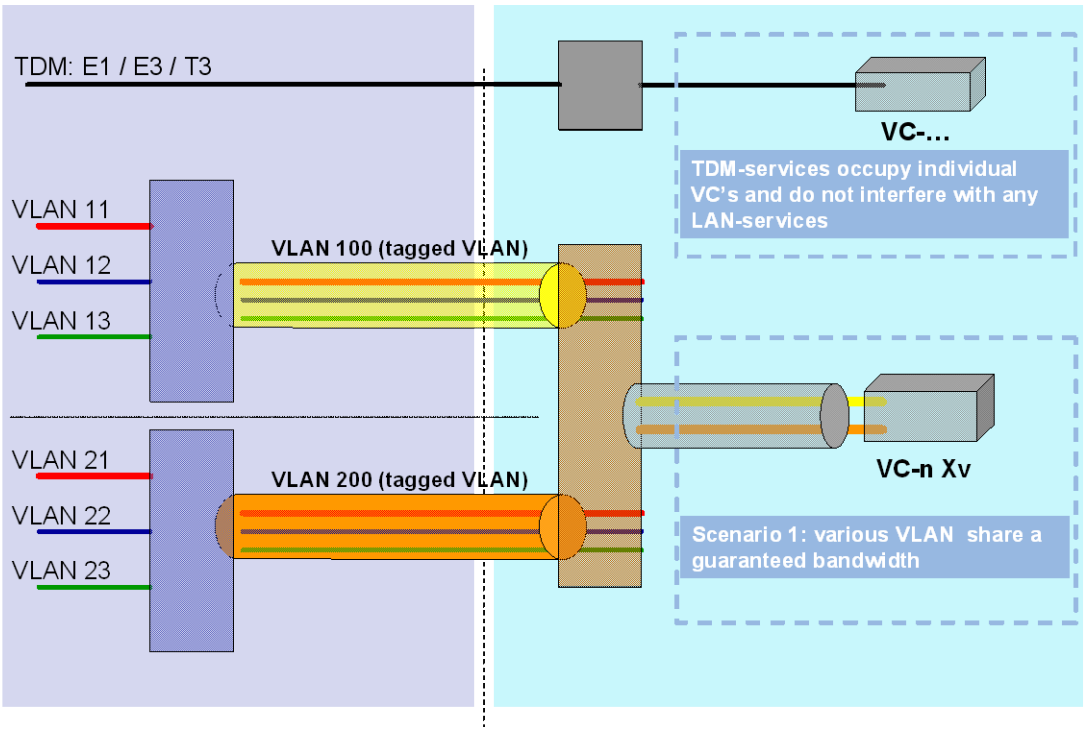


Figure 5.5 - TDM-services run independently from LAN-services sharing the allocated bandwidth

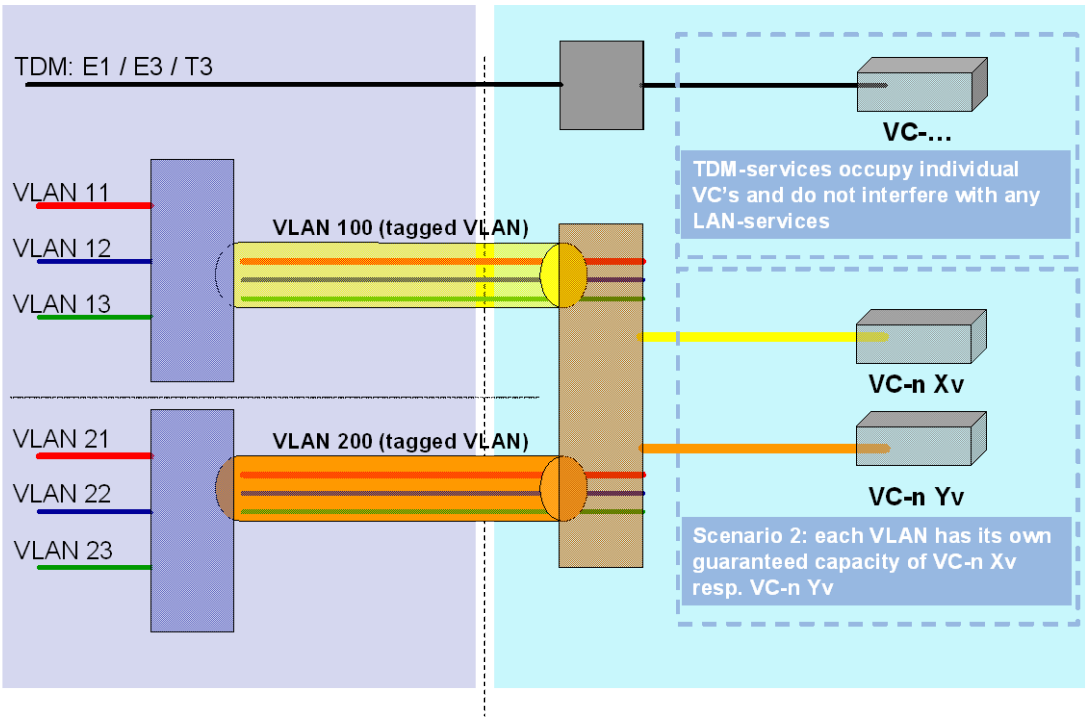


Figure 5.6 - TDM-services run independently from LAN-services with dedicated bandwidth per application or service-group (e.g. VLAN 100)

6 ETHERNET ACCESS TECHNOLOGIES

6.1 Ethernet over xDSL

Digital Subscriber Line (xDSL) covers a group of copper wire Local Loop (first/last mile) technologies which may be useful in the Electrical Power Utility context for:

- ⇨ Customer Premises access
- ⇨ Connection of substations in the urban environment
- ⇨ Connection of Utility technical offices in the proximity of HV substations
- ⇨ Connection to 3rd party service providers
- ⇨ Temporary connections before establishing permanent network connectivity

Digital Subscriber Technologies can provide 2Mbps capability (HDSL) for connecting primary multiplexers, and broadband IP capabilities (ADSL) across one (or two) pairs of ordinary telephone copper wire with limitations that have already been described in the copper wire transmission section.

HDSL (High speed DSL) G.991.1	3 modes of operation over up to 3 copper pairs - 784 kbps x 3 (or 2) pairs - 1168 kbps x 2 pairs - 2320 kbps x 1 pair
ADSL (Asymmetric DSL) G992.1	Occupies 2MHz frequency band above voice with filter separation 6.144 Mbps downstream and 640 kbps upstream net data rate.
SSDSL (Synchronized Symmetric DSL) G992.1	Symmetric data rates 192 kbps to 1.6 Mbps
ADSL2 (Asymmetric DSL2) G.992.3	Second generation ADSL Optional features: transport of STM, ATM and Packets. Up to of 8 Mbps downstream and 800kbps upstream.
SHDSL /SHDSL-bis (Single-pair High-speed DSL) G.991.2	Supports symmetric user data rates in the range of 192kbps to 2312kbps in increments of 8kbps. Optional 4-wire mode supporting data rates from 384kbps to 4624kbps in increments of 16 kbps (using Trellis Coded Pulse Amplitude Modulation, TC-PAM line code) SHDSL.bis supports symmetric user data up to 22.76 Mbit/s. The used bandwidth is divided between used pairs: one pair 5.69 Mbit/s, two pairs 11.38 Mbit/s and four pairs 22.76 Mbit/s. The interface support TDM and Ethernet traffic.
ADSL2+ (Asymmetric DSL2+) G992.5	Additional features relative to ADSL2. Higher data rates for shorter loops and longer reach for high data rates Up to 16 Mbps (min) downstream and 800 kbps upstream.
VDSL2 (Very high bit rate DSL2) G.993.2	Uses of up to 30 MHz of the spectrum above voice. Net data rate (upstream+downstream) up to 200 Mbps Fibre-extension to premises not directly connected to fibre network Allows HDTV, video-on-demand, videoconference, high speed Internet access and VoIP on std copper wire Supports legacy ATM and next generation IP-based networks.

Table 6.1 – ITU-T specified xDSL technologies

xDSL - Ethernet – The extension of Ethernet transmission over xDSL technologies is based on the IEEE 802.3ah (integrated into IEEE 802.3-2005), Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications. The standard IEEE 802.3 comprises five sections. The first four sections include specification for 10 Mbps through 10 Gbps operation, and the fifth section deals with exchange of IEEE 802.3 format frames in a subscriber access network. This IEEE 802.3 (2005) standard is also known as "Ethernet in the First Mile (EFM)". The physical layer of the standard comprises optical fibre and voice grade copper cable for point-to-point (P2P) connections in subscriber access networks.

The Recommendation ITU-T G.998.2 deals with transporting Ethernet over VDSL, and SHDSL at 100 Mbps. There is no IEEE standard for transporting Ethernet over ADSL, nevertheless the ITU-T Recommendation clarify that operation. The IEEE standard focuses in the first/last mile communications. The ITU-T Recommendation defines several exceptions with respect to the standard, and focuses on the operation of xDSL technologies on multiple pairs of voice grade TPC (twisted pair cable) providing a 100 Mbps data rate, and full duplex operation.

6.2 PDH sub-E1 mapping

A common practice in Power Utility networks is to use a bridge/switch board integrated into the substation's Primary Multiplexer in order to map the Ethernet connection of the SCADA RTU (used for TCP/IP SCADA) into a sub-E1 TDM channel (Nx64). This allows providing a separate bandwidth which may be common with other substations' SCADA across the network, while providing full separation from other services in each substation.

Ethernet over PDH (EoPDH) is a technique used to provide Ethernet connectivity over PDH networks and hence to transport native Ethernet frames over the existing legacy PDH telecommunications networks.

Several technologies are used in this transport method:

- GFP frame encapsulation
- Ethernet Mapping
- Virtual Concatenation (VCAT)
- Link Capacity Adjustment Scheme (LCAS)
- Management Messaging – for operation and maintenance actions

Other practices such as traffic tagging (separation of traffic in different virtual networks) and traffic prioritization (differentiation of traffic according to priority) are also commonly used.

Relevant ITU-T standards for EoPDH can be found in the appendix.1.

6.3 Inverse Multiplexing

Inverse Multiplexing allows establishing a single data flow at higher capacity through several lower capacity digital links (E1/T1). The implementation of inverse multiplexing in Ethernet and its related synchronization is proprietary. Despite apparent simplicity, inverse multiplexing

introduces many difficulties related to the different circuit delays, even when taking the same path through the network. This differential delay must be cancelled out through buffering.

6.4 Microwave Radio

Microwave radio technology is one of the longest established technologies used in the field of telecommunications. It has taken a new importance and market interest due to the cellular mobile system backhauling applications.

The deployment of point-to-point line-of-sight microwave links implicates frequency planning, link and propagation engineering, tower design, and many other considerations which are beyond the scope of the present report and fully covered in more specialized documents. The aspect which is of interest here is rather the use of microwave radio to transport Ethernet services in the Power Utility environment and applications. Microwave radio is employed in the implementation of Power Utility telecom networks for two purposes:

6.4.1 Microwave Backbone Ethernet

As a "Backbone" building block, microwave radio is used to complete, to complement, or in some cases to substitute a fibre network. It often constitutes a solution for providing connectivity across difficult terrain in the backbone fibre network and where no topological resilience can be provided across the fibre network, microwave radio constitutes a backup to fibre links. These tasks are performed at present through SDH multiplexing and transmission (STM-1, 155Mbps or higher) and therefore, as far as Ethernet connectivity is concerned, the same principles and constraints described in Section 5 (Transport of Ethernet over SDH) apply.

Direct high capacity Ethernet across backbone microwave systems is also appearing under the name of "Carrier-class Wireless Ethernet", certified through the Metro Ethernet Forum (MEF) specifications and tests, mainly addressing Telecom Service Provider markets.

Carrier-class Wireless Ethernet is characterized by:

- Native Ethernet packet transport
- Adaptive modulation scheme adjusting link capacity dynamically to maintain the link under difficult conditions with constant bandwidth (e.g. move between 64QAM, 16QAM and QPSK to provide a capacity between 40 and 128Mbps)
- Layer 2 network optimization and control (QoS and layer 2 resiliency)
- Link aggregation and Cross-polarization interference cancellation (XPIC) – enables a high capacity by combining two polarizations and multiple links into one virtual Ethernet circuit (GigEth)

These systems are so far not used for Power Utility telecom networks and consequently are not described in the present report.

6.4.2 Microwave Access Systems

As an Access technology, microwave radio allows connecting sites where fibre coverage is not feasible or economically viable (e.g. Control Centres and Utility office sites in the urban and suburban environment). Digital microwave access systems are at present designed with native Ethernet-over-radio capabilities. This allows implementing LAN extensions or LAN-to-LAN bridging solutions to span over a short distance (typically few kms).

Only licensed frequency systems are considered here, as the use of proprietary, license-free microwave access systems is not a commonly accepted solution in the Electrical Power System applications.

Some specific features of these native Ethernet, licensed microwave access systems are given below:

- Full outdoor implementation, consisting of a single compact module installed at the antenna and connecting in Fast Ethernet to the indoor LAN switch
- Lower cost than microwave radio associated to SDH/PDH multiplexer and data interface
- Net throughput (Ethernet frames) in the range of 4 to 34 Mbps according to radio channel bandwidth (3.5 to 28 MHz)
- Urban and suburban coverage (1 – 30km)
- ITU-T standard frequency bands in the range of 7 GHz to 38 GHz (other products exist in the market operating in the UHF band, typically 900MHz or 2.5GHz, when these bands are available)
- Low power consumption generally powered through PoE (Power over Ethernet)

6.5 DPLC Bridge

Power Line Carrier technology over HV transmission lines has been widely used by electrical power utilities worldwide for more than half a century. Modern digital PLC technology (DPLC) allows to transmit a digital stream of 20- 200kbps over the HV transmission line (around 33 kV to 1100 kV)and hence makes feasible its use as an Ethernet LAN-to-LAN bridging connection, covering distances of tens to hundreds of km.

DPLC provides an implicitly reliable transmission medium (due to mechanically robust HV transmission line's high reliability) and allows coverage in otherwise isolated areas. In particular, it has a range without repeaters which is far greater than any other comparable transmission medium.

PLC performance and bandwidth capabilities depend upon the line conditions. The PLC link's maximum transmission rate is determined by the available frequency bandwidth, which depends upon the density of the frequency plan and hence the number of PLC links in the immediate vicinity. The available transmission rate depends also upon the channel's Signal to Noise Ratio (SNR) and consequently upon the line noise and attenuation: we can therefore go far but at low speed, or go fast but on short links. Typically, with an SNR of about 40 dB, the system can operate at 8 bps/ Hz (32kbps in 4kHz). The system generally adapts its speed according to line noise and attenuation conditions.

The noise across HV PLC links is mainly due to the corona effect (ionization of the air) depending upon atmospheric conditions (air humidity, rain, pollution, and ice over the transmission line). In order to assure high availability, the performance of the PLC link must therefore be estimated under adverse atmospheric conditions.

Ethernet bridging over Digital PLC is a reliable and economical solution for providing a low throughput Ethernet access for specific operational applications in a HV substation without

fibre or microwave coverage. Typical applications that may be covered through DPLC Ethernet connection are:

- Connection of SCADA RTU in the substation to the Control Centre or to the main digital backbone network, allowing higher data rates and TCP-IP-based communications (IEC60870-5-104)
- Voice connection of the substation in an IP environment
- LAN interconnection for extracting data from the HV substation

As for other low capacity bridging technologies, it is important to optimize the payload and therefore the size of the Ethernet frames when the Ethernet system includes a DPLC bridge. This optimization and the consequent transport efficiency is related to the overlaying network (typically TCP/UDP over IP), and therefore is beyond the scope of the present document which is dedicated to Ethernet. Compression and caching are appropriate techniques to optimize the applicative payload in these systems.

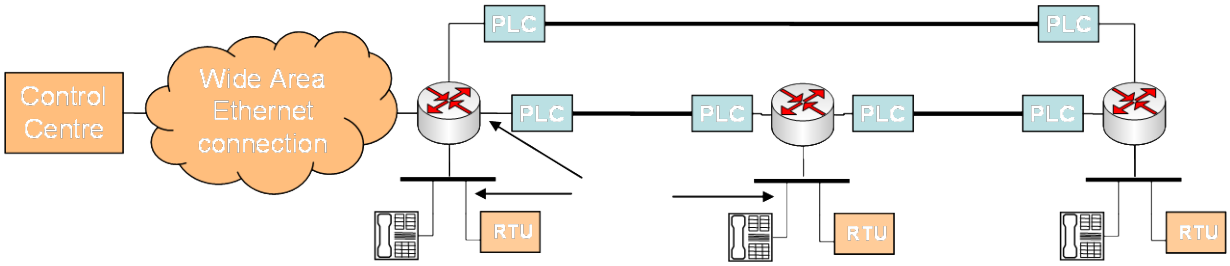


Figure 6.2 - Use of DPLC as an Ethernet Bridge

6.6 GPRS and UMTS

GPRS (General Packet Radio Service) is a mobile data service offered in GSM systems. GPRS is a packet switched service, where subscribers use the available channels only when they have data to send. This scheme suits non real time applications such as file interchange, email or web browsing.

The GPRS service is provided by Mobile Network Operators throughout the world, using GSM licensed frequency bands (800MHz, 900MHz, 1800MHz, 1900MHz). In this case, as opposed to Wifi or other technologies, the infrastructure network is owned by the Mobile Operator. GPRS is widely used in IP networks today as a WAN wireless technology to link remote or physically separated Ethernet LAN networks. Data throughput can vary from 9 to 60Kbps (downlink) and 9 to 40Kbps (uplink), depending on the GPRS terminal and the Operator Network, and is usually asymmetrical (uplink and downlink do not have the same data transmission speed), where downlink speed is somewhat higher than uplink's.

In a similar way UMTS (Universal Mobile Telecommunication System) is an evolution of GPRS networks using CDMA modulation in the band of 2100MHz. The data rate can reach 384Kbps or up to 7.2 Mbps in HSDPA networks.

However, there are some peculiarities of GPRS/UMTS technology that must be taken into account for a successful integration of Ethernet networks and the GPRS network:

- Latency. The GPRS network has a remarkable latency (usually in the 0.5 to 2 seconds range), and is non-deterministic, depending greatly on the carrier network utilization. This issue must be considered when carrying delay sensitive data. The latency in UMTS is considerable smaller with a typical value between 150 and 400msec.
- Packet losses. The GPRS network is lossy, due to radio propagation conditions and their variability with time. Moreover, network operators tend to pay more attention to voice calls, assigning resources to GPRS traffic on a best effort basis, unless enforced by the end customer by means of a Service Level Agreement (SLA). Then a minimum data throughput shall be guaranteed by the operator.
- Traffic cost. In Ethernet networks once the infrastructure is deployed the traffic is virtually free. But in GPRS networks the traffic is billed per byte or per high volume quantities. Thus Ethernet traffic must be filtered before accessing the GPRS WAN link, ensuring that only the required traffic uses the link, and reducing the operation cost.

With the introduction of new technologies such as UMTS and HSDPA, these drawbacks have been mitigated: latency is halved and packet losses greatly reduced, as the capacity is increased tenfold. However, due to the high costs of deployment in the short term these technologies will only be available in urban areas, and so in the mid term the majority of substations and power generation plants will likely only have access to GPRS Networks.

Some networks carriers have started to offer a service based on private GPRS domains, which can be of interest for utility applications. In this application, the customer can buy or lease SIM cards which have private (not public) IP addresses. They form a private IP subnetwork, which is isolated and not accessible from the internet. The IP addresses can be chosen to fit the existing IP addressing scheme in the utility.

It is expected that in following years the number of GPRS lines and applications will grow, since operators are promoting GSM/GPRS over traditional PSTN lines for new subscriptions.

It should however be noted that in some countries IP connection from the public Internet to GPRS is not allowed and this must be taken into account in designing specific applications and architectures.

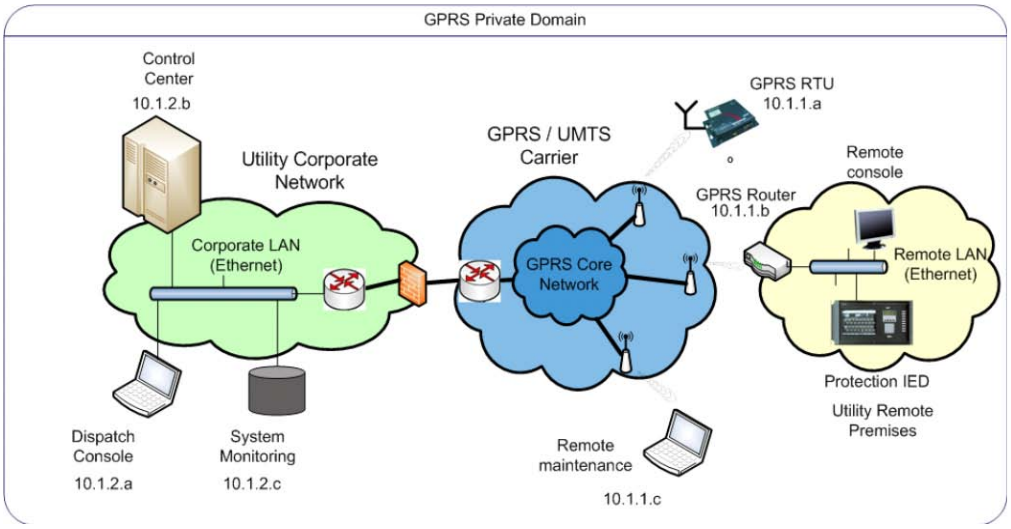


Figure 6.3 – Typical application for Ethernet over GPRS in Utility applications
(note: references in the figure are from the original, not related to the present document)

6.7 VSAT

A Very Small Aperture Terminal (VSAT) is a telecom device that is used to communicate with geostationary satellites. Generally these devices work in the C (3-7GHz) and Ku (11-15GHz) frequency bands.

The “very small” component of the VSAT acronym refers to the size of the antenna or dish, whose diameter is typically (55 cm – 120 cm). A VSAT device consists of an ODU (Outdoor Unit) and an IDU (Indoor Unit). The outdoor unit contains the antenna dish, a low noise block converter and a transmitter. The indoor unit contains a receiver and a transmitter unit (to communicate with the ODU via coaxial cable) and a router engine, which connect to the user networking equipment.

VSAT networks advantage is related to service accessibility. In a GEO satellite illuminated area, a VSAT earth station can be installed in any place – as long as a direct sky view exists. Moreover service availability is very good, rating above 99% of total time, typically a better availability than that of leased lines or private networks.

VSAT networks are designed in a hub-and-spoke fashion, with customer locations connecting directly over the air to a central “hub” site. The equipment at customer locations are VSAT routers attached to a small dish. At the central hub site, a large dish and sophisticated hub RF components exchange information with VSAT devices, and route information to / from Internet or customer private data networks.

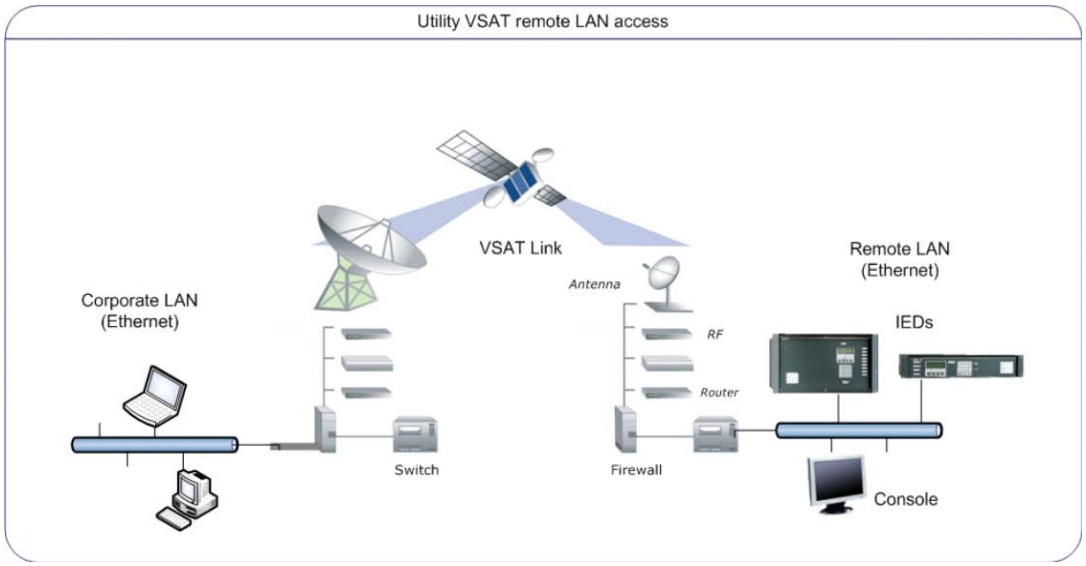


Figure 6.4 - Typical application for Ethernet over VSAT in Utility applications

The main drawback of VSAT technology is **latency**. It takes about 500 ms to make the trip to the satellite and back. Special care must be taken for latency-sensitive applications.

VSAT equipment manufacturers have addressed this problem by developing VSAT acceleration technologies, such us TCP accelerators. Applying standard TCP/IP to VSAT circuits leads to the underutilization of the link and degraded performance. Despite satellite circuits having advanced FEC (*Forward Error Correction*) algorithms, there is still a big issue of round trip latency. Additionally, there may be packet losses. These issues cause TCP/IP to automatically reduce its window size as a precaution and the slow start algorithm to work incorrectly. There are some proprietary solutions available in order to overcome TCP/IP performance degradation. Usually, these solutions are named TCP accelerators and Performance Enhancing Proxies. TCP accelerators use different techniques to substitute TCP/IP with a protocol set which is more optimized for Satellite circuits. Most of these solutions use UDP as the primitive IP packets transport while speed and window size negotiations are done inside the TCP accelerator protocol set. Most of the TCP accelerators also bundle a number of well known techniques in order to improve the performance of the Satellite Internet circuit as seen by the common user. These techniques usually include DNS caching, HTTP pre-fetching and on the fly traffic compression.

It should be noted that certain encryption technologies are not compatible with VSAT acceleration technologies, which make the manufacturers develop their own solutions for VPN, SSL …

VSAT networks have a great flexibility in the amount of bandwidth that can be obtained in point-to-point links. Typical values range from 9.6Kbps to 8Mbps upwards. The bandwidth is directly contracted with the satellite service provider, and can be scaled up or down in a relatively fast and cheap process depending on the evolution of bandwidth requirements.
VSAT links are used very often in the electric utility sector. The main applications include:

- Remote emulated Ethernet access to distant locations, where the availability of a fixed network is either too costly or impossible to deploy. This solution is used widely in large countries, where distances among remote locations may be very large.
- Remote serial port emulation for telecontrol applications. In typical SCADA to RTU communications, this technology overcomes the drawbacks imposed by remoteness or absence of fixed communication means in substations or other remote controlled sites.

In all these applications VSAT is the preferred access technology due to the fact that it provides independence between cost and distance, as opposed to private communication means or leased lines.

6.8 Broadband Power Line Communication

BPLC uses the existing medium and low voltage electricity cable infrastructure to provide broadband point to multipoint telecommunication services.

Medium and low voltage cable infrastructure has not been designed to support telecommunication services so their transmission performance is very poor. Due to this, robust modulation schemes together with an advanced MAC layer are required to provide telecommunication services.

BPLC transmission layer is based on the OFDM modulation. The advantage of this modulation scheme is its robustness to impulsive noise, its capability to work over channels with a poor and variable frequency response and its efficiency in multi-path fading channels. BPLC provides up to 300 Mbit/s bandwidth shared by the users of a segment.

The MAC layer is normally based on proprietary implementations specially design to manage a point to multipoint network. The MAC layer functions used to be coordinated by the Head end node. The most relevant services supported are:

- Channel access coordination
- Medium access control
- QoS including bandwidth reservation and priorities management
- Standard IEEE MAC services such as spanning tree or VLAN.

QoS provision is based on a Class of Service scheme. Traffic can be classified and prioritised, bandwidth can be reserved. The Head and node administrate network resources in order to comply with all the QoS profiles defined by the users under its control.

The QoS level achieved may be acceptable form most of the service provided by and access network. The use of this technology for critical operational services has to be thoroughly assessed since there are many factors that may influence the long-term QoS provision.

BPLC technology can be used to deploy Ethernet service in metropolitan areas. The internal MAC layer emulates Ethernet MAC layer services in such a way that users obtain a fully compatible Ethernet service.

BPLC technology is being used by some telecomm operators in the access networks as well as in the deployment of broadband telecommunication services in places or building where it is not possible to install a wiring or wireless infrastructure.

The application of BPLC technology for operational service provision is being trialled, the most relevant applications being smart metering application and demand side control.

6.9 Passive Optical Networks (EPON)

Passive optical network (PON) is a technology allowing the distribution of optical signals to multiple sites through a single transmitter using passive components (Optical stars, WDM components, Attenuators, Polarizations filter optical switches). The employed topology is that of a passive star based on a Star Coupler manufactured by fusion splicing of multiple optical fibres (refer to figure 6.5 hereafter).

The available optical power being split into multiple beams in order to reach multiple receivers, the passive star introduces significant loss into the system leading to a very short range (3dB in a 1 x 2 star). This short range limits considerably the applications of the PON technology, mainly to the Customer Premises access applications (e.g. Cable TV distribution). EPON (Ethernet Passive Optical Network) is the application of PON technology to Ethernet Access networks, used for customer premises data connectivity (e.g. FTTX).

Figure 6.6 hereafter presents the principles of operation of an EPON system connecting multiple user sites to a common network switch. The system operates as a Full Duplex GigaEthernet with continuous flow. Upstream (users to the network) and downstream (network to the users) flows are wavelength division multiplexed into a single fibre. In the Downstream sense, Ethernet frames for all users on the EPON are transmitted on the same physical port to the Passive Optical Splitter (star coupler) and the resulting optical signal distributed to all user Network Units which recognize the appropriate address frames for each particular user. In the upstream sense, time slots of varying capacity are allocated to each user (according to a pre-established SLA), into which the Network Unit of each user shall insert its Ethernet frames.

The short range of the technology limits its potential applications in the Power environment. The only power application for EPON technology at present, may be for remote access to power devices at customer premises (e.g. advanced metering) when other non-power applications justify the investment.

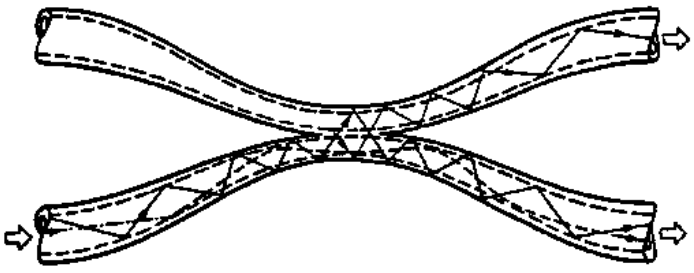
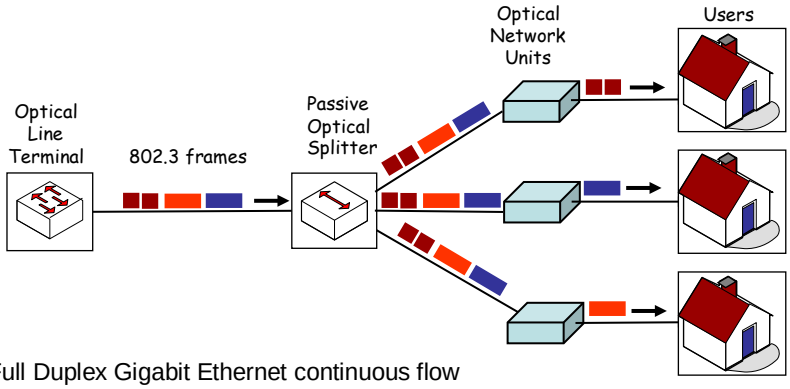


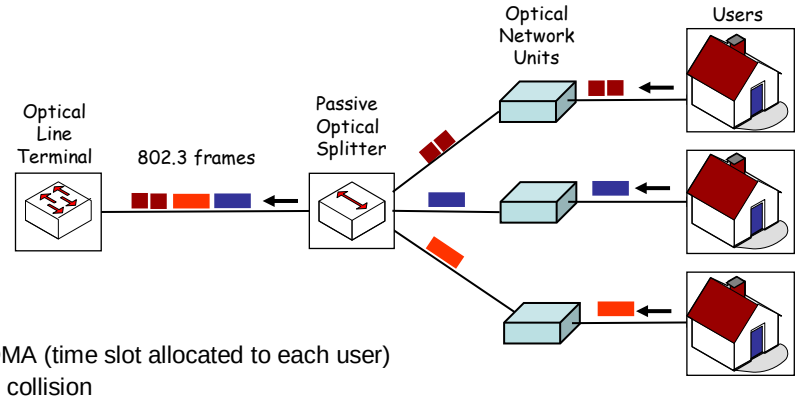
Figure 6.5 – Optical Coupler with 3dB signal loss

EPON Downstream Flow



- Full Duplex Gigabit Ethernet continuous flow
- Passive splitter for 32 optical fibres
- Wavelength multiplexing of upstream and downstream flow (one fibre)

EPON Upstream Flow



- TDMA (time slot allocated to each user)
- No collision
- Bandwidth allocation according to SLA

Figure 6.6 – Operation principles for an Ethernet Passive Optical Network (EPON)

6.10 Free Space Optical links

Free space optical links are available on the market but not commonly used. A free space link is very compact using a fibre optical laser as transmitter. When using a free space link, there must be line of sight for the link. Depending on the weather conditions, this kind of link can be used up to some kilometres in places like Southern California. In Europe, the maximum range normally is some hundred meters.

Free space optical links have a small optical beam and normally operate with 2 links mounted in parallel with a distance of approximately 1 meter in order to avoid medium sized birds causing interruption in the transmission.

Free space optical links can be a cost effective alternative for inter-building communications where fibre installation is expensive or complicated.

A free space link does not require any frequency permissions for installation, unlike microwave links.

Most free space links have a general transparent interface using electrical SDH/PDH or Ethernet interfaces

7 WIRELESS ETHERNET NETWORKS

7.1 Introduction

Broadband wireless technology has gained maturity in different data networking environments and is gaining increasing importance in the power utility. At present WiFi is a very common way for PC access to public internet, WiMAX is becoming a viable technology for broadband coverage in the rural and dispersed environment, and different Personal Area Network technologies such as Bluetooth and ZigBee are the common technology for connecting different "everyday life" appliances in the short-range.

Broadband wireless data technologies have been covered by IEEE as follows:

- IEEE 802.11 – Wireless Local Area Network (WLAN), known as WiFi, covering a few hundred meters, generally one site or facility
- IEEE 802.16 – Wireless Metropolitan Area Network (WMAN), known as WiMAX covering 10-20km
- IEEE 802.15 – Wireless Personal Area Network (WPAN) with a span of a few meters

In the Power Utility operational environment, the following main applications are envisaged:

- Wireless nomadic access inside the substation perimeter for connecting a Craft Terminal (laptop or compact industrial PC) to different Intelligent Electronic Devices for reading and setting of parameters, status, etc. Assuring the security of the data exchange is the main issue in this case.
- Coverage of dispersed facilities and broadband access to customer premises. Licensing of the large frequency spectrum bandwidth is generally the issue.
- Wireless Sensor Networks for connecting instrumentation in a constrained space. Service availability and security are the main issues.

A short account is given to each class of technologies and related standards with particular focus on the applications in the power domain.

A detailed analysis of the concerned technologies as well as engineering rules in different indoor and outdoor environments is beyond the scope of the present document and can be found in standard literature (e.g. refer to [7]). Moreover, the presented technologies are only starting to find their way into the power environment and measurement data compilation concerning their operation in the electrical substation switchgear, substation control building and power plants is not yet available in any significant manner.

Finally, it should be noted that the technologies described in this chapter are not Ethernet physical layers, they use specific control and management packets and specific headers and protocols which are adapted to the operation over a multi-site radio system.

7.2 Wireless LAN or WiFi (IEEE 802.11)

The term WiFi makes reference to a collection of wireless LAN networking technologies organized under the IEEE 802.11 family of standards. It uses Direct Sequence Spread Spectrum (DSSS) and Multi Carrier Orthogonal Frequency Division Multiplexing (OFDM) radio technologies. Unlike other wireless communication technologies, WiFi makes use of 2.4 and 5GHz unlicensed frequency bands. This fact has the following advantages:

- Plenty of equipment and vendors available.
- Guaranteed interoperability via an independent product certification entity (WiFi Alliance).
- Worldwide availability of (at least some channels) on the same frequency bands.
- Transmission data rates of the order of tens of megabits can be achieved (802.11g technology has a limit of 54Mbps).
- Low cost of the devices and no exploitation costs for the service.

On the other hand, there are some drawbacks that must be taken into account:

- The system has a low coverage due to transmit power limitations.
- Because the frequency bands are free for anyone willing to use them, there may be some interference problems arising from congestion, both by WiFi devices and other appliances using the same unlicensed band.
- Last, but not least, security aspects are mandatory, as WiFi systems can be easily sniffed. Strong encryption mechanisms, such as WPA and preferably WPA2, have proved secure enough to enable WiFi technology use in utility environments.

There are two main application scenarios from a Power Utility perspective where WiFi technologies may be used in conjunction with an Ethernet network:

- Provide wireless bridging between fixed Ethernet networks. In this case a fixed Ethernet network can be reached by means of two wireless bridges, which create a wireless link between them, and create a layer 2 bridge. This is very useful when the deployment of a fixed Ethernet connection is not feasible due to physical constraints or high costs. Link distances in the order of kilometres may be reached using standard equipment.
- Allow wireless access to the fixed Ethernet network by means of a WiFi Access Point. This application addresses the access of itinerant users, such as maintenance personnel, to a fixed Ethernet LAN, without the need of a physical connection. However, due to the nature of WiFi technology, security aspects become a serious concern and careful security policies must be implemented (WPA, WPA2).

The 802.11 family currently includes multiple over-the-air modulation techniques that all use the same basic protocol. The segment of the radio frequency spectrum varies between countries and includes the 2.4 GHz and 5GHz bands.

Table 7.1 hereafter presents the most important standards produced in the series IEEE 802.11 together with their major features.

- 802.11b was the first widely accepted wireless networking standard, followed by 802.11g and then 802.11n. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to previous specifications.

- ⇨ 802.11n is based on a new multi-streaming modulation technique and at the time of preparation of the present document, is still under draft development, although proprietary products based on pre-draft versions of the standard are available on the market.

802.11b has been successfully tested at substations in bridge applications, and the radio link proved reliable under severe electromagnetic conditions, such as switchgear operation.

Protocol	**Release Date**	**Operating Frequency**	**Throughput (Typ)**	**Data Rate (Max)**	**Range (Indoor)**	**Range (Outdoor)**
Legacy	1997	2.4–2.5 GHz	0.7 Mbps	2 Mbps	Depends on walls	~75 m
802.11a	1999	5.15- 5.25 G 5.25 -5.35 G 5.725-5.875	23 Mbps	54 Mbps	~30m	~100 m
802.11b	1999	2.4–2.5 GHz	4 Mbps	11 Mbps	~35m	~110 m
802.11g	2003	2.4–2.5 GHz	19 Mbps	54 Mbps	~35m	~110 m
802.11n	2007 - 2008	2.4 GHz 5 GHz	74 Mbps	248 Mbps	~70m	~160 m

Table 7.1 – Main 802.11 standards

7.3 Wireless MAN or WiMAX (IEEE 802.16)

The IEEE 802.16x standards, called Wireless MAN, or "WiMAX" (Worldwide Interoperability for Microwave Access), define a "last mile" wireless broadband technology competing with or complementing DSL technologies and cellular-based 3G technologies.

An industry group called the WiMAX Forum promotes and certifies compatibility and interoperability of WiMAX broadband wireless products around certain defined frequency profiles.

As a telecommunications technology, WiMAX can provide wireless data connections over long distances (40km) and high data rates (50Mbps). In practice, there is a trade-off between distance, throughput and channel size. Unlike conventional microwave systems operating in similar frequency bands, WiMAX provides non-line-of-sight (NLOS) capabilities which are enhanced through the use of OFDM modulation and advanced antenna diversity techniques.

There are two versions of WiMAX standards promoted by the WiMAX forum. It should be noted that the two standards have different radio interface technology, and thus are not interoperable. WiMAX technology can be used in both unlicensed and licensed frequency bands, even though most of the interest up to now has been devoted to licensed spectrum. Currently there are licensed applications in 2.3, 2.5 and 3.5GHz bands, and unlicensed applications in the 5 GHz band. One of the main limitations is that these frequency bands are not globally available.

- IEEE 802.16d-2004 known as "Fixed WiMAX" – This was the first standard certified by the WIMAX forum. It is designed around a fixed usage model. There are a handful of early vendors who obtained certification for this band. The approved profiles for interoperability include 3.4-3.6 GHz only, in both TDD and FDD modes of operation. An initially proposed 5GHz band received less vendor support.
- IEEE 802.16e-2005 known as "Mobile WiMAX" – This standard supports a number of feature enhancements designed to enable mobile and portable usage, to reinforce security, and to improve non-line-of-sight (NLOS) performance and coverage on top of fixed use. This is where the interoperability and new development is at present focused.

WiMAX potential applications in the power utility include the following:

- CCTV surveillance of sites and facilities (wireless cameras and infrastructure)
- IP access to sites and facilities which are not on fibre infrastructure (i.e. DSL)
  - Remote LAN access
  - Monitoring applications
- Backhaul of other wireless systems (e.g. WiFi, TETRA and other Private Mobile Radio)
- Advanced Metering Infrastructure (AMI)
- Backup link for fibre communications

7.4 Wireless PAN, Wireless Sensor Networks (IEEE 802.15)

A WPAN (Wireless Personal Area Network) is a network of electronic devices within short distance, usually some meters. These are the devices belonging to or around a person, such as a laptop, a PDA, a phone, a headset, consumer electronics... WPAN networks may be used as a gateway for connecting to other networks (e.g. access the internet) or to communicate data among the devices (a wireless headset connected to a phone).
WPAN networking standards are developed under IEEE working group 802.15. This group has produced the following standards:

- IEEE 802.15.1-2005, which consists of Bluetooth v1.2 short range access technology. Specifies MAC and PHY layers for a technology which is capable of a maximum throughput of 1Mbps over the globally available 2.4GHz frequency band.
- IEEE 802.15.2, which addresses the coexistence of WPAN networks with other unlicensed frequency band wireless devices and applications based on IEEE 802.11 standards.
- IEEE 802.15.3 addresses high data rate (>20Mbps) WPANs. It has produced a MAC layer and is studying different alternative PHY implementations.
- IEEE 802.15.4 focuses on low speed WPANs. Its main objectives are to achieve very low complexity and very low power WPAN implementations. Targeting battery powered devices, the idea is to obtain battery lifespans of months, even years. This group has developed a MAC layer and two different PHY implementations for the 868/915MHz and 2.4GHz frequency bands, with maximum throughputs of 20Kbps and 250Kbps respectively. The Zigbee protocol stack is based upon this series of standards.
- IEEE 802.15.5 targeting mesh networking in WPANs.
- IEEE 802.15.6, which is addressing the subject of BAN (Body Area Networks) with the goals of low power and the use of low frequencies.

The interest in wireless networks of very small coverage in the power utilities is rising. The concept of Wireless Sensor Networks (WSN) associates low power consumption to short range mesh networking and a relatively small speed, allowing the connection of instrumentation inside a constrained area to a processing, concentrating or gateway device. Energy management applications at the domestic consumer premises are an important constituent of the present SmartGrid initiative and the Zigbee protocol stack using IEEE 802.15.4 and Mesh Networking is the basis of the Home Area Network to enable these applications.

8 EMULATED LAN SERVICE

8.1 Ethernet Emulation

The transport infrastructure upon which the Ethernet connectivity is to be implemented is not necessarily a dedicated network. The power utility may use outsourced services of a multi-user IP Service-Provider for accessing certain sites or as a core network. An Ethernet connectivity can be emulated on the top of a multi-service IP network for connecting LANs dispersed in a large geographical area.

Moreover, the dedicated telecommunication network of the Power Utility may grow in size and move from a single-customer situation serving the operational services of one Utility, to a many-customer situation serving the different operational and corporate requirements of one or of several Utilities and other external parties. In this case, the implementation of Ethernet Virtual LANs (VLAN) is no longer sufficient and scalability issues shall arise. In this case, a multi-service IP/MPLS infrastructure may be implemented as described in this chapter and serve as a Core transport network. Ethernet connectivity can be assured through this Core network through Encapsulation schemes. However, it must be noted that the use of MPLS and encapsulation may introduce time latency incompatible with certain applications such as Teleprotection and this must be carefully considered at the time of network design.

In both of the described situations, a Hierarchical Hybrid Architecture as presented in the following figure shall be appropriate:

- ⇨ Ethernet VLAN (L2 Ethernet) through the Power Utility's dedicated infrastructure (e.g. Ethernet over SDH) connecting the service access site to an Access Point of the Core Network
- ⇨ Core network connectivity across an IP/MPLS multi-user network provided through either an external or an internal Service Provider.

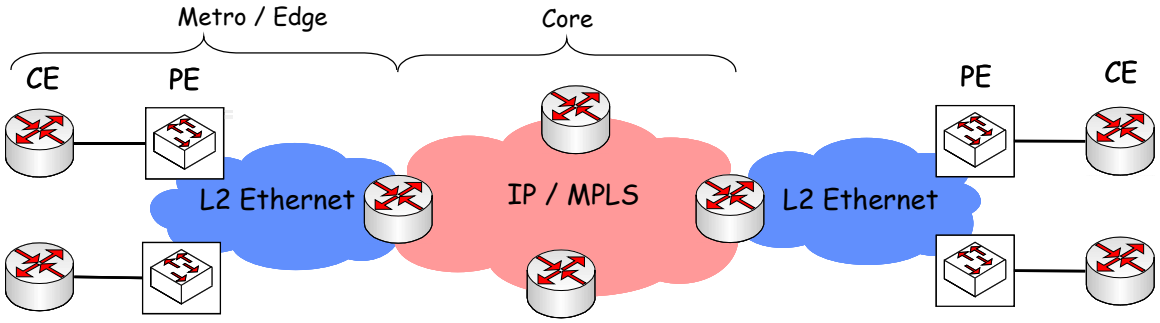


Figure 8.1 - Hierarchical Hybrid Architecture

8.2 Ethernet over MPLS – VPLS

8.2.1 Multi-Protocol Label Switching (MPLS)

As IP communication is based on a datagram protocol, the routing and forwarding of data packets are based on the datagram header, particularly the IP address of the receiving party. This mode of operation has the advantage of simplicity: once the different IP routers have performed their initialization, every packet can be forwarded to the next node using the routing tables that have previously been established dynamically in the Routers.

However, IP routing and forwarding does not distinguish traffic flows in order to manage the Quality of Service as efficiently as a Connection-oriented (Virtual Circuit) system such as ATM (Asynchronous Transfer Mode).

The Multi-Protocol Label Switching (MPLS) is not a communication protocol but a Forwarding Technique. In the communication network layer model, it is often inserted between layer 2 (link) and layer 3 (network) and is hence called "layer 2.5". MPLS provides a way to transport IP (or non-IP) packets using "Labels" which are not simply IP addresses. It provides in this way a Unified Control Plane (the "signalling layer" which is missing in the IP protocol) permitting ATM-type Connection-Oriented operation for IP datagram without the complexity inherent to ATM. Many standard IP routers today offer LSR (Label Switch Router) facilities and therefore allow the implementation of a private MPLS infrastructure.

This "Label Swapping" technique is based on the insertion of a Label at the Ingress port of the network and the association of a Forwarding Equivalence Class (FEC) to the Label. Each FEC defines the manner in which the packet is to be treated in each MPLS node. The label is removed at the Egress port of the network. A connection established in this way is called a Label Switched Path (LSP).

MPLS enables the control of traffic flows in the network and the mapping of traffic demand onto a network topology (Traffic Engineering TE). It can distinguish traffic flows, adopting different strategies for different service requirements (QoS Routing) and through the separation of different traffic streams, it provides the required Service Isolation and hence implicit Security.

The use of MPLS techniques allows deploying Virtual Private Networks (MPLS VPNs) in a unified Multi-service Network. A VPN is a group of network access nodes using the same Label and hence capable of exchanging data packets in a closed manner across an otherwise public multi-service network.

8.2.2 Transporting Ethernet over an IP/MPLS network

Implementing separate Ethernet Virtual LANs (VLAN) through Layer2 Tagging, as described in previous sections, provides a simple but not a scalable solution. As the number of VLANs grows, the size of the MAC Address Table can become extremely large. The switches constituting the network will have to "learn" the MAC address per port for the whole network and VLAN management may become complex.

Transporting Ethernet over MPLS provides the technology for the creation of a core layer overcoming the problem of scalability, while maintaining the end-to-end Ethernet service provision.

MPLS can be used to transfer encapsulated data from different technologies over a certain network. An additional label is inserted in the data for the encapsulation purpose and this label is used for the forwarding and classification inside the MPLS network.

This additional label can be used to encapsulate a layer 2 frame e.g. Ethernet frame. This solution, called Layer 2.5 MPLS or L2 VPN, is very scalable but can be quite complex. It is currently on the way to be implemented in the field.

Ethernet service over MPLS can be point-to-point (P2P) or multipoint-to-multipoint (MP2MP):

- The P2P Ethernet service (E-Line), also called the Pseudo-wire (PW) is based on a "Packet Leased Line" concept and can employ the L2 Tunneling Protocol (L2TP).
- The MP2MP Ethernet Service (E-LAN) implemented over an MPLS infrastructure is generally referred to as Virtual Private LAN Service (VPLS).

The current way for implementing Ethernet over MPLS is known as draft-Martini (named after the author of the original draft). It describes L2 encapsulation over the MPLS infrastructure and allows the transport of layer 2 frames across an MPLS Service provider domain.

The Ethernet frame received at the MPLS edge is encapsulated without any modifications. The MPLS label is inserted directly in front of the old Destination MAC address and then a new Ethernet Header is added in front of the MPLS label.

Two labels are therefore used:

- Tunnel label – The Tunnel label is used to carry frames across the MPLS network. Core Label Switch Routers (LSR) only look at this label. The Tunnel Label is removed by the penultimate hop prior to the egress node.
- Virtual Circuit (VC) Label – The Virtual Circuit Label is used by the egress node and determines how to process the frame and where to deliver the frame on the destination network.

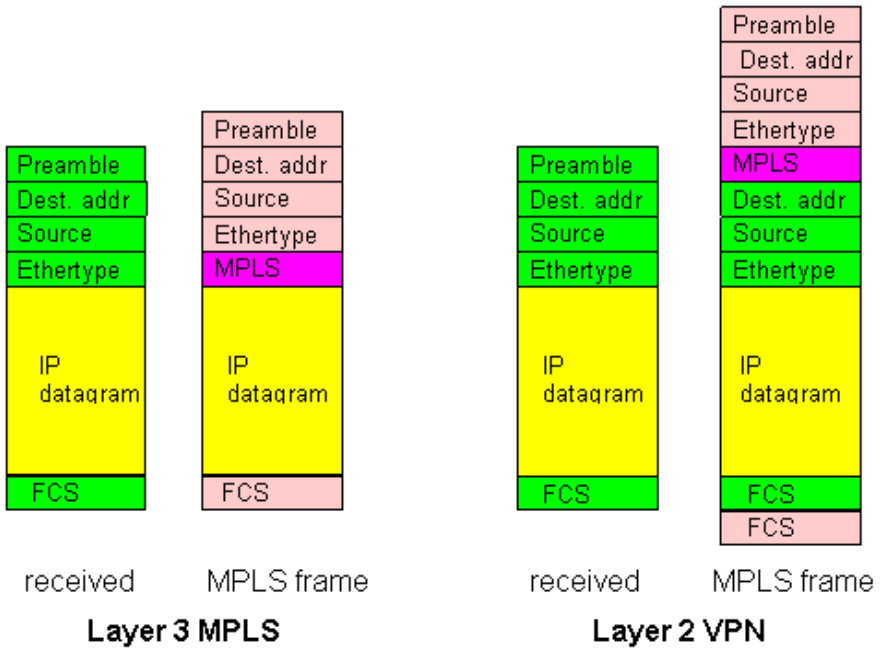


Figure 8.2 – Encapsulation of IP datagram received on an Ethernet interface using Layer 3 and using Layer 2 VPN.

8.2.3 Virtual Private LAN Service (VPLS)

Virtual Private LAN Service (VPLS) provides a scalable, switched Ethernet LAN over an IP/MPLS network. It uses MPLS layer2 encapsulation (Draft-Martini) to create an L2VPN as its building block.

It allows for the transport of Ethernet traffic (unicast, broadcast, and multicast) from a source 802.1Q VLAN to a destination 802.1Q VLAN over a core MPLS network, by mapping these VLANs to MPLS Label Switched Paths (LSP). Ethernet over MPLS uses the Label Distribution Protocol (LDP) to dynamically set up and tear down LSPs over the core MPLS network for dynamic service provisioning.

VPLS allows the user to profit from the implicit service security and availability features of MPLS:

- Traffic Engineering – The use of Forwarding Equivalence Class (FEC) in the MPLS and adequate use of its Labels allow identification of traffic flows and hence to perform Traffic Engineering.
- Fast Protection against node/link failure – MPLS selective forwarding facilities are more efficient and faster than corresponding reconfiguration possibilities incorporated into the Ethernet Bridging standards (Spanning Tree Protocol and its variants) especially for large and topologically complex networks.

- Bandwidth guarantee through RSVP-TE - the Resource Reservation Protocol used for the MPLS Label Distribution (Control Plane) allows the introduction of the determinist Quality of Service and Bandwidth guarantee missing in the essentially Best Effort IP network, making the VPLS very close to a dedicated infrastructure Switched Ethernet.

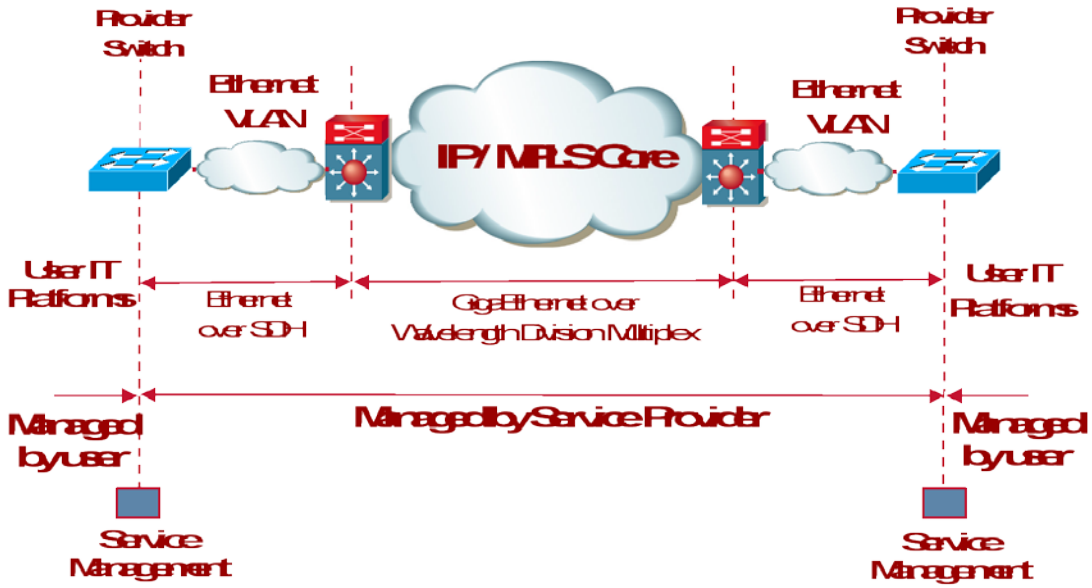


Figure 8.3 - Example of implementing VPLS service across a Power Utility

8.3 Ethernet over ATM – LANE

Asynchronous Transfer Mode (ATM) has been used by certain Power Utilities in the past but has been or is being replaced by MPLS technology. The subject of Ethernet over ATM in Utilities' networks is therefore no longer an issue of interest. This section presents just a brief summary for some possible legacy systems.

In order to make it possible to continue using existing LAN application software, while taking advantage of the increased bandwidth of ATM transmission, standards have been developed to allow the running of LAN layer protocols over ATM. LAN Emulation (LANE) is one such method, enabling the replacement of 10 Mbps Ethernet or 4/16 Mbps Token Ring LANs with dedicated ATM links. It also allows the integration of ATM networks with legacy LAN networks. This software protocol running over ATM equipment offers two major features:

- The ability to run all existing LAN applications over ATM without change. The immediate benefit is that it is not necessary to reinvest in software applications.
- The ability to interconnect ATM equipment and networks to existing LANs, and also the ability to link logically separate LANs via one ATM backbone. The benefit is that ATM equipment may be introduced only where it is needed.

The function of LANE is to emulate a LAN (either IEEE 802.3 Ethernet or 802.5 Token Ring) on top of an ATM network. Basically, the LANE protocol defines a service interface for higher

layer protocols which is identical to that of existing LANs. Data is sent across the ATM network encapsulated in the appropriate LAN MAC packet format. Thus, the LANE protocols make an ATM network look and act like a LAN, only much faster. (ATM Forum Standards version 1.0 for LAN emulation)

8.3.1 LAN Emulation Components

There are several participants in the LAN emulation (LE) protocol operation: the LAN Emulation Client (LEC), the LAN Emulation Server (LES), the LAN Emulation Configuration Server (LECS), and the Broadcast and Unknown Server (BUS).

8.3.2 Location of LAN Emulation Service Components

While the ATM Forum specifies that there are three separate *logical* components to the LAN Emulation service (the LES, LECS and BUS), it deliberately does not specify whether they are *physically* separate or united. This decision is left to the vendors.

Many vendors merge the LES, LECS and BUS into a single physical unit. There have been two popular choices where to place this unit:

1. Adding the LE service functionality into switches.
2. Providing an external station which connects up to any switch and provides LE services.

9 APPLICATION REQUIREMENTS

The requirements of every application involved in Power System Control and Protection depends on many factors such as Power System topology, voltage levels, etc. and also varies from country to country. Former CIGRE works have gathered these requirements and produced an agreed compilation of requirements which have been used, together with the requirements of the IEC 61850 standard, as a reference in this chapter.

Application performance greatly depends on communication performance in terms of capacity and total latency. Communication performance requirements are developed in chapter 9.1 whereas application performance requirements are summarised in chapter 9.3.

9.1 IEC-61850 Performance Requirements

The IEC 61850 structures Protection and Control functions in terms of Logical Nodes (LN) that may be located in different devices communicating through an Ethernet network. The performance of the Ethernet LAN and particularly the "Transfer time" of messages between LNs are therefore essential for the proper performance of the Substation Automation System (SAS) functions.

The term "Transfer time" refers to the complete transmission time of a message between two physical devices connected by means of a communication system.

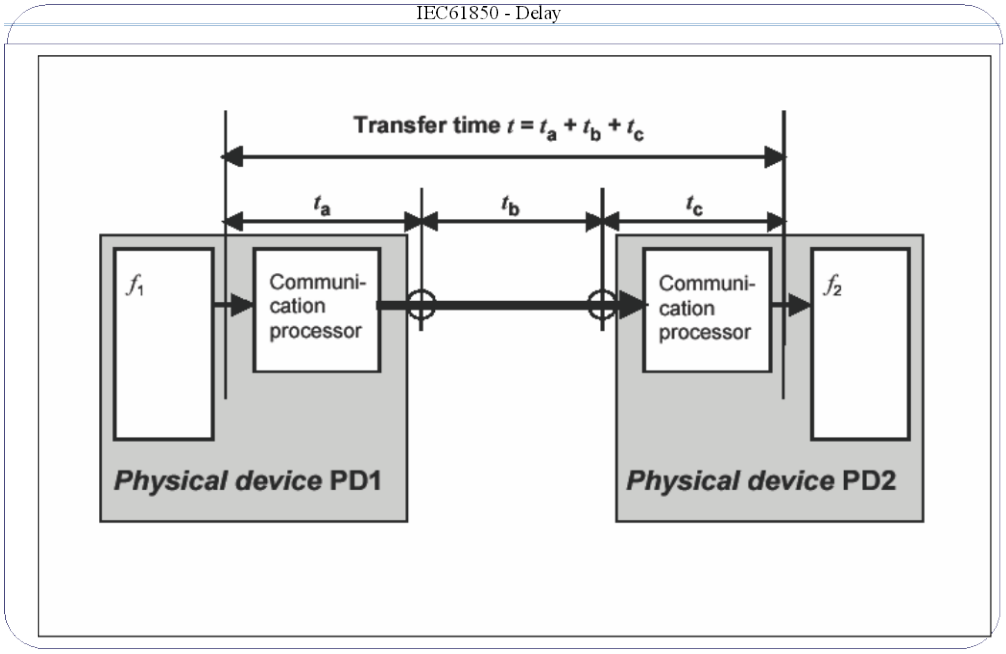


Figure 9.1 – Transfer Time [ref 19]

The transfer time is defined as the addition of the processing time of the communications stack of the IED emitting the message (ta), the Ethernet network transmission time (tb), and the processing time of the communications stack of the IED receiving the message (tc). On the other hand, IEC61850-5 (refer to [19]) specifies that the processing times ta and tc cannot surpass 40% of the total transmission time. As a result of this, tb has an upper limit of 20% of

the transmission time, and this percentage equals 600 microseconds for the most restrictive case.

The standard IEC61850, in its part 5, states that the maximum transfer time for a given message cannot surpass certain values, depending on the message's priority. Some of them, such as type I messages, require that this time shall not exceed 3 milliseconds.

Time constraints for different services are defined in IEC61850-5 and can be summarized as shown in figure 9.2 shown below.

Type	Max Delay (ms)	Message Type Description
1	<10	Fast messages, typically for binary signals transmitted between controllers attached to the same communication network (LAN). Even faster times for high performance transmission applications.
2	<100	Medium speed messages; with a total transmission delay of less than 100ms.Type 2 is used for monitoring functions.
3	<500	Low speed messages with total transmission delay below 500ms, typically used for parameter access.
4	4	Raw data messages with sampling.
5	>1000	File transfer functions.
6		Time synchronisation messages. Accuracy of 1ms (time tagging of events) and 0.1 ms (synchrocheck, point on wave switching) defined for control and protection; down to 1 ms for synchronised sampling. Delay is less critical than jitter. Time performance classes are depicted in figure 9.3
7	>1000	Command message with access control are commands typically received from outside the SA system, which require authority checks.

Figure 9.2 – Message types according to IEC61850

Time perf. class	Accuracy	Purpose
T1	±1ms	Time tagging of events on bay level
T2	±0.1ms	Time tagging of zero crossings and of data for the distributed synchro check. Time tags to support point on wave switching.
T3	±25µs	Synchronised sampling and advanced functions.
T4	±4µs	
T5	±1µs	

Figure 9.3 – Synchronization and time tagging

The use of Ethernet for substation communications with IEC61850 requires that:

- ⇨ EMC and environmental requirements be met by the communication equipment as stated in IEC 61850-3.
- ⇨ all links support 100Mbps, full-duplex interfaces throughout the plant.
- ⇨ critical real-time data be transmitted with multicast communication throughout the plant and at the same time, traffic to be kept as localised as possible to the data sources and sinks.

The use of well-designed, and possibly dynamic VLANs, can help to solve this problem by filtering the relevant traffic. The VLAN identification can not be assigned per port of a switch but needs to be carried in the telegrams if optimum system operation is to be achieved.

The most important functions in a SAS relate to protection of the primary equipment. If this protection relies on communication, then it must be able to deal with an event avalanche of vertical traffic leaving horizontal communication still functional. Therefore selecting utility communication devices supporting IEEE 802.1p priorities with at least four priority queues is key. Sampled values, GSE communication, and time synchronisation should be configured to use a priority class that is assigned to the high priority queue in the relevant switches. Vertical communication uses TCP and is thus less susceptible to telegram loss, so it should be given low priority.

Redundancy on the Ethernet backbone level is easily achieved without affecting IEC61850 implementations on the IEDs. For protection, complete redundancy is required, meaning that the whole equipment (IEDs and network) is doubled up implying that no special redundancy solutions have to be chosen. In cases requiring redundancy down to the IED, different proprietary solutions are offered.

9.2 Service Availability Issues

Availability of Protection and Control functions depends on different design approaches such as:

- The distribution of the functions on devices and LN allocation
- The implementation of the LAN
- The MTBF of every equipment involved in the implementation of a function

IEC61850 strongly encourages the implementation of a fault tolerant network, with no single point of failure. That means that a single failure in a communications device or a link shall not affect the functionality of the communications network. To achieve this goal in an Ethernet network, the following issues must be taken into account:

- Network topology.
- MTBF of network equipment and components.
- MTTR. It depends on maintenance, spare parts availability, etc.
- Equipment redundancy.
- Service recovery time.

Service availability requirements depend on the function and its criticality. Protection function is the most critical system in the Power System, 99,999% availability is typically required whereas Control functions requires 99,99%.

9.3 Applications Performance Requirements

This section presents the traffic volume and performance requirements and constraints associated to operational Ethernet applications, presented in chapter 2. It is practically impossible to put precise figures to the performance requirements which are by definition dependent on applications, voltage levels of the power network, company and national practice, etc. Here the table intends to give only an outline of data communication capabilities that must be taken into consideration when dimensioning Ethernet connectivities. The values that are given here are based on the traffic that generally is considered as being exchanged rather than the data that is being generated. This being variable among Utilities and applications, there shall inevitably remain areas of uncertainty.

Information used in the section has partially been compiled from Reference [2]. Other references used for the collection of information are acknowledged in the Reference and Bibliography section.

Service	Description & Status	Traffic Volume	Traffic Profile	Availability	Response Time	Data Flow
Substation Control						
Local Substation Control		Measures: 2-5 per bay, 40 bytes Alarms: (1 – 20) , per bay, 40 bytes Indications : (1-8) events/ bay, 40 bytes Commands: (1-5 per bay) , 32 bytes	Measures : Periodic & on threshold Alarms: event driven Indications : event driven Commands :on demand	Critical	1 – 10 sec 1 – 3 sec 1 – 3 sec 0.5 – 3 sec	Substation local
Energy Management / SCADA	Only the traffic out of substation is considered					Substation to Control Centre
Remote Substation Control						Control Centre to Substation
Real Time Protection and Automation						
Protection and Protection initiated automation	At present implemented through dedicated channel and continuous operation (64kbps – 2Mbps)	A few bytes	Event driven	Very Critical	5 – 50ms depending on application	Substation local Substation to substation
Tele-protection	At present implemented through dedicated channel and continuous operation (64kbps – 2Mbps)	Up to 6 commands / feeder	Event driven	Very Critical	5 – 50 ms depending on application	Substation to substation
Zone Protection and Wide Area Control schemes		Around 100 bytes per phasor (including UDP/IP/Ethernet overhead)	Event driven	Very Critical	20 – 50 ms	Substation to substation Substation to Control Centre
Low Speed Substation Automation		A few bytes (5 – 10)	Event driven	Critical	300ms to few sec	Substation local Substation to substation
Time Synchronization and distribution	From event record tag	A few bytes	Periodic	Critical	1 - 60 pulse per minute	Substation local
Security Applications						
Video-surveillance		Several Mbytes	Event driven	Fairly Important	5 – 60 sec	Substation to Management Platform
Cyber-security remote management	Remote access to firewall and barrier data	Several Mbytes	Event driven	Not critical		
Access Control		Few bytes to 1 kbyte	Event driven	Important	5 – 60 sec	
Substation Automation Platform Management						
Substation Automation System Monitoring Data		Up to 100 bytes for a complex failure	Event driven	Not critical	few sec	Substation local Substation to substation
Configuration downloading		Several kbytes	On demand	Not critical		

Service	Description & Status	Traffic Volume	Traffic Profile	Availability	Response Time	Data Flow
Substation data analysis						
Event Reports		Up to 100 info per fault 1 info < 80 bytes	Depends on network and applications Event driven, Burst or on demand	Not critical	From few seconds to several minutes	Substation to Control Centre
Oscillography File Transfer Fault locator	There are protections that register not only the oscillography but also estimates where the fault is located	1 – 5 files / fault 1 file = 20 – 500 kbytes		Not critical		
Confirmation of Parameters/ Setting uploading		Around 100 kbytes per bay		Not critical		
Substation Management						
HV Apparatus Health and Performance Monitoring	Condition Monitoring & Asset Management	Few kbytes	Periodic and event driven	Not critical	Minutes	Substation to Management Platform
Weather and environment Monitoring		Few kbytes	Periodic and event driven	Not critical	Up to 60min	Substation to Management Platform
Site Working						
Safety Information	Exchange of procedure progress to de-energize a circuit	Several kbytes	On demand	Very critical	1 min	Substation to substation Substation to Control Centre
Online Documentation		Several Mbytes	On demand	Not critical	Minutes	Substation to Central Server
Substation Operational Voice System						
Substation Control Room Emergency Telephone		1 – 3 Telephone lines per Substation	On demand	Very critical	Delay < 150ms Jitter sensitive	Substation to Control Centre
Switched telephone access in the substations	Connections between IP PBX, Call Servers and remote telephone sets	10 - 50 telephone extensions	On demand	Not critical	Delay < 150ms Jitter sensitive	Substation to substation Substation to Control Centre
Commercial Applications						
Revenue Metering		Several kbytes	Periodic	Not critical	Few min	Substation to Management Platform
Energy Quality Monitoring		100s of kbytes	Burst or on demand	Not critical	30 min	Substation to Control Centre

Service	Description & Status	Traffic Volume	Traffic Profile	Availability	Response Time	Data Flow
Collaborative Multi-media Communications						
File Transfer, web-traffic, Client-server applications Videoconferencing		Several Mbytes per session	Burst, on demand	Not critical	Seconds to few minutes	Substation to Central Platform
Telecommunication Network Management						
SDH/PDH and IP Network Fault Management and Performance Monitoring	Point-to-point links connecting Mediation Device to the Management Centre	Several kbytes	Periodic and event-driven	Not critical	Second to few minutes	Substation to Management Platform

Figure 9.2 – Operational Services using Ethernet infrastructure in the Electrical Power Utility

10 ARCHITECTURAL DESIGN GUIDELINES

Implementing a Wide Area Ethernet infrastructure for operational applications of the Electrical Power Utility requires an adequate architectural design. The previous sections of this document described the technical principles, the different underlying transmission infrastructures and the functional building blocks that may be employed. However, it should be noted that the simple "plug and play" concepts commonly assumed in the deployment of office networks are far from being sufficient when time-critical power applications with high availability and fault tolerance are to be supported. Moreover, the severe environment of the electrical substation requires particular attention to be given to the electromagnetic immunity of the equipment, the choice of connectors and cables, as well as the installation practice employed in the deployment of the system.

The present chapter provides design guidelines for the implementation of time- and performance-critical Wide Area Ethernet infrastructures. The environmental and mechanical issues and corresponding guidelines are discussed in the next chapter.

10.1 Performance

The most essential aspect of architectural design for an operational Ethernet is the control of performance as experienced by the different service users across the network. Performance can be qualified as the capability of delivering data with an appropriate throughput, in adequate and constrained time, and with an appropriate level of service availability. These service attributes can be achieved through a number of network design rules and precautions and using certain Ethernet techniques as described hereafter.

An appropriate level of service performance depends also on further factors such as resilience and fault tolerance which are discussed in following sections of the present chapter.

10.1.1 Network Throughput and Full Duplex Operation

Network throughput can be defined as the maximum amount of data the network can handle without loss or service degradation. The main factors that affect network throughput are:

- ⇨ Network topology design - the first and most important issue is defining the topology of the network, and the characteristics (speed, type) of the links which will be used in the network. Throughput bottlenecks (i.e. low capacity trunk links or links aggregating several other Ethernet links of similar capacity) should be avoided.
- ⇨ Full vs Half duplex operation - Ethernet LAN throughput depends indeed on the capability of Full Duplex or Half Duplex operation modes.

Full duplex is a method by which the communication can be carried out in both directions with the same capacity. Full duplex in principle has double capacity compared to half duplex. It should be added that Ethernet traffic is in general non-symmetric especially in the substation environment. The effect of Half Duplex operation on the actual traffic needs to be considered at the design stage.

IEEE802.3x – Full Duplex Operation

Full duplex mode, when implemented in all ports, ensures that no collisions occur and thereby makes Ethernet deterministic, eliminating one of the most critical issues about using Ethernet in operational applications.

Ethernet is a packet based communications technology where an IED may start transmitting a data packet at any time. The function of a switch is to prevent collisions of these packets and to send the packet in the direction of the desired recipient. This is done using the descriptively named ‘store and forward’ process where received packets are buffered in memory on ingress, placed in a queue for the egress port, and then transmitted once the packet reaches the front of the queue. It is the queuing mechanism that eliminates collisions and allows full duplex operation. This is in contrast to repeaters or hubs of the past that used CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to detect that a collision occurred and then retransmitted a random amount of time later. Determination of the egress port is done via MAC address lookup and learning of addresses which makes this entire operation automatic.

Repeating versus Switching
Bridging implies connecting two or more network segments at the data link layer (layer 2) of the OSI model. Bridges are somehow similar to repeaters or network hubs, i.e. devices that connect network segments at the physical layer. However, a bridge works by using bridging where traffic from one network is managed rather than simply rebroadcast to adjacent network segments. In Ethernet networks, the term "bridge" formally means a device that behaves according to the IEEE 802.1D standard - this is most often referred to as a ‘network switch’ in marketing literature.

	Hub	**Bridge**	**Switch**
Basic Function	Layer 1 multi-port signal repeating	Layer 2 traffic forwarding	Layer 2 traffic forwarding
Forwarding Throughput	Low	Medium	High
Full Duplex/ Half Duplex	Only Half	Half/Full	Half/Full
Network Segmentation	No	Yes	Yes

Analyzing the previous table, demonstrates that a switched Ethernet network has clear advantages regarding network capacity and scalability, and makes this approach suited for Substation and Power Automation applications:

- The network is segmented, the switches look upon the destination MAC address in the Ethernet header, and forward the frames only to the port where this MAC is located. This makes the network much more efficient.
- The forwarding is hardware-based, thus latencies are kept low and this is critical for delay sensitive applications, such as Goose or Sampled Value messages.

10.1.2 Network Availability

Business implications and operational impacts of “network downtime” in the communication system of the power delivery process are evident and need not be developed here. It can

therefore be stipulated that from a Utility perspective, the operational Ethernet network must have the best achievable availability.
A*vailability is* a service-related statistical parameter which can be defined as the probability of proper operation of the network for a given data exchange. It is normally quoted as a percentage of "up" time of the network, or the percentage of time that the network can effectively forward traffic (e.g. 99.999%). It can be estimated theoretically and measured practically on a network-wide or per-circuit basis. Circuit monitoring facilities must be implemented in order to measure continuously the availability of communication services across the Ethernet network.

Availability is generally expressed as:

Availability = MTBF/ (MTBF+MTTR)
(MTBF = Mean Time Between Failures, and MTTR= Mean Time To Restore)

In order to enhance network availability, one should simultaneously improve three parameters:

- Reduce the occurrence of link and device faults. This can be achieved through more reliable and robust network devices (e.g. Ethernet Switch) and better protected transmission infrastructure used for linking of network nodes
- Reduce the effect of link and device faults. This can be achieved through a more fault tolerant network topology as described in section 10.2 hereafter, and duplication of network switches, routing resiliency, and "dual homing" of IEDs and other devices requiring communication services as described in section 10.6 hereafter.
- Reduce the duration of the down-time following a network fault. This can be achieved through a better service restoration scheme and implemented network management tools and techniques , as discussed in 10.4 hereafter allowing the user to monitor and manage circuits, devices and hence the network as a whole.

10.1.3 Quality of Service (QoS)

Although QoS is generally a layer 3 (and above) issue, the Ethernet layer provides Class of service by means of Priority Assignments which is a determining factor for the overall performance that can be obtained in the overall network. To achieve full Quality of Service a combined layer 2/layer 3 approach has been given in this section.

Ethernet is a robust technology originally designed to work on poor media. Now it is being used with far more stable and reliable transmission media and technologies and hence is a very reliable communications technology.

Typically data networks forward traffic using a best effort policy, in which all traffic has the same priority. In case of congestion traffic is discarded, independently of its importance.

To prevent this problem Quality of Service (QoS) policies must be used. Priority assignment, dedicated bandwidth, controlled jitter and latency (e.g. for real time traffic) and improved loss characteristics are typical QoS goals.

It is important to emphasize that providing priority for one or more traffic flows does not make other flows fail, as long as there is enough networking bandwidth available to forward the traffic.

Configuration and parameter setting of QoS can be a complex task to overcome in data, voice and video networks. Initially it is recommended to do a network study in order to understand its traffic patterns. It is also important to keep in mind that network traffic pattern can differ during network life cycle and that specific applications with different priority requirements (e.g. SCADA) can exist in the network. QoS configuration is a continuous optimization task, therefore it is recommended to schedule network surveys for precise measurement of the network's QoS characteristics (latency, jitter, bandwidth, and packet loss).

QoS mechanisms guarantee that in network congestion situations, critical traffic (marked as important or real-time) is prioritized and always routed across the network to its destination. To configure QoS parameters normally there are a set of mechanisms available in routers/switches:

- ⇨ Classification – Process used in the network entering point where the traffic is identified according one class of traffic and QoS level are attributed to the traffic flows;
- ⇨ Congestion management – Mechanisms to queue the service flows in different ways in order to provide preferential treatment to a certain flow(s);
- ⇨ Congestion avoidance – Traffic queues in routers/switches are controlled to prevent from filling, to allow high-priority traffic to enter the queue;
- ⇨ Shaping and Policing – Mechanisms used to limit the bandwidth for the traffic. If the traffic exceeds authorized bandwidth the policy decides if it is discarded or marked with lower priority;
- ⇨ Link efficiency – Provides a method of delay justification, normally experienced on low speed transmission links.

In Ethernet networks the priority field within the Ethernet frame structure, according to IEEE 802.1Q/p, is used to differentiate the traffic into the network from best effort to real time. A generally accepted scheme would be as follows:

- Priority level 0 – Best Effort (ordinary LAN)
- Priority level 1 – Background (specific applications)
- Priority level 2 – not defined (reserved)
- Priority level 3 – Excellent effort (business critical)
- Priority level 4 – Controlled load (streaming multimedia)
- Priority level 5 – Voice and Video (< than 100ms latency and jitter)
- Priority level 6 – Voice and Video (< than 10ms latency and jitter)
- Priority level 7 – Network control, critical, reserved traffic

In power delivery system applications, no dedicated priority assignment scheme has so far been established. This depends upon the specificities in each case and the applications which are integrated into the same Ethernet environment. Typically, multiple LANs (Process, Voice, SCADA, Management, etc.) are implemented inside the substation and multiple Ethernet connections are created to the outside world. These architectural choices and service integration/separation philosophy are beyond the scope of the present document.

Measurement of QoS parameters is also a requirement for service level specification auditing, the verification that both the user and network behave in compliance with the required levels.

Some QoS parameters that should be measured include:

- Latency – As a generic definition, latency is the amount of time it takes a packet to travel from source to destination. This total latency time can be sub-divided into media latency and network active components latency such as switches latency, with typical values around 10 microseconds for a 64 byte GOOSE-like message over a 100M Ethernet link including one switch (refer to [20]);
- Jitter – Jitter refers to the allowed variation of the switch latency, normally +/- 2 microseconds (excluding queuing delay);
- Throughput – amount of digital data per time unit that is delivered by a link or channel usually measured in kbps or Mbps;
- Bandwidth – Network bandwidth is normally referred to the amount of data transmitted in a given period of time, normally measured in Mbps;
- Packet/Frame Loss – Is defined by the number of frames transmitted successfully from the source but were never received at the destination. Is normally expressed in percentage of total frames transmitted (e.g. from 1000 frames transmitted, 900 were received corresponds to 10% of frame loss);
- Back-to-Back frames – Defines the maximum number of frames that the device under test (networks equipment) can process without losing frames.

The measurement of QoS parameters including throughput, latency, frame loss and back-to-back frames as well as the definition of methodology and test equipment are specified in [21].

10.1.4 Ethernet Broadcast Control

In operating networks there are situations that can decrease network performance or network availability. Ethernet network traffic can be unicast, multicast or broadcast. In the latter cases a single frame may be forwarded to many or all the network segments, eventually occupying a significant amount of the available bandwidth. One such situation happens when broadcast traffic is not handled properly, overloading network processing capacity, and it may even cause denial of service in networking equipment.

The threat can occur when the network is overloaded with broadcast traffic. In this scenario, when networking equipment receives broadcast traffic in any port, they flood it to the remaining ports, overloading the network. There are some protection policies that should be implemented in order to protect the network, namely:

Port rate limiting

This functionality allows configurable rate limiting per port to limit unicast, multicast and flooding traffic. This can be essential to managing precious network bandwidth for service providers. It also provides edge security for denial of service (DOS) attacks.

When an Ethernet switch receives a frame whose destination MAC is not contained in its MAC address tables, it does not know by which port it should egress the frame. In order to discover where the device with the unknown MAC is located, it floods the frame to all the ports of the switch (except the port where the frame was received). This is also the behaviour when ARP protocol messages try to discover which MAC address corresponds to a certain IP address.

Port rate limiting is a very useful feature in order to limit the impact of these phenomena, which cannot be overlooked in an Ethernet network. This functionality allows the user to set up a maximum bandwidth usage for certain traffic types (multicast/broadcast…), and thus ensures that the network will not reach saturation due to this problem.

Broadcast control

Another particular case occurs when an Ethernet frame has as it destination MAC address a broadcast address. Then this frame is egressed at all the switches' ports. Undoubtedly this kind of behaviour can place a burden on network performance, if the number of broadcast frames exceeds a certain limit. As a solution to this problem, a switch can identify, count and limit appropriately broadcast frames in order to not exceed a certain amount of available bandwidth.

Multicast control

Ethernet switches can effectively limit the amount of multicast traffic which traverses a certain port. As multicast MAC addresses have a common pattern (the first bits of the MAC), it is quite straightforward to identify these frames and limit them appropriately.

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

It is an integral part of the IP multicast specification, operating above the network layer, though it doesn't actually act as a transport protocol. IGMP does allow some attacks, and firewalls commonly allow the user to disable it if not needed.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyzes all IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. While a switch that does not understand multicast will broadcast "multicast traffic" to all the ports in a broadcast domain (a LAN), a switch using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces the workload at the end hosts since their network cards will not have to receive and filter all the multicast traffic generated in the network.

In Substation Applications, IGMP allows for multicast data frames, such as GOOSE frames, to be filtered and assigned only to those IEDs which request to listen to them.

10.2 Topology

Ethernet allows for a wide variety of network topologies providing different levels of redundancy, availability, performance and of course cost. Following are several architectures which seem to be emerging as popular amongst utilities.

10.2.1 Cascade

Each switch is connected to the previous switch or next switch in the cascade via one of its ports. These ports are sometimes referred to as uplink ports and are often operating at a higher speed than the ports connected to the IEDs. The maximum number of switches, N, which can be cascaded depends on the worst case delay (latency) which can be tolerated by the system.

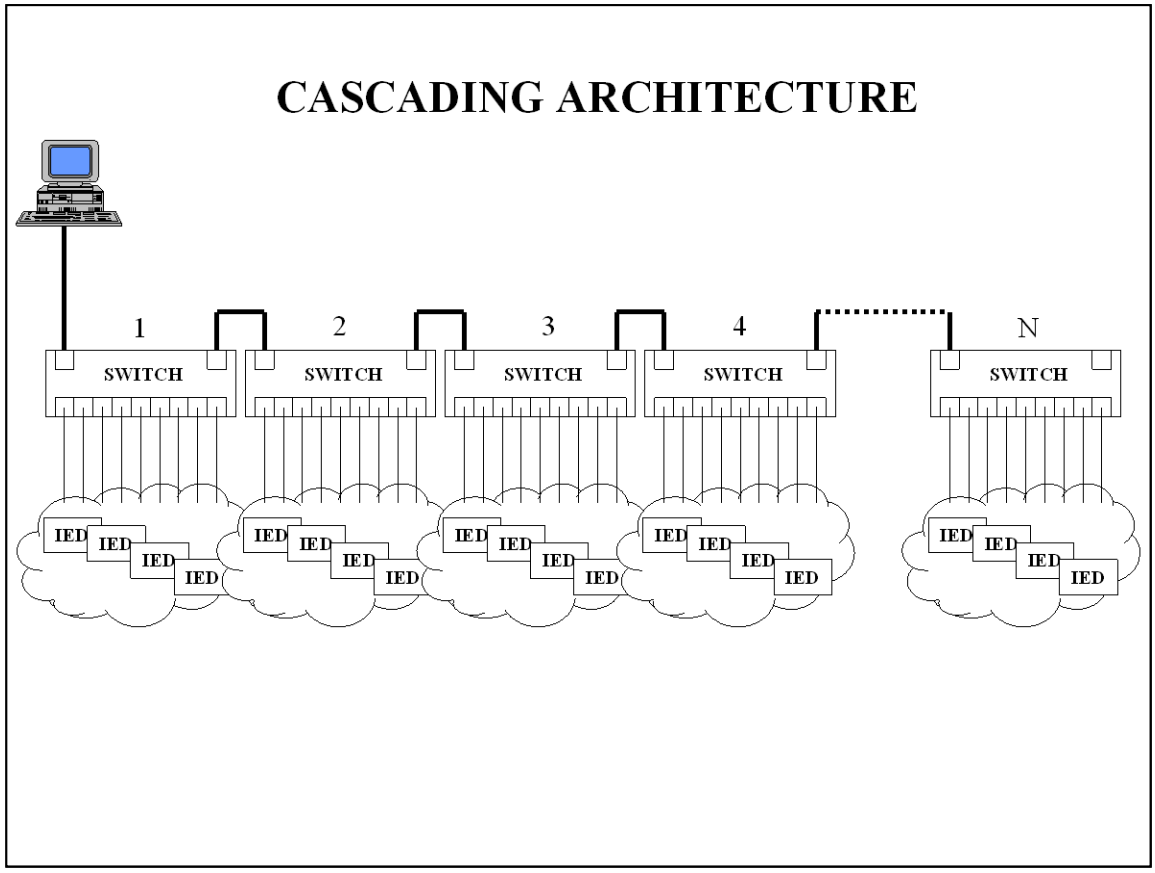


Figure 10.1 – Ethernet cascade topology in the substation [ref 14]

10.2.2 Star Topology

The star topology is based on a “backbone” switch with all of the other switches linking to it.

Advantages:

- Lowest Latency - allows for lowest number of ‘hops’ between any two switches connected to the backbone switch N.

Disadvantages:

- No Redundancy – if the backbone switch fails all switches are isolated or if one of the uplink connections fails then all IEDs connected to that switch are lost.

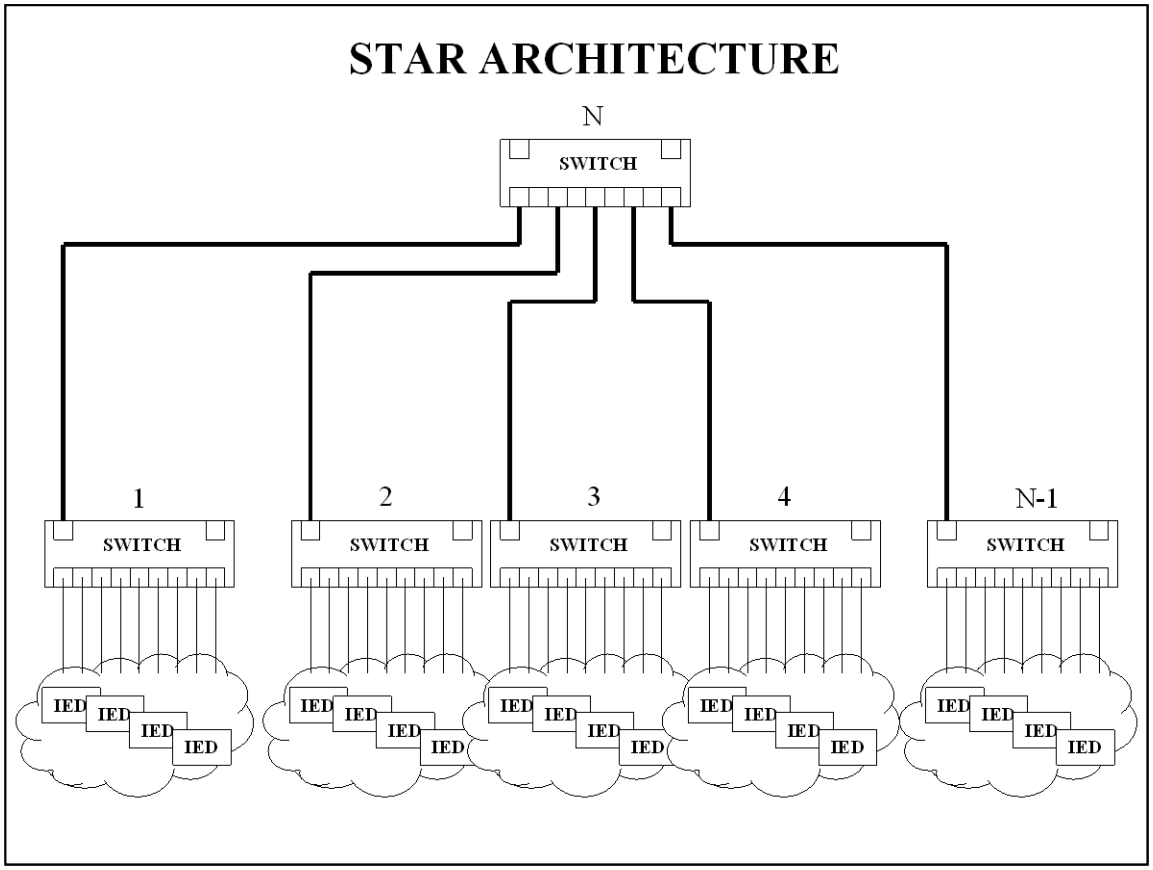


Figure 10.2 – Ethernet star topology in the substation [ref 14]

10.2.3 Ring

The ring architecture provides some level of redundancy as compared to the star or cascade topologies due to the redundant path.

Theoretically, messages could circulate indefinitely in a loop and eventually eat up all of the available bandwidth. However, ‘managed’ switches take into consideration the potential for traffic loops and implement an algorithm called Spanning Tree Protocol (STP) which is defined in the IEEE 802.1D standard. Spanning Tree allows switches to detect loops and internally block messages from circulating in the loop. As a result managed switches with Spanning Tree actually logically break the ring by blocking messages internally. This results in the equivalent of a cascading architecture with the advantage that if one the links should break the managed switches in the network will reconfigure to span out via two paths.

Advantages:

- Rings offer redundancy in the form of immunity to physical breaks in the network.

- IEEE 802.1w Rapid Spanning Tree Protocol allows sub-second network reconfiguration.
- Cost effective cabling/wiring allowed. Similar to Cascaded architecture.

Disadvantages:

- Latency – worst case delays across the cascading backbone have to be considered if the application is very time sensitive (similar to Cascading)
- All switches should be Managed Switches. This is not necessarily a disadvantage per se but simply an added complexity. Although, the advantages of Managed Switches often far outweigh the added complexity.

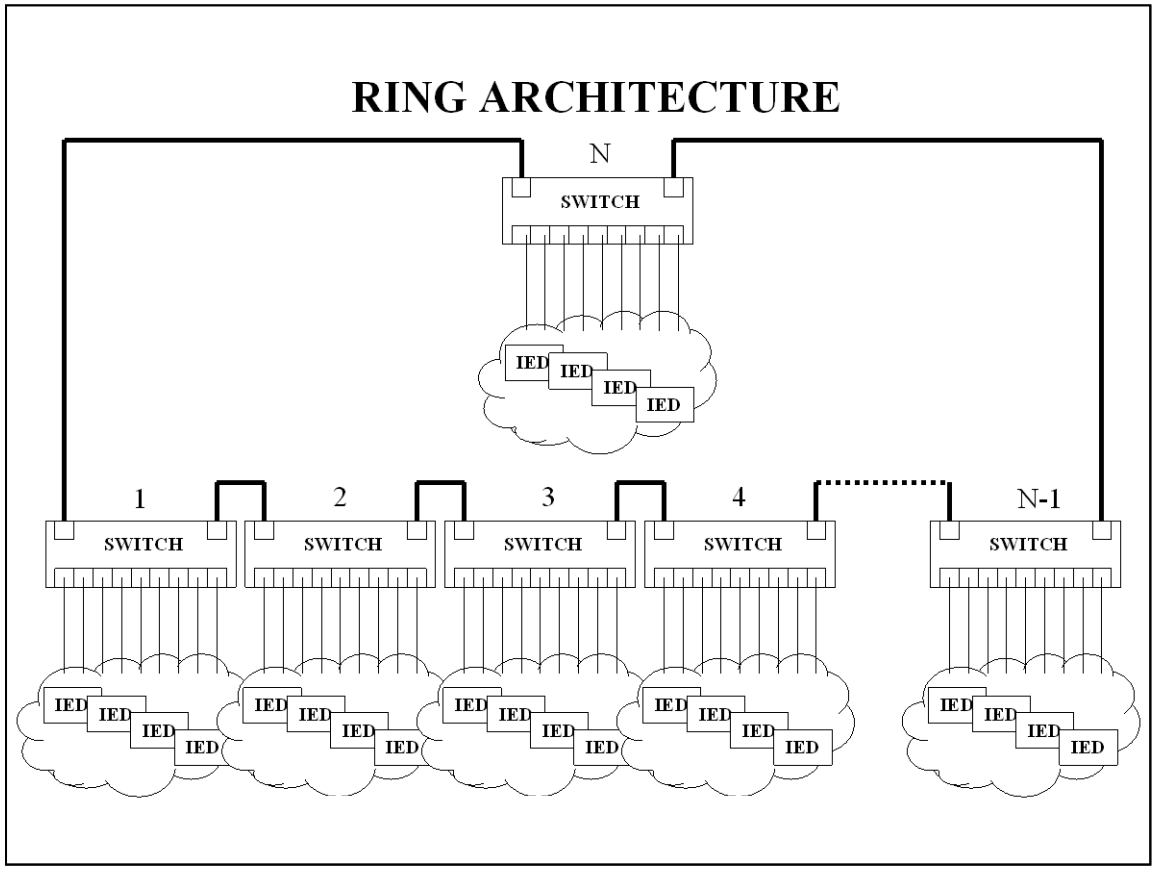


Figure 10.3 – Ethernet ring topology in the substation [ref 14]

10.2.4 Hybrid Architecture

The Hybrid architecture combines star and ring topologies, as shown in the figure below. This architecture can withstand anyone of the fault types shown in the figure and not lose communications between any of the IEDs on the network. In this way, a high level of availability (i.e. uptime) is achieved.

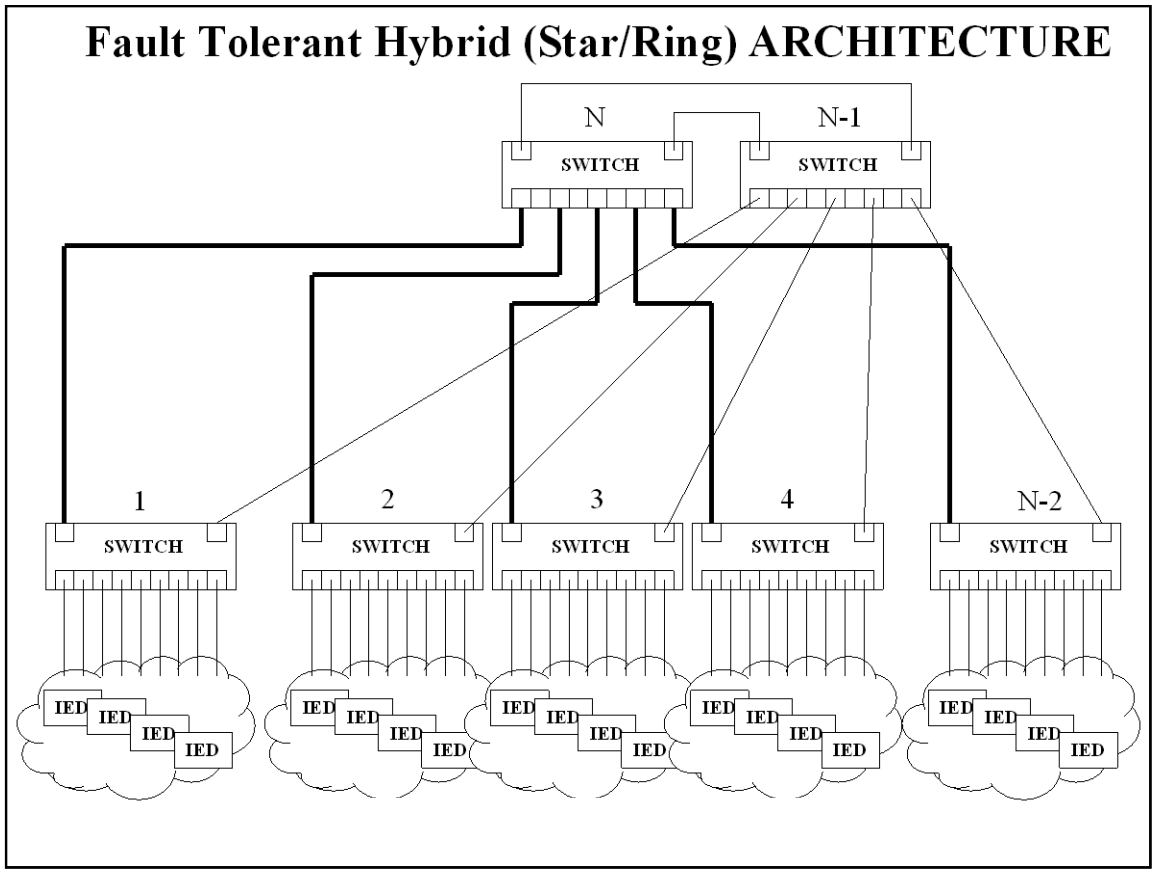


Figure 10.4 - Star/ring hybrid topology tolerant to link and core node faults [ref 14]

10.2.5 Mesh Topology

A Mesh is a topology where devices are interconnected via many redundant paths, therefore increasing availability but also increasing complexity. In a mesh topology if any cable or node fails, there are many other ways for two nodes to communicate. Mesh topology is indeed present at the IP layer implicating routing but also it can be implemented at the Ethernet level through the use of a Spanning Tree as already described in Section 3.2.
Mesh topologies are commonly used in Wide Area Networks and in Wireless Sensor Networks.

Advantages:

- ⇨ High levels of redundancy and availability /survivability
- ⇨ Flexible architecture - The network can be expanded without disruption to other nodes

Disadvantages:

- ⇨ Increasing complexity
- ⇨ Difficult to manage and troubleshot

10.3 Scalability

Scalability is the capability of the network to increase several orders of magnitude in performance and capacity in order to fulfil future network requirements. The scalability concerns the network's architecture, structure, technology and manageability but not necessarily the equipment. This means that although network equipment may need to be changed in future for extension beyond the original spare capacity, or for newer functions and firmware versions, the principles of the network design and its architecture are preserved, avoiding costly redesign and restructuring.

In the power environment, many applications and services are not already implemented and therefore the scalability is one of the important parameters to be taken into account during the design stage.

The following gives some guidelines as to the scalability of the system:

- Architecture – A proper mix of layer 2 and layer 3 must be used to build the network architecture in order to control the performance and the security of the system in a scalable manner.
- Topology – Topology is generally a limiting factor to network growth. A pure topology as described previously (star, cascade or ring) cannot be scaled in a convenient manner. Scalability in the power environment implicates the use of a hybrid topology.
- MAC Addressing space – For large flat networks the size of the MAC address table can become very large. In order to keep the network scalable it is necessary to split the large Ethernet structures into multiple sub-networks separated through layer 3 (refer to Architecture here above).
- VLAN planning – The separation of the different categories of services into identified VLANs from the early design stage avoids the network to grow up to saturation.
- Manageability – Manageability is the aptitude to scale up and keep operating at a large scale without downtime or a large effort for administration. The architectural control described previously and avoiding too much complexity at each Ethernet level provides a scalable manageability.
- Protection mechanisms – Protection mechanism has also clear limitations relative to scalability. The protection strategy of the Ethernet structure must employ the different mechanisms (ring protection, Spanning Tree, layer 3 resilience) in a coordinated manner and combined to provide appropriately scalable resilience.

10.4 Management

The Ethernet infrastructure delivers the required level of performance only if it is adequately managed, that is to say planned, configured, monitored and maintained.

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Generic description of Network Management and its ITU-T defined constituents are already treated in previous CIGRE Technical Brochures (ref. [21]) and shall not be reproduced in the present document. The following description is related to those aspects which are specific to Ethernet networks.

Ethernet Network management consists of different views depending on the time scale and operational roles:

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- Maintenance is concerned with performing repairs and upgrades, patch installations, equipment replacement, and addition of new switches. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.
- Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

It is worth noting that many network components in particular those which are in the substation automation systems may be under the management of the substation automation system or the telecommunication management system, or both. It is therefore important to define clear boundaries between the two management platforms (e.g. visible under one platform and controlled under the other, etc.).

The management facilities associated to the Ethernet infrastructure allow the following tasks:

- Device management - this is the set of functions and tasks that allow each individual component of the network (switch, etc.) to be configured and monitored. The low-end industrial switches normally are not remotely manageable. Device management is generally vendor-specific even if in general it uses SNMP protocol to communicate from the switch to the management platform. It is generally possible however, to retrieve fault information through a vendor-independent SNMP fault management platform.
- Network management – Network management of an Ethernet infrastructure concerns tasks at switch level with an overall effect on the Ethernet network. It includes end-to-end visibility, VLAN management, performance monitoring, priority assignments and management of network resilience. These tasks are made possible by a number of separate communications protocols that operate at various layers.

Management data is collected through several mechanisms, including agents installed on infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring.

Network Management of Ethernet infrastructures is associated with the Simple Network Management Protocol (SNMP). This allows vendor-independent access to all network components. SNMP-based Network Management Systems (NMS) offer the following basic functionality:

- Dash board
- Path monitoring, availability, performance, services, statistics, history, alarms
- Graphical representation of physical and logical network
- Device configuration

10.4.1 Fault-management

Fault management in Ethernet refers to the set of functions that detect, isolate, log, notify and ultimately correct malfunctions in a communications network. It is based on the information transmitted through SNMP (or SYSLOG) and involves tracing and identifying faults, sending or receiving fault notifications, performing diagnostics tests, and correcting faults, on the reported error conditions. Fault information can also be transmitted to the operational scada or substation automation management platform through SNMP, major/minor alarm dry contacts or through various protocol converters.

A fault management console allows a system operator to monitor events from multiple systems and perform actions based on this information. A fault management system should be able to correctly identify events and automatically take action, either launching a program or script to take corrective action, or activating notification software that allows a human to intervene (i.e. send e-mail or SMS text to a mobile phone). Some notification systems also have escalation rules that will notify a chain of individuals based on availability and severity of alarm.

There are two primary ways to perform fault management:

- ***Passive Fault Management*** The NMS waits for, and collects messages (SNMP notifications for example) from devices when an event occurs. If the device in question fails completely or locks up, it won't generate an alarm and the problem will not be detected.
- ***Active Fault management*** addresses this issue by actively monitoring devices via tools such as PING to determine if the device is active and responding. If the device stops responding, the NMS generates an alarm showing the device as unavailable and allows for the proactive correction of the problem.

10.4.2 Performance monitoring

The concept of Performance *Monitoring* overlaps 2 categories in the FCAPS model (ITU-T functional model for Fault, Configuration, Accounting, Performance and Security Management), Accounting/Administration, and Performance Management, and relates to performance monitoring at the device rather than at the network level.

Local, interface-specific performance statistics related to the connected Ethernet segment are reported by the hardware's Remote Monitoring (RMON) capabilities for monitoring purposes. The data is often stored in, and made available to the NMS via, the device's local SNMP Management Information database (MIB).

Aside from simply storing statistics about traffic on the local segment, RMON can assist with fault diagnosis if configured to work with the device's alarm system. In this context, triggers or thresholds can be set such that, when a given monitored statistic exceeds the configured threshold, an alarm is raised, and an SNMP trap is generated and sent to the NMS.

In addition to the above, managed devices should also provide performance information regarding the device CPU, RAM, disk, etc. usage.

10.4.3 Traffic monitoring

Traffic Monitoring is an important source of feedback which can be used to validate the dimensioning of the Ethernet infrastructure. Traffic monitoring at Ethernet frame level can also serve for checking of MAC addresses at the switch level in order to detect security intrusion (refer to section 10.5).

Unless port mirroring or other methods such as RMON are implemented, it is difficult to monitor traffic that is bridged using a switch since only the sending and receiving ports can see the traffic.

- ⇨ Port Mirroring is a powerful tool for troubleshooting in the Ethernet network. The switch sends a copy of Ethernet frames to a monitoring network connection.
- ⇨ Connecting a hub between the monitored device and its switch port to monitor the traffic. Unlike the Port Mirroring which is non-intrusive, this technique reduces the throughput.

10.4.4 Traffic Engineering

Traffic Engineering is the facility to shape and route traffic from different sources in an optimized manner. At present, despite some bandwidth management capabilities in Ethernet, full Traffic Engineering can only be performed at higher layers (refer to [23]).

Traffic Engineering consists of measuring, modeling, planning, and optimizing and protecting networks to ensure that they carry traffic with the speed, reliability, and capacity that is appropriate for the nature of the application and the cost constraints of the organization. Different applications warrant different blends of capacity, latency, and reliability.

The elaboration of a new IEEE standard treating traffic engineering in Ethernet is in progress: IEEE 802.1Qay - Provider Backbone Bridge Traffic Engineering (draft).

10.4.5 Configuration management

Configuration management (CM) focuses on establishing and maintaining consistency of a product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. In the context of the Ethernet infrastructure, CM refers to monitoring network configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Hardware configuration management maintains a record of all network components and their respective documentation, providing support information to different actors as to the type, physical locations and links between them. This information is typically stored in a configuration management database (CMDB).

In the framework of Substation Automation, the Ethernet switch can be assimilated to a substation Intelligent Electronic Device (IED). Current standardization within IEEE C37.2 is planning to attribute a power system device function number to the LAN Switch so that it may be incorporated into drawings in a more consistent manner. The ANSI device number of '16S' proposed for a network switch may one day become as common on one-line diagrams as a '52' breaker!

10.5 Ethernet Security

No discussion of networking is complete without a mention of cyber security. Though the substation LAN is a private network, interconnection to a wide area network is inevitable and this brings the potential for tampering. The substation gateway provides security from the WAN via firewall and encrypted VPN operating at higher layers. However, configuration mistakes do occur and loopholes do exist.

The best approach to security is a layered defence and the managed Ethernet switch provides several approaches. VLANs can segregate the network to isolate critical applications such as GOOSE and sampled values, on the network. Switches have management security via SSL/SSH (Secure Sockets Layer/Secure Shell). Port security and IEEE 802.1x, as discussed in section 3.5, can be deployed to deny physical access to the network; for example, one can connect only recognized laptops to the LAN. Rate limiting can be used to prevent rogue or broken devices from poisoning the network. Finally, the IEC 62351 working group is currently exploring methods for making IEC 61850 and GOOSE messages more secure from tampering. This will further reinforce cyber security in the substation.

10.5.1 Practices and policies

There are several steps in order to implement a secure Ethernet environment. Some guidelines follow:

- Understand the risk – At this point it is necessary to identify all systems and network connections, understand the possible threats, identify process/business impacts of security incidents and evaluate the possible vulnerabilities.
- Security improvements – There are at least two possible actions to be addressed, the short and long term implementations. For the first group, simple actions can be implemented in order to increase security (e.g. remove unnecessary network connections/accounts/access; change passwords; unplug modems; optimize management of existing assets). For the second group, proceed with some network modifications (e.g. use of DMZ, Firewalls, IDS/IPS, etc), use of anti-virus and encryption for the data transferred and increase physical security to the network.

- Establish policy, standards and procedures – There are several entities (BS, ISO, ISA, IEEE, etc) that provide a clear guidance in security issues through several standards (e.g. BS7799, ISO27001, ISO 177799). In order to improve security there must be a regular review for new threats and risks (regular reviews and audits), confirm that the standards are still up to date and assure the correct compliance with the standards.
- Raise awareness and skills – To achieve this objective the design and operational engineers must be aware of all threats sources and attack methods, vulnerabilities, standards, preventive procedures in case of incident. These skills can be improved through working with IT security professionals or consultants and increase specific training (e.g. firewall configuration and management)
- Establish response capability – To rapidly respond in critical situations several methodologies must be known. Several incident management procedures (list of contacts, permanent management teams, communication and notification mechanisms, training, others) must be defined in order to archive a fast response in case of critical situation. Other processes that can also be considered are the implementation of automatic cyber response mechanisms (disaster recovery systems, automatic backup plans, redundant mechanisms and communications, etc).
- Manage third party risks – The access to Internal SCADA, telecom and IT networks must be restricted to internal staff. Outsiders/vendors access must be avoided and if necessary several preventive actions and measures must be applied:
    - Use of DMZ zones (DeMilitarized Zone) where the risk can be controlled and restrained
    - Use of firewall rules to configure several access profiles
    - Encourage vendors to address security proactively
    - Implement appropriate network connections/segregation
- Engage projects early – The following aspects must be taken into consideration:
    - Include security requirements in projects specifications;
    - Provide all security specifications to internal personal and suppliers in order to make them familiar with those policies and standards;
    - Promote frequent security testing into the network (e.g. penetration testing) and put in practice preventive procedures.

Security must be a constant improvement process; there are always details that can be changed in order to comply with new standards or guidelines, or to deal with new and evolving threats.

For a more detailed discussion of some of these areas, the reader is referred to the CIGRE D2 Technical Brochure “Treatment of Information Security for Electrical Power Utilities” (2009).

Fig 10.5 - Security – Constant improvement process

10.5.2 Remote Access

The management and supervision of the entire data network is one important daily routine, therefore it is commonly necessary to verify, modify and analyze equipment configurations. If the network is spread geographically (LAN/MAN/WAN) it is impossible for the user to locally manage it so the solution lies in remote access.

In remote access the user establishes one direct connection/session with the network equipment where management actions must be done and more importantly has remotely the same management options as locally.

Generally, remote access defines the ability to communicate with data processing equipment from a distant location or facility through a data link connection.

This process generally requires a computer (remote client), a data link connection (modem, internet, VPN, etc.) and some remote access software to connect to the remote equipment/network.

To remotely manage network equipment, the following are normally used; TELNET (layer 5 TCP/IP network protocol - IETF STD 8), SSH (layer 5 TCP/IP network protocol - RFC 4251) or HTTP/WEB-BROWSING applications through Virtual Terminal emulation.

Best practices recommend the implementation of a full scale Security System, based on individual username/password and AAA (Authentication, Authorization and Accounting) protocol, as RADIUS (Remote Authentication Dial In User Service), TACACS+ (Terminal Access Controller Access-Control System Plus) or Kerberos. These systems for remote access are normally composed of,

- ⇨ A central or distributed server located at the corporate network level (hardware and software server application);
- ⇨ Remote user client application (normally installed on laptops or PCs;

- A substation-grade router/cyber appliance per substation, with advanced security features such as Firewall, VPN, IDS, etc.

The remote user will first have to present his identification; then request authorization to access a given device at a given substation, the Server will validate all the information and authorize access accordingly by sending the related port information to the relevant cyber appliance at the corresponding substation/remote equipment. The Cyber appliance enables the relevant port and the user receives access confirmation (a key) and only then access to Ethernet equipment is granted.

10.6 Resiliency

Resiliency is the capability of the network to continue delivering communication services in the event of link or device failures. It covers network fault tolerance through different levels of redundancy incorporated into the network and into its components to avoid faulty nodes or links, as well as self healing mechanisms, defined by several Ethernet-related standards, which allow the restoration of service within a reasonable recovery time.

Ethernet infrastructure design comprises the coordination of fault probabilities and mitigations across the network in order to meet service availability requirements. Network design is a trade-off between cost and performance and requires prior knowledge of service objectives. The resiliency design can therefore be defined as follows:

- Define service availability and fault tolerance objectives
- Select appropriate redundancies at different levels (switch hardware, power supply, network ports, transmission links)
- Select an adequate network topology
- Implement adequate restoration mechanisms at transmission and network levels
- Define service continuity objectives and hence maximum acceptable service recovery time

10.6.1 Service Availability and Fault Tolerance Objectives

An overview of communication service availability requirements for different operational and operation support services has already been presented in chapter 9 of the present document. In terms of availability objectives the following table gives some orders of magnitude.

Availability objective	Downtime	Examples of infrastructure	Example of Service
99.999%	5.25 min/year *(~5 Hours/57 years)*	Network node with duplicated common parts	IED connection with dual-homing and protected transmission
99.99%	52.5 min/year *(~5 Hours/ 5.7 years)*	50km of buried optical cable	SCADA with link redundancy
99.9%	525 min/year *(~5 Hours/ 0.57 years)*	Ethernet link through microwave radio	Data service

A common objective for fault tolerance is continued operation in the presence of a single fault (link or node). Fault probability is assumed to be sufficiently low for a double fault to be of negligible probability.

10.6.2 Fault-tolerance and Redundancy Design

As it has been stipulated above, incorporating redundancy into the device and into the network can greatly enhance the network's availability and fault tolerance, but it can also increase considerably the cost of the system for negligible improvement. A meticulous analysis of possible failures must be performed on the complete chain, and reinforcements applied where necessary in order to mitigate different fault situations.

Redundancy can be employed at different levels:

- Module redundancy is the duplication of critical components inside a device in order to reduce its unavailability and/or allow maintenance operations on one component (e.g. duplicated power supply, switching fabric, port hardware, firmware, etc.)
- Equipment redundancy is the duplication of a network device with each device working in stand-alone but for the same purpose or the two working in load sharing, one device being capable of taking over the load of the other in the event of a failure (totally or partially)
- Transmission link redundancy is the duplication of transmission medium and equipment in order to enhance the availability of an otherwise unreliable link.

A common approach to achieve fault tolerance in Ethernet design is "dual homing" as shown in figure 10.6. Dual Homing can be applied to the connection of end devices to the network or to the connection of secondary switches to the core network (Hybrid Star/Ring).

As an IED connection technique, each device has two connections to the network via different switches either as primary/backup links using a single MAC address, or having both links active and using different IP addresses. In the former scheme, the Ethernet switch must support failover and recovery mechanisms.

As a hybrid star/ring switch network, Spanning Tree (RSTP) mechanism determines the frame forwarding in the network.

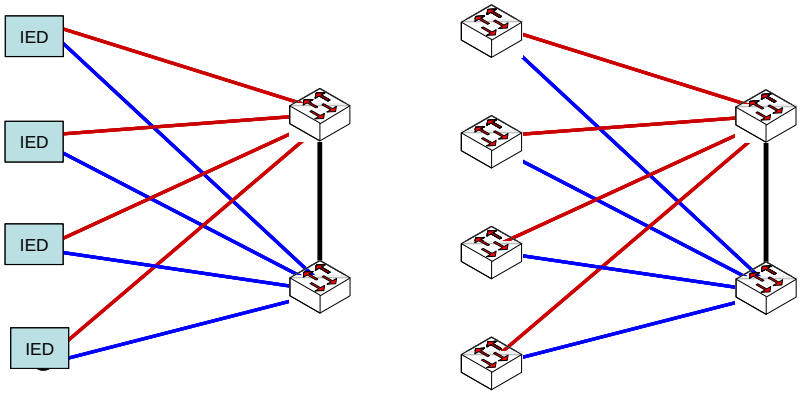


Figure 10.6 - Dual Homing for end device connection and hybrid star/ring switch network

Different faults that can be mitigated in the hybrid star/ring "fault tolerant" network are presented in figure 10.7 hereafter.

10.6.3 Topology

The impact of topology design on the network's resilience has been covered in section 10.2 and demonstrated here above. It should be noted that topology selection highly impacts the cost and complexity of a solution. Moreover, topology selection is highly dependent on the required coverage, transmission media and the dispersion of end users. Except some basic rules such as "no single point of failure" which is part of normal practice in operational network design, it is extremely hard to produce general rules and recipes. It can only be repeated (once more) that a global approach to availability and fault tolerance is necessary: a chain is no stronger than its weakest ring!

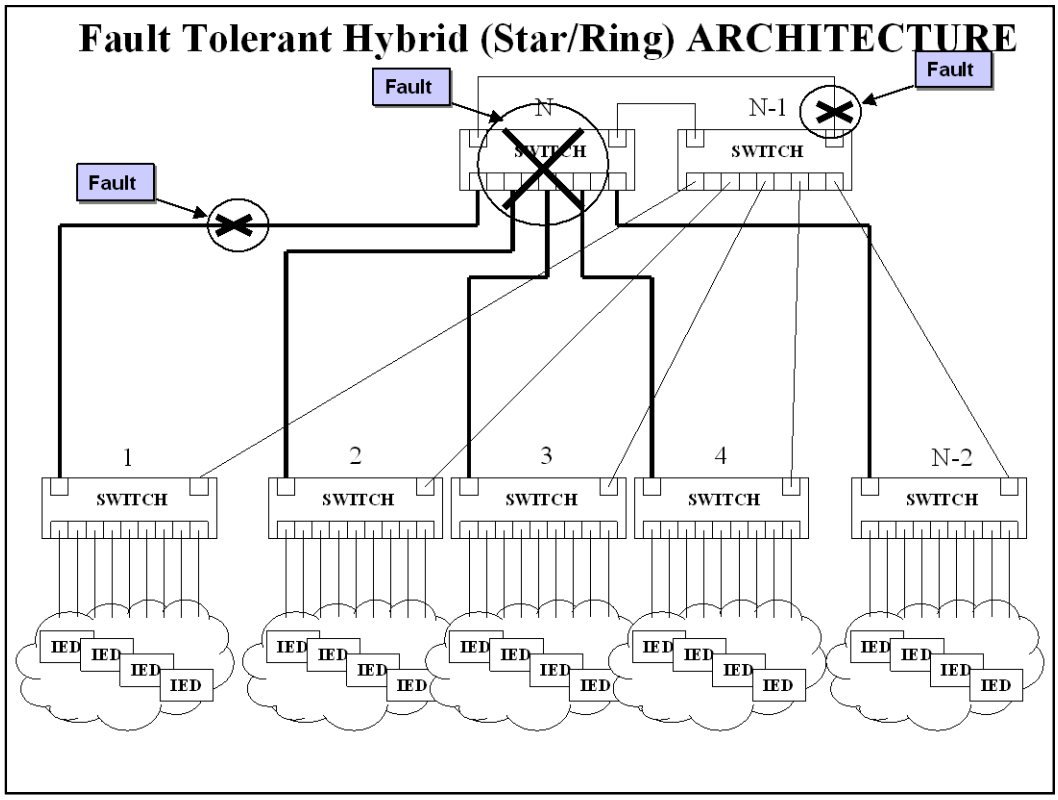


Figure 10.7 – Fault-tolerance in a hybrid topology star/ring network

10.6.4 Restoration Mechanisms and Recovery Time

The resilience of an Ethernet infrastructure relies highly upon the existence of alternative ways to attain the destination and hence avoiding faulty nodes and links. However, Ethernet being a broadcast system, it is essential that at any instant of time the destination can be attained only through one route. Spanning Tree protocols as described in section 3.3 allow to "carve a tree out of the mesh" and to restart every time that some node or link fails. This automatic restoration process grows in complexity and in required time with the size of the network. It is therefore necessary to use it "with moderation" and to associate different mechanisms into the network design.

Typical recovery times using RSTP (IEEE 802.1D-2004) are around 5 ms x Number of Switches.

Legacy applications through time multiplexed channels across an SDH network are restored within 50 ms using SDH ring protection mechanisms. This value can be considered as a reference objective if we consider that the great majority of critical operational applications to be switched over an Ethernet network are presently routed through an SDH network.

This implies that “automatic recovery” sub-networks can be made of up to around 10 switches (configured into a ring or mesh topology), though it is common not to exceed 7 hops for convergence reasons.

When larger numbers of switches are involved it is appropriate to use a two- or multi-layered hybrid topology in which automatic restoration is constrained to no more than 7-10 switches.

10.7 Service isolation and VLAN Mapping

An essential task of operational network design is to plan the partitioning of traffic into VLANs with different Classes of Service (CoS) and priority assignments. VLAN segregation assures an adequate level of service performance for each application, and prevents an anomaly in one application from propagating into the whole network. Moreover, using a Multiple Spanning Tree Protocol, a VLAN segregated network can limit the extent of network outage due to reconfiguration.

10.7.1 Segregating and Prioritizing Data

IEEE 802.1Q VLAN (section 3.2.3) allows for logical segregation and grouping of traffic into virtual LANs regardless of where the end stations are physically located. A virtual LAN allows the advantages of a logically separate network while sharing cabling and equipment infrastructure with other VLANs to reduce cost and resources. Each VLAN has its own broadcast domain, meaning that Ethernet frames from one VLAN will not be transmitted onto another VLAN, and two devices can share a switch and yet not share each others broadcast traffic nor send packets to one another unless a router is deployed to route between the corresponding VLANs. This is accomplished by inserting a ‘tag’ header on the Ethernet frame that identifies VLAN membership so that switches may direct traffic appropriately.

Separating the network into different VLANs has many advantages.

- ⇨ Devices with high volume traffic output such as merging units or video encoders do not flood other devices with traffic they cannot tolerate.
- ⇨ Securely controlled access to different VLANs at a central router demarcation point.
- ⇨ Access to real time VLANs like GOOSE and Process Bus restricted to involved devices.
- ⇨ Protection A+B schemes can be implemented with a single physical network without sacrificing reliability.

Priority assignment allows different levels of service for multiple traffic streams being served by a single network resource (e.g. a single link). IEEE 802.1p Priority Queuing manages limited resources such as bandwidth on a transmission link from a network router. In the event of outgoing traffic queuing due to insufficient bandwidth, all other queues can be halted to send the traffic from the highest priority queue upon arrival. This ensures that the critical traffic is forwarded with the least delay.

Although there is no standard way for traffic segregation into VLANs in the power utility, or for assigning priorities, the following are some of traffic flows in the operational environment that may be considered for separate VLANs:

- Protection A / Protection B
- Process bus (IEC 61850-9-2 sampled values)
- GOOSE Messages
- Synchrophasor communications
- Voice over IP
- SCADA/Engineering Access
- Substation LAN management (e.g. switches, routers, modems, etc.)
- Video surveillance and access control

10.7.2 Isolating Device Failures

VLANs also offer the possibility of limiting the impact of network failures. In the simplest sense this is done by limiting the broadcast domain of a device to a single VLAN. This prevents a misbehaving device, which is continuously broadcasting, from impacting all of the stations on the network and limits the scope of an outage caused by this type of event. If the problem was caused by a malicious user this would be called a denial of service, DoS, attack.

By assigning mission critical systems and services to separate VLANs the possibility of a single device disrupting the entire network can be greatly reduced. For example a misbehaving VoIP telephone would no longer be a direct threat to the SCADA traffic if they were on separate VLANs.

10.7.3 Limiting Network Outages with MSTP

The VLANs in most networks share a common spanning tree. When the spanning tree is forced to reconfigure due to a link or switch failure this will impact all of the VLANs regardless of whether or not they are all impacted directly by the failure that occurred.

The Multiple Spanning Tree Protocol, MSTP, is a protocol that can further isolate network failures by placing groups of VLANs on a separate spanning tree instances. This means that not every spanning tree reconfiguration will impact all of the VLANs. Some groups of devices will remain completely unaffected.

Managed Ethernet switches are required to implement a VLAN-enabled network; the managed switch ensures that traffic from one VLAN does not cross the boundary to another VLAN.

10.7.4 Service, VLAN and Priority mapping

The managed switch also can be configured to assign the 3-bit priority field to untagged ingress traffic (IEEE 802.1p Priority Queuing). This results in eight different Classes of Service (CoS) with seven being the highest priority and zero being the lowest. The CoS priority causes ingress frames to be placed in different queues within the switch. The higher priority queues get emptied first, therefore reducing the travel time through the switch for more important traffic. When the network is lightly loaded, CoS has little impact; however, as the traffic load increases, the probability increases for frames to be queued. When frames are queued, the latency increases for that frame to reach its final destination.

CoS serves to reduce latency, which is crucial for time and jitter sensitive traffic such as GOOSE-based real-time control.

While there are eight possible priorities, it is important to determine the actual number of priority queues being supported by a particular Ethernet switch. This number is normally between two and four. Actual priority mapping example for four queues would be as shown in the following table.

Queue	VLAN Priority
Highest	6, 7
Medium High	4, 5
Medium Low	2, 3
Lowest	0, 1

Table 10.8 - Priority Queue Mapping Example (4 Queues)

10.8 Switch Requirements for Operational Ethernet

Selecting Ethernet switches for the implementation of Power Utility operational network infrastructure is a task with important consequences as to the suitability of the network for mission-critical applications. The present section lists the most important functional features that the switch must provide, in addition to its electromagnetic and environmental properties which are discussed in chapter 11.

IEEE 802.3x Full-Duplex Operation (no collisions)

As described in section 10.1.1, supporting Full Duplex operation in all ports as per IEEE 802.3x allows the switch to ensure that no collisions occur and thereby assures a deterministic behaviour.

IEEE 802.1p Priority Queuing

As described in section 10.7.1, operational Ethernet switches must support IEEE 802.1p Priority Queuing to manage limited bandwidth resources. In this way, frames can be tagged with different priority levels in order to ensure that real-time critical traffic like GOOSE Messages can be forwarded with the least delay even during periods of high network congestion. In order to prevent high priority packets from choking off all other traffic, a bandwidth limitation is usually set to the highest priority traffic queue.

IEEE 802.1Q VLAN

As described in section 10.7.1, operational Ethernet switches must support IEEE 802.1Q VLAN to allow the segregation and grouping of different traffic flows into logically separate networks while sharing the network infrastructure. Service isolation through VLAN segregation provides a powerful security mechanism, and prevents high traffic volume devices such as merging units or video encoders from flooding other devices with traffic they cannot tolerate.

IEEE 802.1 D-2004 Rapid Spanning Tree

As described in section 3.3.1 and 10.6.4, supporting IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) allows the switch to be used for the creation of fault tolerant ring network architectures. While providing a much better performance than the STP, the IEEE 802.1w RSTP still requires up to a few seconds to restore large network connectivity when a topology change occurs. IEEE 802.1D-2004, a revised and highly optimized RSTP, reduces network recovery times to just milliseconds. Performance of a good RSTP implementation can yield worst case failover and recovery times of the order of 5 ms per switch in the network. It is therefore recommended to use Ethernet switches that support IEEE 802.1D-2004 RSTP.

IGMP Snooping / Multicast Filtering

As described in section 10.1.4, network switches which support IGMP Snooping allow the network to reduce multicast traffic from streaming and other bandwidth intensive IP applications and hence to reduce packet processing at the switch and at the end hosts who will not have to receive and filter all the multicast traffic generated in the network. In Substation Applications, IGP allows for multicast data such as GOOSE frames, to be filtered and assigned only to those IED’s which request to listen to them.

Redundancy and Dual Homing

Supporting redundancy is an important functional feature for assuring service availability and fault tolerance when selecting switches for an operational Ethernet. A commonly employed fault tolerant configuration is a “Dual Homed” structure in which devices have two connections to the LAN via different switches. This may be performed either by implementing primary/backup links using a single MAC address or by having both links active and using different IP addresses. In the former case, the selected Ethernet switch must support adequate failover and recovery mechanisms.

Security

As discussed in section 10.5, cyber-security is a global issue requiring a coherent security policy and overall system coordination. It cannot be reduced to the specification of the operational network switch. However, in order to enable the implementation of a secure network infrastructure, the employed switches and their management facilities must support security features in addition to VLAN segregation. Substation gateway switches connecting to the wide area network must provide firewall and encrypted VPN functions.

Switches must have management security via SSL/SSH (Secure Sockets Layer/Secure Shell). Port security and 802.1x can be deployed to deny physical access to the network; for example, one can connect only recognized laptops to the LAN. Rate limiting can be used to prevent rogue or broken devices from poisoning the network.

Operations, Administration and Management

As described in section 10.4, an operational Ethernet switch network must comprise management and monitoring facilities to achieve and maintain adequate performance. Remote monitoring of Ethernet switch generated alarms through SNMP (Simple Network Management Protocol) is the minimum level of acceptable management. More detailed diagnostic information such as link status and traffic flow and hence a network rather than device view, as well as remote configuration and parameter setting, greatly increase the visibility of the network maintenance staff and therefore the overall performance of the system.

10.9 Internetworking

10.9.1 Layering architecture

Internetworking is the way of providing a ubiquitous and seamless service by means of a network formed by two or more subnetworks of different technologies. Thanks to the use of different technologies in different parts of the network, more efficient network designs can be achieved.

Internetworking is a concept introduced at the late 90's. Reference [24] introduces the details of this approach as well as the different models and their typical applications.

Internetworking is a rather new concept in the communication network field. It represents an evolution of the classical approach of building networks using a single technology to this new concept where different technologies are combined to obtain reliable, cost-effective and scalable network designs.

An Overlay architecture presents the advantage of sharing the basic communication infrastructure and transport layer by all the users of different services and layers. The equipment required to deploy the network is more specialized in the function it has to provide in the layer that is allocated but a larger number of equipment is normally required.

With the advent of new broadband technologies such as optical networking, and 1 and 10 Gbit/s Ethernet switches with built-in routing functionalities the trend nowadays is to simplify the network trying to reduce the number of layers and the number of different equipment required to provide broadband integrated services.

The drawbacks identified in a complex internetworking architecture are:

- The interactions between devices of different layers can introduce rising management and implementation costs as the network grows due to the fact that one device of one layer can interact with several layers.
- Mismatch of Life-cycle. Since the technology life-cycle of every layer may be different, the obsolescence of one layer may drive to larger refurbishment costs than expected.

Consequently, the network architecture is evolving towards a three layered network, Ethernet over SDH over an optical layer. The future trend seems to be the deployment of networks with two layers, the optical layer with transmission and transport capabilities and the Ethernet layer which provides transport services and application services both based on legacy frames or/and in Ethernet frames.

10.9.2 Implementation of distributed LAN

The frontier between the transmission and the networking layer has largely moved due to new possibilities incorporated into the SDH system as described in chapter 5 (GFP, Ethernet bridging and switching), simplifying the interface adaptation layer. A fully distributed LAN can at present be implemented using the SDH nodes of the network and through VLAN and broadcast domain emulation features.

In present SDH networks, it is possible to find point-to-point, point-to-multipoint and multipoint-to-multipoint Ethernet links where different LAN environments and configurations can be created.

Another feature of actual SDH networks is that the routing capabilities are being integrated into SDH nodes. In this way, the SDH equipment can provide Layer 1, 2 and 3 services integrated into the transmission nodes.

Distributed LAN architecture can also be implemented through other technologies such as MPLS as already discussed in section 8.2 with the same practical design considerations as here above.

10.10 Physical packaging of network functions

The compact design and integration trend in the IT and communication equipment leads to physical building blocks which often go beyond the functional roles defined originally in the networking world. In this way, each original block is integrating some or all of the functions of the overlaying or underlying block leading to multiple ways to design and implement the same systems but not necessarily at the same cost and performance:

In general using integrated capabilities beyond the functional role of a building block increases the risks of interchangeability but allows easier common management and reduces the number of building blocks.

- Ethernet Switch/ IPRouter – Many manufacturers include both functions in a single box.
- Layer 3 (or 4-7) Switch – An Ethernet switch that is able to use higher layer information (e.g. IP header, etc.) in order to perform its forwarding function.
- SDH Multiplexer/Ethernet Switch – SDH Add-Drop Multiplexer have Ethernet point-to-point bridging and switching capabilities. This switch function is generally used for constituting the Ethernet over SDH infrastructure and providing separate substation gateways towards the substation LANs without substituting them.
- Primary Multiplexer / sub-E1 Ethernet Switch – The primary Multiplexer can provide Ethernet bridging and switching with limited capacity and sub-E1 mapping to be groomed and aggregated further across the network, e.g. SCADA RTU traffic. This solution introduces additional time latency due to encapsulation.
- Ethernet Switch/WDM – Many Ethernet switches provide SFPs allowing the capability of CWDM and DWDM. The use of an integrated WDM is not the most suitable solution for building a wide-scale WDM network but rather to overcome some particular obstacles (e.g. bottlenecks).
- Ethernet Switch integrating legacy interfaces – The choice between primary multiplexing for legacy interfaces and using a switch/router with legacy interfaces is again a question of scale. Designing with these devices is a difficult trade-off between delay and jitter due to buffer dimensioning issues.

- ⇨ Substation IED / Ethernet Switch – Most IEDs integrate switching functions to some extent. This indeed does not replace the need for LAN switches in the substation but rather for interconnecting few IEDs.
- ⇨ Router/ Switch with SDH interface – These interfaces are no longer commonly used because of simpler and cheaper Gigabit interfaces connecting to the backbone.

10.11 Transport technology design

The practical design of the Ethernet infrastructure includes also careful selection of physical media and access technologies, suitable wiring, connectors and environmental aspects. These issues are treated in other sections of the document. As a general guideline, the following table is given here.

Domain of Use		**Span**	**Transmission Technology**	**Remarks**
Equipment Room	Cabinet level (Backplane)	Few meters	Copper	
	Local interconnection Interface to application		Copper or Fibre interface	
	Temporary & nomadic access		WLAN (WiFi)	Security issues
Substation Control Building	Automation LAN Videosurveillance & Access security LAN	10 – 100 m	Fibre interface	
	Voice & data LAN		Fibre, Wireless (WiFi)	
Multiple Substations and Buildings on one site		100 - 1000 m	Fibre Ethernet Ethernet over PDH/SDH Wireless Ethernet DSL Access	
Small geographical region	Urban interconnections Windfarms, Hydroplants	1 - 20km	Fibre GEth Ring, RPR WiMAX	Frequency availability
Remote access to Electrical sites	S/S on fibre network	1 – x km	Ethernet over SDH Native Ethernet over Fibre	
	S/S not on fibre network		DPLC RF & Wireless	HV site MV site
Remote access to device on customer premises	Advanced Metering	1 – 10 km	DSL Access BPLC GPRS Wireless Broadband EPON Narrowband Distrib. PLC	Existing copper Value Added services Low bandwidth, Single service Value Added services Simple Metering service
Remote access to facilities at Operation Support sites	Site on fibre network	5 -50 km	Ethernet over SDH	
	Site not on fibre network		WiMAX Microwave Ethernet VSAT Metro Ethernet Service	
Substation to substation		National or Regional	Ethernet over SDH Native Ethernet over fibre Microwave Ethernet	

Ethernet interconnection backbone across the network	Limited bandwidth req'd Larger bandwidth req'd		Ethernet over SDH Dedicated wavelength (WDM)	

10.12 Migration & Legacy Integration

10.12.1 Migration with legacy systems

In developing the migration strategy for changing the communications architecture in a substation, there is a need to examine the different approaches possible and to match the best process for retrofitting in the presence of legacy systems and to ensure that the correct constraints are taken into account. At a general level, the key phases involved in such a project are:

- Checking existing assets at bay and substation levels, i.e. collating the drawings, identifying the interfaces and functions involved in the changeover, power supply requirements, as well as any associated issues, such as obsolescence of existing equipment/systems etc.
- Evaluating retrofit constraints such as the maximum and minimum outage duration possible, identifying whether any key functions are going to be degraded and the risks associated with this, the testing principles to be employed, etc.
- Definition of preferred strategy, e.g. total or partial replacement, step-by-step, etc.
- Cost/Benefit evaluation and prioritization (lifetime cost, performance indicators, return on investment).
- Detailed design may be necessary for the handling of Protection and Control changeover, depending on the requirements and the scale of the project.
- Optimal maintenance procedures should be identified and possibly designed into the project, such as reliability centred maintenance, work orders management, etc.

Costs associated with retrofit programs include

- Specific integration costs
- Continuity of distributed automation, where applicable.
- Space requirements/ availability
- Power supply capacity

Migrating from existing technology to Ethernet, while protecting existing investment, requires careful planning and management. The investment in legacy devices will be considerable and they will not be replaced overnight. The investment made will be marked down over a number of years precluding their immediate replacement with more modern devices and systems. Moving to a system interconnected with Ethernet technology is not just about building a network. It is planning the replacement of equipment and plant and integrating existing technologies with new Ethernet devices as they are installed.

Installing an Ethernet network into existing substations and power stations will therefore be much more complex than for a "Greenfield" site. Some existing equipment will have an informative interface usually a serial port. These devices will generally have data formats specific to the equipment model being accessed. Even equipment from the same manufacturer often do not have a common data structure.

Where a substation is to be upgraded to Ethernet a useful strategy is to upgrade when a bay is refurbished. In this way, risk to the substation can be minimized and the work is contained in manageable packages. Commissioning will also be more straightforward, enabling the operation of the network components (e.g. new IEDs, etc.) to be proven before the bay is put back in service.

The main problem connecting legacy devices to a LAN is that their information is in a variety of formats and most equipment is only equipped with a serial port.

The simplest solution for a small number of devices to be accessed is to use a stand alone device server. This provide serial to Ethernet conversion for individual devices. A Telnet session can be established between the remote user and the device to be accessed.

Where there are a number of serial devices to be interfaced, it may be more appropriate to use devices with multiple ports. This can be a serial multi-port device; one such device employs a fibre optic ring with optical to serial port remotes. This is ideal for the substation environment. A single device server can be used to provide a connection from the multi-port device to the LAN. Alternatively multi-port device servers are available with multiple serial ports to one Ethernet port.

10.12.2 Integration of Legacy devices

Although IEC-61850 architecture is more than a protocol but a complete object modelling, this paragraph will focus on communication interface adaptation aspects.

The communication infrastructure of an IEC-61850 substation will be formed by a number of different devices connected to a LAN, which acts as the core of the communication system. When legacy devices have to be integrated in such new architecture, the use of transmission media adapters, communication interface adapters, communication controllers, protocol adapters will be required. This may form non-uniform and quite complex communication architecture. The evaluation of its performance and its services guarantees may become a quite complex task. Availability of every device included in the communication infrastructure and the latency introduced both, by the devices and by the proprietary or legacy interfaces and protocols, has to be considered in the calculation of the communication system performance.

10.12.3 Integration of existing SCADA RTUs

To protect earlier investments in serial RTUs, the following scenarios are possible to go towards an IP-based SCADA-system:

- Use decentralized Front-end processors (FE) which collect and consolidate serial traffic from legacy RTUs. (refer to figure 10.9, case A). The Front-end is connected to the Control Centre using IEC60870-5-104 (TCP/IP) across the communication network.
- Use Terminal-Servers (TS) that can tunnel a varying number of serial lines coming from legacy RTUs via IP to the Control Centre. In this case, the RTUs' communication protocol is not converted for transport, but messages are encapsulated into Ethernet frames and extracted at the Control Centre via virtual COM-ports (refer to figure 10.9, case B). When using this approach, special attention has to be given to the timing issues to avoid time-outs due to the delay introduced by the encapsulation.

⇨ Keep the existing installations and connect the new IEC 104 RTUs directly via IP (refer to figure 10.9, case C).

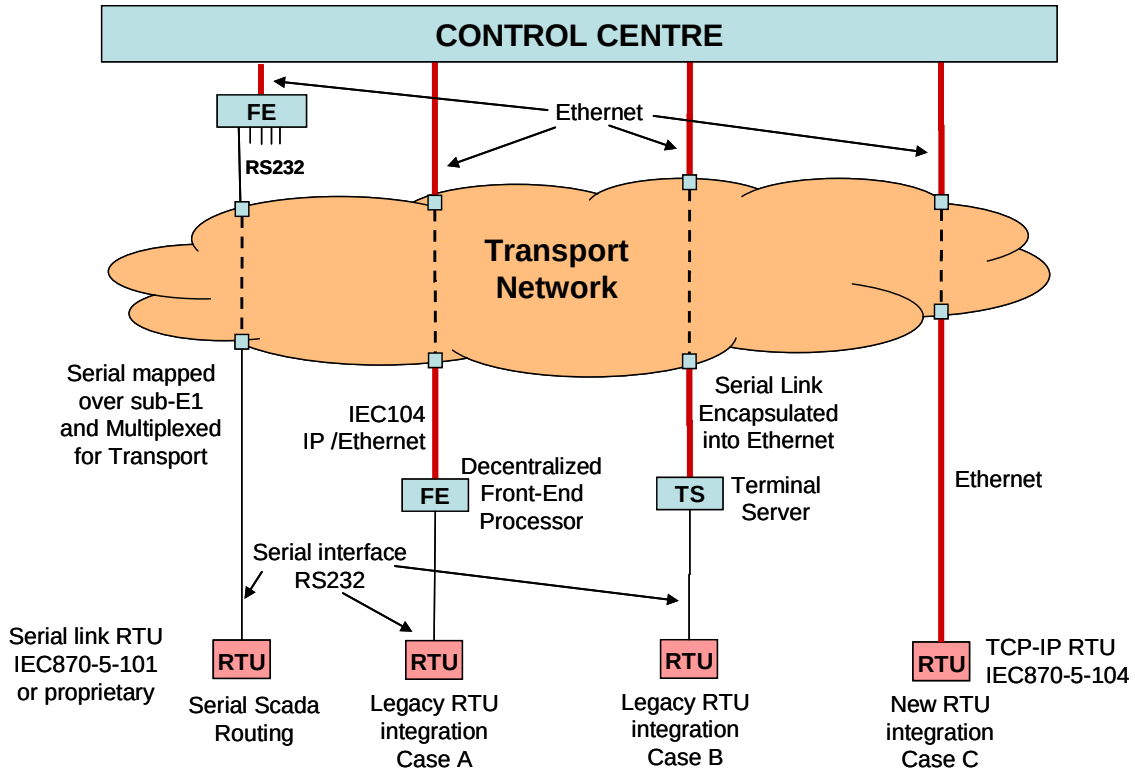


Fig 10.9 - Integration and migration scenarios for RTUs

11 ENVIRONMENTAL & MECHANICAL ISSUES

11.1 Fibre types

Optical cables used for connecting Ethernet nodes and devices employ the following types of fibre:

- Graded Index Multi Mode (GI MM) fibre (62.5/125 μm or 50/125 μm) - These fibres are mainly used inside buildings for office LAN/WAN applications.
- Single Mode (SM) fibre with a core diameter of 8-10μm (known as 9/125μm or 8/125μm) is the traditional fibre used for long distance high speed communication.

11.1.1 Multimode fibre (MM)

Most fibre installations inside buildings are multimode fibres. Older installations up to 1990 are mostly 50/125μm fibres. Although some installations dating from 1990-2000 use 62.5/125 μm fibres, the new multimode installations since then have generally employed 50/125 μm fibre providing better performance (Single Mode fibre in building installations is not common).

Multimode fibre is popular because of LED/PIN transceiver technology and connectors, which are cheaper and less precision-sensitive than corresponding components for a Single-Mode fibre system.

The LED/PIN transceiver is available for Ethernet up to 100 Mbps. When using Gbit Ethernet and above, more advanced light sources (Laser) and receivers (APD) must be used, and multimode fibre has no advantage only limitations in link distance.

It can be a problem to upgrade the Ethernet speed by using 62.5/125 μm and 50/125 μm fibres, since these fibre types have limited bandwidth. Depending on the quality, the age, and the type of the fibre, the performance can vary. Some “typical” values are presented in table 11.1.

Most manufacturers, ISO/IEC 11801 and IEEE specify the maximum fibre lengths for an Ethernet link. Considerably longer distances may be possible due to important bandwidth variations among multimode fibres, but this requires to be tested by the user every time.

All limitations must be taken into consideration when upgrading an existing installed network using multimode fibre to a higher speed.

When installing a new fibre inside an office or a building, for higher transmission rate >100 Mbps, installation of SM fibre or a mix SM-MM fibre should be considered.

Also connection of the two types of MM fibre will cause problems such as higher attenuation when connected and lower bandwidth as result.

ISO/IEC 11801 Fibre Type	Wavelength (nm)	Bandwidth IEC (typical) (MHz/km)	Data Rate	Maximum distance (m)
OM-1 (OM-1+) 62,5/125 µm	850 nm	200 (200)	1000 BASE-SX	275 (500)
	1300 nm	500 (600)	1000 BASE-LX	550 (1000)
	850 nm	200 (200)	10 GBASE-SR	33 (65)
	1300 nm	500 (600)	10 GBASE-LX4	300 (450)
OM-2 (OM-2+) 50/125 µm	850 nm	500 (600)	1000 BASE-SX	550 (750)
	1300 nm	500 (1200)	1000 BASE-LX	550 (2000)
	850 nm	500 (600)	10 GBASE-SR	82 (110)
	1300 nm	500 (1200)	10 GBASE-LX4	300 (900)
OM-3 50/125 µm	850 nm	1500 (2000)	1000 BASE-SX	860 (1100)
	1300 nm	500 (500)	1000 BASE-LX	550 (550)
	850 nm	1500 (2000)	10 GBASE-SR	270 (300)
	1300 nm	500 (500)	10 GBASE-LX4	300 (300)
(OM-3+) 50/125 µm	850 nm	(4700)	1000 BASE-SX	(1100)
	1300 nm	(500)	1000 BASE-LX	(550)
	850 nm	(4700)	10 GBASE-SR	(550)
	1300 nm	(500)	10 GBASE-LX4	(300)

Table 11.1 – Multi-mode Optical Fibre Standardized Performances (Corning values in parentheses)

Some suppliers offer enhanced specifications for OM-1, OM-2 and OM-3 multimode fibres. These higher performance versions are referred as “OM-1+”, “OM-2+” and “OM-3+”, respectively, but they are not standardized as per IEC/IEC 11801. As an example, table 11.1 shows the fibre bandwidth for standardized ISO/IEC and Corning OM+ fibres for some typical applications.

11.1.2 Single Mode fibre (SM)

Single mode fibre 9/125 µm is the traditional fibre for telecommunications for long distance high speed systems. The typical distances between repeaters are up to 50 km (1310 nm) and 100 km (1550 nm).

Single mode fibre has been widely installed all over the world since the mid 1980’s. There are some different types of fibres with performance difference.

Standard fibre type ITU-T G.652 is the mostly used one. This fibre has zero dispersion at wavelength 1324 nm. This fibre can be specified in 4 categories: A, B, C, and D, with different performance in attenuation and PMD.

For long distance signal with high speed, CWDM or DWDM fibre systems fibre type C or D should be used.

Older SM fibre normally has limited performance for high-speed system. Dispersion and PMD must be measured to verify values.

Sometimes fibre type ITU-T G.653 is installed. This fibre is today obsolete. It is optimized for 1550 nm and has zero dispersion around 1550 nm. This type of fibre cannot be used for DWDM systems but for single fibre systems it is still a good choice.

There is also a newer fibre type specified by ITU-T G.655 and G.656 which are optimized for DWDM and CWDM systems.

11.1.3 Optical connectors

Many different optical connector technologies are available on the market including some which are no longer employed into new deployments and some which are specific to a country or to an application. In this document, only those types which are commonly used in many countries are described.

Most connectors employ a mating adapter which may be for MM fibres, for SM fibres, or for both.

Similarly, different polishing methods are employed in connectors: flat polishing, convex polishing (SPC and UPC), and angle polished connectors.

- Flat and convex polishing are used for MM fibres. Convex and angle polishing are used for SM fibres. Flat and convex polished connectors can be mixed but not angle polished (APC).
- Convex and angle polished connectors have low back reflection UPC better than 50 dB and angle polished better than 55 dB.
- Flat polishing gives back reflection not better than 15-20 dB. High back reflection may cause problems for high speed laser transmitters (interference).
- For convex polishing, low back reflection requires that two connectors are connected.
- Angle polished connectors have low back reflection even if they are not connected.
- Angle polished connectors are popular in cable television networks when using an optical star. Angle polished connectors and mating adapters normally have a clear green colour.
- Convex polishing gives lower attenuation than flat polishing.
- Angle polishing gives higher attenuation than convex polishing.

Commonly used connectors are SC, ST, and LC. Also type FC and SMA are common in older installations.

SC- type Connector

Optical connector type SC is the most commonly used connector in all types of installations with SM and MM fibres. Originally it was invented by NTT in Japan. SC connector is of "snap in type". They are available as single or as duplex. In a 19" ODF (Optical Distribution Field) up to 48 (24 pair) can be installed. SC has a 2.5 mm diameter ferrule in zirconium with plastic housing.
Attenuation are typical 0.2 dB (SM fibre) and 0.3 dB (MM fibre).

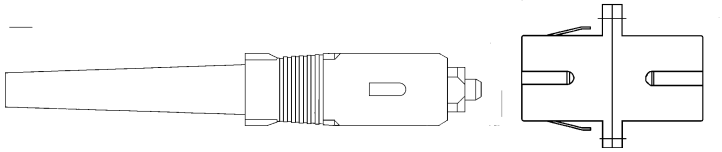


Figure 11.2 - Optical connector and mating adapter type SC

LC-type Connector

LC is a newer connector than SC. It has similar optical performance and is available as single or duplex. LC has1,25 mm diameter ferrule in zirconium with plastic housing. The only advantage is the small size which makes it possible for higher packing of connectors in the ODF.
LC connectors are used for SM and MM installations.

Optical connector type ST

ST is a type of connector which is commonly used on equipment for WAN/LAN equipments. Originally it was invented in USA by ATT and is used for SM ad MM fibres.

ST uses a bayonet and only a maximum of 12 connectors can be packed in a 19" ODF. It is not very popular in network installations.

When using similar 2.5 mm diameter ferrule, ST has the similar performance as type SC.

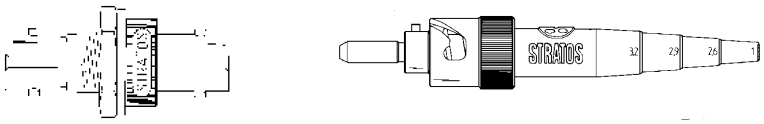


Figure 11.3 - Optical connector and mating adapter type ST

FC-type Connector

Optical connector type FC is one of the first connectors with high performance. Originally it was invented by NTT in Japan and is used in telecommunications installations all over the world. This connector has screw-thread, and maximum 12 connectors can be installed in one 19" ODF. FC is still very common in older installations and at test equipment.

Using similar 2.5 mm diameter ferrule, FC has the similar performance as type SC.

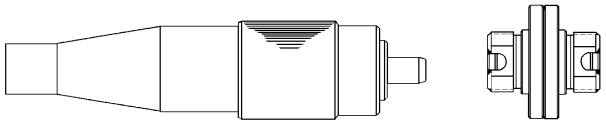


Figure 11.4 - Optical connector and mating adapter type ST

SMA-type Connector

SMA or SMA 905 is an optical connector used commonly in MM installations up to mid 1990's. Today it is obsolete. The attenuation is quite high with a typical value of 0,7 dB. Older installations with these connectors can be used, but SMA connectors' bad performance must be taken into consideration. This connector has screw-thread and maximum 12 connectors can be installed in one 19" ODF.

Ferrule has a diameter of 3.17 mm. The newer one is made of zirconium, but full metal is also common.

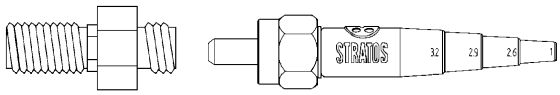


Figure 11.5 - Optical connector and mating adapter type SMA

11.2 Copper cables

Three main cabling standards are in use:

- EIA/TIA 568A - The American standard, first to be published (1991).
- ISO/IEC 11801 - The International standard for structured cabling systems.
- CENELEC EN 50173 - The European cabling standard

The following table defines different cable categories (as defined in EIA/TIA 568A/B).

Type	Connector	Frequency Range	Guidance
Cat 3	8P8C (RJ45)	0…16MHz	Historically popular for 10 Mbit/s Ethernet networks. This type is not recommended (TIA/EIA-568-B)
Cat 5	8P8C (RJ45)	0…100MHz	Category 5 cable can be used for 10/100 Mbit/s Ethernet
Cat 5e	8P8C (RJ45)	0…100MHz	Category 5e cable is an enhanced version of Cat 5 to improve the performance with 1 Gbit/s Ethernet (TIA/EIA-568-B)
Cat 6	8P8C (RJ45)	0…250MHz	Category 6 can be used with 10 Gbit/s Ethernet over shorter distances (10 meter). (TIA/EIA-568-B)
Cat 6a	8P8C (RJ45)	0… 500MHz	Cat. 6a allows up to 10Gbit/s Ethernet with a cable length up to 100 meter. (ANSI/TIA/EIA-568-B.2-10)
Cat 7		0…600MHz	Cat 7 is a future cabling standard that should allow up to 100Gbit/s Ethernet over 100 meters cable length.

Table 11.6 – Copper Cable Categories

11.3 Electromagnetic Compatibility (EMC)

Electrical substations are severe electromagnetic environments, and various types of disturbances can be easily encountered, as opposed to light industrial environments. All electronic equipment installed in the HV electrical substation must be able to resist to electromagnetic phenomena produced in this environment. When selecting Ethernet networking equipment for use in electrical substations, the communications designer must be aware of the special requirements imposed by the application.
To overcome this situation, the networking equipment shall be protected against the following hazards:

- Conducted and radiated noise – These disturbances are solved by means of shielding and filtering, and are detailed separately in the following section.
- Overvoltages – Usually substation power supplies are derived from battery arrays, which may experience overvoltages when charging. Also if the supply is directly obtained from the grid, fluctuations may occur, mainly during disconnections and reconnections in the substation bars. This may easily lead to equipment breakout. To prevent this substation-grade Ethernet devices shall withstand a higher than usual supply voltage range.
- Reverse polarity – Every device shall withstand an accidental reversal of the power supply terminals during installation.
- Electrostatic discharge – The networking equipment shall be able to work under the presence of electrostatic discharges in exposed metallic parts and interfaces. The devices must not only avoid any damage, but also malfunctioning during the discharges. They occur when electrostatic voltage builds up in humans due to poor electric contact to ground (inadequate shoes) with certain air conditions (lack of air moisture…), and as a result there is big voltage difference between the operator's exposed body parts and the networking devices, which are usually grounded.
- Surge protection – Ground faults, switchgear operation, breaker activations… are substation events which originate very intense current flows and discharges. The currents are coupled into any metallic conductor. As a result of this, huge voltages appear in the power supply terminals of every network device or IED. Thus the equipment must include the mechanisms to cope with these surges. Common design practices include voltage spark gaps, X/Y-type safety capacitors, gas discharge tubes, varistors, zener diodes…
- Failure mode – Last, but not least, the networking equipment shall be designed to guarantee a benign failure mode. This will guarantee that the failure of a switch's power supply, for instance, will not affect any of the devices powered by the same power rails, or even the primary power supply. In this way the networking device effectively protects the rest of the equipment from its own failure.
- It is important to note that every Ethernet link shall be based on fibre optic technology, in order to get rid of all these potentially harmful phenomena since optical communications are immune to electromagnetic noise and can travel longer distances without performance degradation.

IEC 61000-4-x defines the criteria, tests and severity classes, the most important are as follows:

61000-4-2	Electrostatic discharge , class 3
61000-4-3	Radiated radio-frequency Electromagnetic field from 80 MHz to 3000 MHz, class 4
61000-4-4	Fast transient/burst , class 4
61000-4-5	Surge 1,2/50 µs line to ground and line to line, class 3
61000-4-6	Conducted disturbance induced by radio frequency fields
61000-4-11	Voltage dips and Voltage interruptions
61000-4-12	Damped oscillatory wave, Common Mode and Differential Mode, class 3

It should be noted that depending upon the nature of the test, the equipment must either continue to function correctly under the test conditions, or resume normal operation after the condition has disappeared without the requirement for a Reset.

IEC61850 in its part 3, “General Requirements” specifies the climatic and electromagnetic environment necessary for Ethernet hardware to be used in the substation.

Functions and Device Models” specifies the requirements for data integrity in Ethernet communications in substations.

11.3.1 RF interference

Every cable or device or capable of conducting electricity is a potential victim to pick up radio frequency interference from the surrounding environment. This problem is of great importance in those environments where the electromagnetic noise is considerable due to large current flows or voltage differences, such as electrical substations.

Some frequencies are particularly harmful for twisted pair-based Ethernet communications, such as 12.5MHz, 125MHz and 1.25GHz, which are the signalling rates for Ethernet running at 10, 100 and 1000Mbps.

Vulnerability to RF Interference depends also in the way the cabling is done through the substation, types of ducts used, type of cable deployed, proximity to noise sources (coils, motors, circuit breakers, switchgears).

Field- to-cable coupling is not the only RF interference mechanism that may be present. Crosstalk between conductors running in parallel for some distance is a common problem with unshielded cables.

As fibre cables are not electrical conductors, they are inherently immune to electromagnetic interferences, and suit the application of Ethernet in power plants and substations.

11.3.2 Shielding and Grounding

Shielding is an effective way of reducing the electrical noise and transients coupled into electric cables. It can be very efficient for cancelling the effect of electric fields and high frequency magnetic fields (> 100KHz). However it brings little benefit against low frequency magnetic fields.
There are two main points of interest regarding shielding practices:

Shielding of cables and connectors

Electrical cables and connectors are often shielded to protect them from incoming radio frequency interferences. Electrical cables running on long distances in electromagnetically noisy environments are particularly sensitive to these hazards, as they can act as receiving antennas for the incoming radiation.

On the other hand, shielded cables end in shielded connectors. In a typical installation in a communications equipment, shielded connectors are electrically connected to the casing, which in turn is chassis ground. A user may inadvertently create a ground loop by connecting both ends of the cable to chassis ground, separated by tens or hundreds of meters. In fact as electrical cables are the main mechanism for coupling noise into electronic equipment.

In Ethernet networks three type of shielded cables are used for 10/100BaseTx or gigabit applications:

Shielded Twisted Pair, STP - In this cable every copper pair is individually shielded.

Screened Foiled Twisted Pair, S/FTP - In this cable all the four twisted pairs are foiled with a metal sheet.

Screened Shielded Twisted Pair, S/STP- In this cable type every copper pair is individually shielded, and then the aggregated four pairs are covered by a metal sheet. This type of cable provides the best protection against external interference coupling and crosstalk between pairs.

As a result of all these facts, the use of optical fiber cabling in Ethernet networks for electrical substations is strongly recommended. The use of copper shielded twisted pair cables should be restricted to intra-cabinet connections.

Shielding of equipment

Electronic equipment is usually installed in metallic cabinets, which are grounded. In order to provide extra protection against radio frequency interference, metal housings are widely employed.

The metal housing can effectively mitigate the electromagnetic field that surrounds the equipment. The electric currents in the metal frame decay exponentially with the width of the material. The skin depth is a magnitude that identifies the width of metallic material needed to attenuate the electromagnetic wave to a certain degree (1/e). The skin depth decreases when the frequency increases. So if the material is wide enough, no electromagnetic field will reach the interior of the equipment. For instance, iron has a skin depth of 0.1mm at 10KHz, whereas Aluminium’s is close to 1mm.

Every slot in the case may act as a receiving or transmitting antenna, since surface currents may flow in the conductor around the slots creating a radiating field. This issue is prevented with conductive gaskets that provide effective electrical contact between the different parts of the housing.

11.4 Power over Ethernet (PoE)

One important aspect that favours the use of copper wire connections in Ethernet environment is the possibility to provide remote power supply through the LAN cabling to some network devices. This in particular applies to smaller devices requiring relatively small amount of power:

- Monitoring and surveillance video cameras,
- IP telephone devices,
- Wireless LAN access points
- Site Access Control ID card readers
- Ethernet Microwave transceiver, etc.

Many industrial Ethernet switches provide PoE capability on their copper wire interface ports and hence reduce the necessary site cabling and increase the flexibility of the installations (e.g. Wireless LAN base stations can be repositioned without modifying power cabling).

Furthermore, the use of PoE enables the remote management of power delivery to the concerned devices using the previously described SNMP switch management facilities.

The currently available standard, IEEE 802.3af allows the delivery 48Vdc supply up to around 13W per port using a Cat5 or Cat 5e copper cable. New work at IEEE is in progress for an enhanced standard for delivering up to 30W of supply power (IEEE 802.3at).

Two options are available for the operation mode of the Power Over Ethernet.

- Power can be injected by the Power Sourcing Equipment (Ethernet Switch) into spare copper wire pairs in the Ethernet cable and recovered into a DC/DC converter at the Powered Device.
- Power can be injected by the Power Sourcing Equipment across the centre taps of the two isolation transformers (associated to Transmit and Receive directions) and recovered across the corresponding transformer centre taps at the Powered Device DC/DC converter.

A “discovery process” at the Ethernet Switch allows to examine the Ethernet cable and to sense PoE devices with a smaller voltage (2.7-10 volts) and limited current before applying the full 48Vdc remote power.

12 CASE STUDY – REN Portugal

12.1 Introduction

REN, the Portuguese Transmission System Operator (TSO) responsible for the electricity and gas transmission in Portugal, owns a private telecommunications network responsible for data and voice services. The evolution of telecommunication technology, the demands of internal clients and the business continuity requirements forced the evolution of this private network in terms of bandwidth and introduction of unified data telecommunication technology. For this propose Ethernet/IP technology was chosen.

In the first phase of implementation REN data network, also designated as Security Services Network (SSN), was implemented in 27 electrical substations in the 2 main control sites and Disaster Recovery Site (DRS). The second phase will include the expansion to 28 new substations.

This IP / Ethernet convergent network provides integrated voice data and video services for the diverse substations where is implemented. The services provided are:

- Device settings and monitoring of power system control equipment;
- SCADA/EMS;
- IP telephony;
- Management of telecommunication systems;
- Video and security surveillance in an experimental basis;
- Corporate services.

Initially it was predicted to implement one pure layer 2 Ethernet network since the initial objective was to implement several VPN Layer 2 (VPLS) for different types of services and in a selected number of sites. Afterwards other needs were detected namely the requirement for IP sub-networks geographical division, the ability to implement strong mechanisms of traffic engineering and QoS and network scalability in order to integrate future expansions of the IP/Ethernet network for all RENs sites (electrical and gas). The option was to implement a mix of layer 3 (core MPLS network) and layer 2 network as explained in the following sections.

12.2 Network topology, technology and design issues

The principal structure of the Ethernet/IP network is based in 7 core nodes with routing and switching equipment and to which 20 access sites are connected (secondary sites - around 25% of high voltage utility substations), with switching equipment.

The core network has two main nodes (A and B), located in main control sites, they are directly connected to each other, all others nodes are connected to each of these, as shown in Figure 1. The connections between the main nodes are established in Gigabit Ethernet optical links provided by internal transmission platforms, DWDM links. Each pair of main nodes shares responsibility for secondary sites in an area, in order the guarantee redundancy for the service.

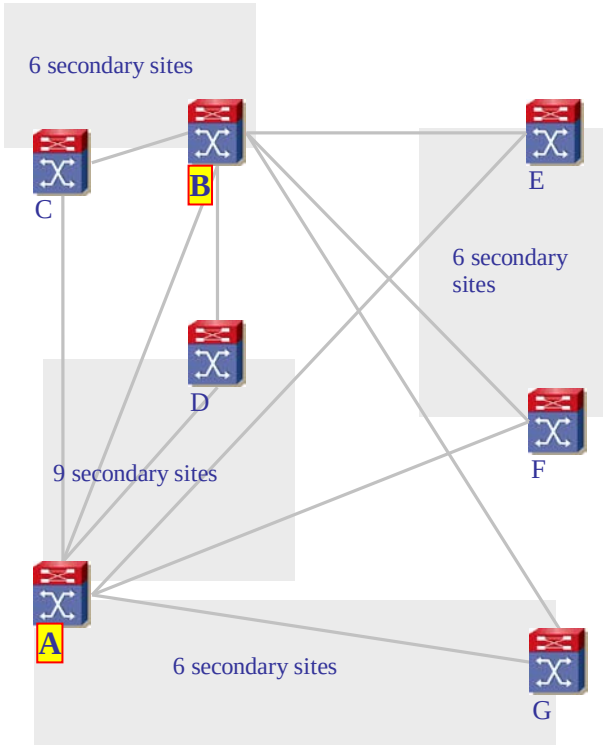


Figure 1 – Core Network

In concept the MPLS network is composed of routers for different functions as per Figure 2:

- Provider (P) – Equipments with high availability and performance having the responsibility of forwarding IP packet as fast as possible using MPLS label (LSP – Label Switch Path). These equipments are in the interior of core router and do not have clients connected directly.
- Provider Edge (PE) – Point of interconnection between core and client network. At this level the traffic is mapped/de-mapped into the VPNs MPLS and where are applied the traffic policing and classification.
- Client Edge (CE) – Client router serving only one client.

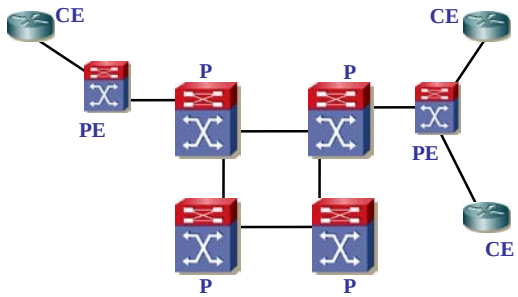


Figure 2 – MPLS Network

In the first phase of the project the provider and provider edge router function were merged in the core routers since the initial network dimension didn't oblige one clear separation of layers. In future with network growth and traffic increase the PE/CE layer could be separated and each function be assumed by different equipments. Finally, the client edge layer is implemented by switching equipment connected to PE/P sites.

In the second phase it is expected to be implemented all three levels of routing: P, PE and CE. In the sites the connectivity will be provided through switching equipment spread into the substations buildings.

In more detail, the MPLS network is implemented using the following protocols:

- ⇨ For IGP (Interior Gateway Protocol), core routing protocol, OSPF (Open Shortest Path First) is used;
- ⇨ MPLS labels distribution, LDP (Label Distribution Protocol) is used;
- ⇨ Between the several PEs MP-BGP (Multi-Protocol Border Gateway Protocol) is used to distribute and announce client routes. This permits the implementation of several VPN – MPLS.

12.3 Network architecture

The actual network is composed by core and access layer, the core is based in the 7 core routers connected to each other (Figure 1) using dedicated DWDM Gigabit Ethernet optical links, each access site is connected to 2 different core routers, for redundancy and reliability reasons, the connections between them are assured trough 100Mbps dedicated SDH Ethernet links.

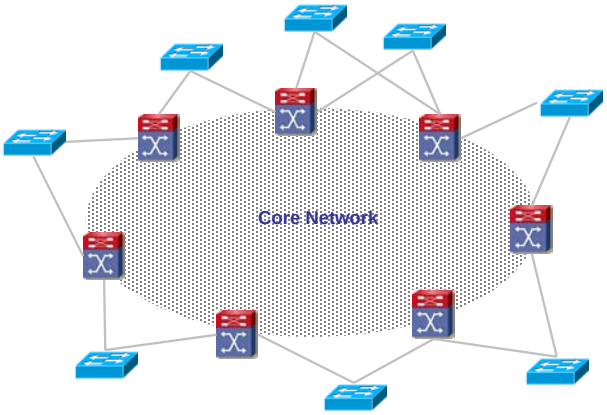


Figure 3 – Access Network

In the first phase, 20 access sites were considered and with phase two the Ethernet/IP network will be present in 28 new sites. Including the core sites this network will be present in 55 point of presence.

The main characteristics of this network are:

- Layer 3 VPN MPLS services in the core to provide different types of service;

- Layer 2 VLAN in the access layer. This layer is dedicated to internal services, typically Substation / Substation and Substation / Control Centre communication;
- The different services are supported by dedicated VPN MPLS in the core and by VLAN in the access level to provide the required traffic isolation, quality of service schemes and prioritization;
- The network equipments followed several requirements:
    - The core equipment is completely redundant in terms of power, fan system, hardware modules and software controller cards;
    - The access layer equipment is adapted to harsh substation environment by using special switches in strategic points;
    - Optical interfaces were widely used in substations to interconnect the equipments to avoid electromagnetic problems.
    - Ethernet Electrical interfaces were used only inside each room where the active switching equipment is installed. CAT6 SFTP (Shielded Foiled Twisted Pair) cabling. However the uplink, from the switch to the aggregation layer is in optical fibre.
- The GbE and Ethernet links are supported by REN DWDM/SDH private security telecommunications network. Several requirements were taken into consideration in the plan in order to assure redundancy of communications (e.g. path redundancy, no routing overlapping, equipment independencies, etc);
- Centralized Firewall to control SSN traffic;
- Creation of DMZ (Demilitarized Zone) for LAN security;
- Centralized management systems.

12.4 Management and central services of Ethernet network

The management of entire network is centralized in REN NOC (Network Operation Centre) principal data centre. In the second phase of evolution, predicted for this year, it will be implemented mirror configurations in one DRS site.

To control this network there is one centralized management system for switching and routing network equipment, call manager for VoIP management, video over IP management system, firewall management system, IDS (Intrusion Detection System) /IPS (Intrusion Prevention System) management systems, ACS management system and bandwidth control supervision system.

The management and monitoring functions and services are:

- RADIUS (Remote Authentication Dial in User Service) /ACS (Authentication Control Server) – Authentication service used to identify users allowed for internal network administration (direct access to core and access network equipment). This service is necessary also for 802.1x implementation for substation user validation and for corporate network login (client VPN access).

- DHCP (Dynamic Host Configuration Protocol) – provide IP addresses to network clients that use DHCP. In SSN this service is used by IP telephony and PC equipment connected to the corporate network in the substations.
- SYSLOG (System Log) – Storage for network logging for maintenance reasons.
- NTP (Network Time Protocol) – Synchronization for network equipments. The NTP server (primary and secondary) receives the Stratum 1 clock signal from atomic clock and spreads to the network.

In addition to the management systems used for maintenance, supervision and provision actions all relevant alarm conditions are being supervised by one umbrella supervision system. This solution permits correlation between events of this data communication network with telecommunication transmission network status, providing one integrated vision of services condition.

12.5 Conclusions

The SSN network provides standardized interfaces and high bandwidth communications between all locations where is present in order to reduce communications operational costs but improving the overall performance.

SSN is being gradually used for internal Ethernet/IP services: LAN/WAN implementation, SCADA, utility data applications, access from substation location to corporative applications (SAP, email, intranet, etc), IP video-surveillance and telephony, and others. Some implementations of VPNs dedicated to specific clients related to RENs activities are being also provided.

The future development, second phase, will emphasize the coverage of several new substations, to provide the some IP/Ethernet services as given in first phase, the growth of MPLS cloud to the substation level as well as the duplication of the central systems (servers, applications and management systems) in RENs disaster recovery site.

13 APPENDICES

Appendix 1 – Ethernet Related Standards

IEEE Standards	
IEEE 802.1D	Spanning Tree
IEEE 802.1w	Rapid Spanning Tree
IEEE 802.1s	Multiple Spanning Tree, Superseded by 802.1D
IEEE 802.1Q	VLAN
IEEE 802.1p	Priority Assignment
IEEE 802.1x	Port-Based Network Access Control.
IEEE 802.1ad	Provider Bridge, Amendment to IEEE Std 802.1Q-2005.
IEEE 802.3	Ethernet Standard
IEEE 802.3u	100BASE-TX Fast Ethernet
IEEE 802.3x	Full-duplex Flow Control
IEEE 802.3ab	1000BASE-T Gigabit Ethernet
IEEE 802.3ad	Link Aggregation Control
IEEE 802.3af	Power Over Ethernet
IEEE 802.11	Wireless LAN Standard (WiFi)
IEEE 802.15	Wireless Personal Area Networks
IEEE 802.16	Wireless Metropolitan Network standard (WiMAX)
IEEE 802.17	Resilient Packet Ring (RPR) Access Method & PHY Layer Specifications
ITU-T Recommendations	
ITU-T G.991.x	HDSL/SHDSL (High bit rate Digital Subscriber Line) ⇨ G.991.1/1998: HDSL ⇨ G.991.2/2003: SHDSL (Single-pair HDSL) ⇨ G.991.2: SHDSL.bis
ITU-T G.992.x	ADSL (Asymmetric digital subscriber line) ⇨ G992.1/1999 : **ADSL** ⇨ G992.1/2000: **SSDSL** (Synchronized symmetric DSL) ⇨ G.992.3/2001-05: **ADSL2** (Asymmetric DSL 2). ⇨ G992.5/2005: **ADSL2+** (Asymmetric digital subscriber line 2 plus)
ITU-T G.993.x	VDSL2 (Very-high-bit-rate DSL 2) ⇨ G.993.2/2006: **VDSL2**
ITU-T G.998.x	xDSL-Ethernet
ITU-T G.7041	Generic Framing Procedure (also ITU-T Y.1303)
ITU-T G.7042	Link Capacity Adjustment Scheme for virtual concatenated signals (also ITU-T Y.1305)
ITU-T G.7043	Virtual concatenation of PDH signals (also ITU-T Y.1343)
ITU-T G.8031	Ethernet Protection Switch (also ITU-T Y.1720)
ITU-T G.8040	GFP frame mapping into PDH (also ITU-T Y.1340)
ITU-T G.8261	Timing and synchronization aspects in packet networks
ITU-T Y.1730	Requirements for OAM (Operation, Administration and Maintenance) functions in Ethernet based networks
ITU-T Y.1731	OAM functions and mechanisms for Ethernet based networks

Appendix 2 – Abbreviations

ADSL	Asymmetric Digital Subscriber Line
AMI	Advanced Metering Infrastructure
ATM	Asynchronous Transfer Mode
BPLC	Broadband Power Line Communication
BUS	Broadcast and Unknown Server
CD	Collision Detection
CDMA	Code Division Multiple Access
CMDB	Configuration Management DataBase
CoS	Class of Service
CRC	Cyclic Redundacy Code
CSMA	Carrier Sense Multiple Access
CWDM	Coarse Wavelength Division Multiplexing
DMZ	De-militarized Zone
DNS	Domain Name Server
DoS	Denial of Service
DPLC	Digital Power Line Carrier
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DWDM	Dense Wavelength Division Multiplexing
EDFA	Erbium Doped Fibre Amplifier
EFM	Ethernet in the First Mile
EIRP	Equivalent Isotropic Radiated Power
EMC	Electromagnetic Compatibility
EMS	Energy Management System
EoPDH	Ethernet over PDH
EoS	Ethernet over SDH
EPL	Ethernet Private Line
EPLAN	Ethernet Private LAN
EPON	Ethernet Passive Optical Network
ERP	Ethernet Ring Protection
EVPL	Ethernet Virtual Private Line
EVPLAN	Ethernet Virtual Private LAN
FCAPS	“Fault, Configuration, Accounting, Performance and Security” management
FEC	Forward Error Correction
FEC	Forwarding Equivalence Class
FTTX	Fibre To The Curb, Home, etc.
GARP	Generic Attribute Registration Protocol
GFP	Generic Framing Procedure
GFP-F	Generic Framing Procedure - Frame Mapping
GFP-T	Generic Framing Procedure - Transparent Mode (low latency)
GigEth	Gigabit Ethernet
GIS	Geographical Information System
GOOSE	Generic Object Oriented Substation Event
GPRS	General Packet Radio Service
GPS	Geostationary Positioning Satellite
GSE	Generic Substation Event
GSM	Global System for Mobile Communication
GVRP	Generic VLAN Registration Protocol
HDLC	High-level Data Link Control
HDSL	High Speed Digital Subscriber Line
HMI	Human Machine Interface
HSDPA	High Speed Downlink Packet Access
HTTP	HyperText Transfer Protocol

ICCP	Inter-Control Centre Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IDU	Indoor Unit
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronic Engineering
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internetworking Protocol
IPG	Inter-packet Gap
IPS	Intrusion Protection System
ISP	Internet Service Provider
ITU-T	International Telecommunication Union
LAN	Local Area Network
LANE	LAN Emulation
LCAP	Link Aggregation Control Protocol
LCAS	Link Capacity Adjustment Scheme
LDP	Label Distribution Protocol
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
LN	Logical Node
LOS	Line-of-Sight
LSP	Label Switched Path
LSR	Label Switch Router
MAC	Medium Access Control
MAN	Metropolitan Area Network
MEF	Metro Ethernet Forum
MIB	Management Information Base
MM	Multimode Fibre
MMS	Manufacturing Messaging Specification
MPLS	Multi Protocol Label Switching
MPLS-TP	MPLS Transport Profile
MSTP	Multiple Spanning Tree Protocol
NLOS	Non-Line-of-Sight
NMS	Network management system
OAM	Operation, Administration & Maintenance
ODF	Optical Distribution Frame
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplexing
OSPF	Open Shortest Path First
PAD	Packet Assembler Disassembler
PBB	Provider Backbone Bridge
PDH	Plesiochronous Digital Hierarchy
PLC	Power Line Carrier
POE	Power over Ethernet
PON	Passive Optical Network
POS	Packet over Sonet (similar to EoS)
PPP	Point to Point Protocol
PRP	Parallel Redundancy Protocol
PSTN	Plain Switched Telephone Network
PW	Pseudo-Wire
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service

RF	Radio Frequency
RMON	Remote Monitoring
RPR	Resilient Packet Ring
RSTP	Rapid Spanning Tree Protocol
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
RTU	Remote Terminal Unit
SAN	Storage Area Network
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition (system)
SDH	Synchronous Digital Hierarchy
SHDSL	Single-pair High Speed Digital Subscriber Line
SLA	Service Level Agreement
SM	Single Mode Fibre
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SNTP	Simple Network Time Protocol
SONET	Synchronous Optical Network
SSDSL	Synchronized Symmetric Digital Subscriber Line
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
STP	Shielded Twisted Pair
SV	Sampled Value
TASE	Telecontrol Application Service Element
TCP	Transport Control Protocol
TC-PAM	Trellis Coded Pulse Amplitude Modulation
TDM	Time Division Multiplexing
TE	Traffic Engineering
TLS	Transport Layer Security
TPC	Twisted Pair Cable
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunication System
UTP	Unshielded Twisted Pair
VC	Virtual Container (in SDH)
VCAT	Virtual Concatenation
VCG	Virtual Concatenation Group
VDSL	Very High bitrate Digital Subscriber Line
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VOD	Video on Demand
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VSAT	Very Small Aperture (satellite) Terminal
VT	Virtual Tributary
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA / WPA2	WiFi Protected Access
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
XPIC	Cross-Polarization Interference Cancellation

Appendix 3 – References

1	CIGRE D2, Ethernet Transport in Power Utility Communication Networks, CIGRE D2 Tutorial, Cuernavaca, Mexico, 2005	General
2	CIGRE Technical Brochure 315, Communications technology fundamentals for the design of modern Protection and Control systems, April 2007	Section 2.2 & Chapter 9
3	Potential Applications of Resilient Packet Ring Technology for Power Utilities, CIGRE WG D2.07, CIGRE Session 2002, Paris.	section 3.2
4	H. Kirrmann, M. Hansson, P. Muri, IEC 62439 PRP- Bumpless recovery for highly available, hard real-time industrial networks, paper presented to IEEE ETFA conference, 2007	Section 3.3
5	IEEE PSRC H6, Application Considerations of IEC 61850/UCA2 for Substation Ethernet Local Area Network Communication for Protection and Control, IEEE PES/PSRC Special Report	Section 3.4
6	CIGRE Technical Brochure 317, Security for information systems and intranets in electric power systems, April 2007	Section 3.5 & section 10.5
7	B. Fette, R. Aiello, et al. , RF & Wireless Technologies, Elsevier, 2008	Chapter 7
8	CIGRE Technical Brochure 318, WIFI Protected access for Protection and Automation, Working Group B5-22, April 2007	Chapter 7
9	P. Skeffington, WiMAX in the Utility Sector, EUTC 2008, Lisbon	Chapter 7
10	IETF - RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks - Transport of Layer 2 Frames over MPLS	Chapter 8
11	S. Halabi, Metro Ethernet, CiscoPress, 2003	Section 1.3 & Chapter 8
12	T. Kenyon, High Performance Data Network Design, Digital Press 2002	Chapter 10
13	Perlman, Radia. Interconnections, Second Edition: Bridges, Routers, Switches, and Internetworking Protocols. Boston: Addison Wesley, 1999	Section 10.1
14	Ethernet in the Substation, M. Pozzuoli, R. Moore, Paper presented to the IEEE PES General Meeting, June 2006	Section 10.2
15	A. Clemm: Network Management Fundamentals. CiscoPress, 2006	Section 10.4
16	MIL-HDBK-61A Configuration Management Guidance, Feb. 2001	Section 10.4
17	IEEE 802.3af Power Over Ethernet: - A Radical New Technology, www.PowerOverEthernet.com	Section 11.4
18	UTC, Substation Communications: Enabler of Automation, UTC Report, Nov. 2006	Section 9 & 10

19	IEC61850-5, Communication networks and systems in substations. Part 5, Communication requirements for functions and device models", 2003	Section 9.1
20	Ethernet LAN Reliability in Electrical Substations", Arzuaga, J.M., Cadenas, A., Paper presented to XII CIGRE ERIAC, 2007	Section 10.1
21	RFC2544 Benchmarking methodology for network interconnect devices	Section 10.1
22	CIGRE Technical Brochure 341 "Integrated Management Information in Utilities", February 2008	Section 10.4
23	CIGRE Technical Brochure 249, "Integrated Service Networks for Utilities", August 2004	Section 10.4.4
24	CIGRE Technical Brochure 153, The use of IP technology in the Power Utility Environment, April 2000	Section 10.9
25	Substation Migration into an IP Network, Cigre WG35.07, CIGRE Session, Paris 2002	Section 10.12
26	Architectures for the Migration and Progressive Deployment of 61850 in Legacy Substations, C. Samitier, R. Pellizzoni, CIGRE SCD2 Colloquium 2005, Cuernavaca, Mexico	Section 10.12