507

Communication Architecture for IP-based Substation Applications

Working Group D2.28

August 2012

COMMUNICATION ARCHITECTURE FOR IP–BASED SUBSTATION APPLICATIONS

WG D2.28

Members

H. RIIS, **Convenor** (DK), J. FONSECA, **Secretary** (PT), A. MOAINI (FR), A. ARZUAGA (ES), D. BORDEA (RO), J. DARNE (ES), J. FEIJOO MARTINEZ (ES), L. LHASSANI (NL), M. GORAJ (ES), M. FLOHIL (NL), M. JANSSEN (NL), M. SCHATZ (CH), M. STEENSHARD (DK), M. GROSSINHO (PT), O. CODREANU (RO), T. V. PEDERSEN (NO), S. SALYANI (UK),

Corresponding Members

A. WALLACE (NZ), E. MELO (BR), A. SILFVERBERG (FI), P. CRISTAUDO (AU), R. PELLIZZONI (AR)

Communication Architecture for IP-based Substation Applications

Table of Contents

Figures

Tables

EXECUTIVE SUMMARY

IP communication is being extensively introduced into the operation of the Electrical Power Utility. The substation IP network environment has evolved from acting as an extension of the office LAN to a state, where it is carrying multiple services, including the transport of critical and sensitive data.

IP communication, being a one-platform solution which relieves you from designing and maintaining more than one network, is definitely not a one-technology solution. Therefore, the implementation of an IP network needs to be carefully planned in order to achieve the expected scalability and performance.

This Technical Brochure includes the following:

- A compilation of user requirements and expectations concerning existing and envisaged services in the new networked environment of the substation.
- A description of possible network migration processes
- Guidelines on how to choose an optimum network architecture
- A description of important parameters to be considered for each relevant technology.
- Six case studies describing project and process experiences

1 Introduction

IP communication is being extensively introduced into the operation of the Electric Power Utility.

The substation IP network environment has evolved from acting as an extension of the office LAN to a state, where it is carrying multiple services, including the transport of critical and sensitive data.

The multiplicity and the variety of new and existing IP-based applications in the High Voltage substations create the need to investigate the requirements of users and services as well as developing guidelines for a successful implementation.

This Technical Brochure contains

- A compilation of user requirements and expectations concerning existing and envisaged services in the new networked environment of the substation. This information was gathered by conducting a survey among Cigré members and major vendors
- A description of a possible network migration processes
- Guidelines on how to choose an optimum network architecture, covering all services which require connectivity beyond the substation perimeter
- Technical details for technologies that are commonly used in the document
- Six case studies from utilities, aiming at describing project and process experiences, rather than technicalities

We describe important parameters to be considered for each different main technology. It is not centered on specific applications and is therefore open to the usage of IP in different areas.

The brochure was created over a 2 year period, started in 2009, and the contributions were merged and coordinated through teleconferences and a total of 6 physical working group meetings. During the development phase, a survey was conducted which had a good response: 58 individual responses from 30 countries.

2 Requirements from users

Information technology enables the exchange of large amounts of data over great distances. The Internet Protocol IP is currently the most used protocol. IP offers new opportunities for information exchange for utilities. This chapter describes the current status of IP implementation and future plans for IP implementation for applications used by utilities. This chapter also describes the barriers and challenges that utilities encounter when implementing IP.

Electric Power Utilities (EPU) are migrating TDM systems and applications onto IP protocols. Some applications reside and work within the substation perimeter, and some applications work beyond the substation perimeter.

Control and protection systems are of crucial importance in the substation. Some of these applications are moving onto an IP platform and require utmost attention with respect to information security and resilience. Protection signals in particular have strict requirements in terms of performance requirements (e.g. delay or delay variation), which are very challenging for packet switched networks. Other applications represent different challenges to the system integrator.

Cigré Joint Working Group B5/D2.30 is dealing with communication for teleprotection.

2.1 Survey

In order to obtain a better view of the IP-based substation applications currently used and the communication architectures in use or being planned, a survey was conducted amongst CIGRE study committee D2.28 and other CIGRE members. In total 120 members were approached. The survey is included in appendix 1. Of the 120 surveys sent, 58 filled out questionnaires were received.

The survey was completed December 2010.

The results of the survey are presented in the following figures and comments. A preliminary version of the results has been published through Cigré as a separate document.

2.1.1 Survey response general aspects

The 58 filled out surveys were received from 51 individual companies, based in 30 different countries. The detailed results including answers to the questions asked in the survey as well as comments are presented in the next sections. Figure 1 shows which countries have responded and what percentage of the results they represent.

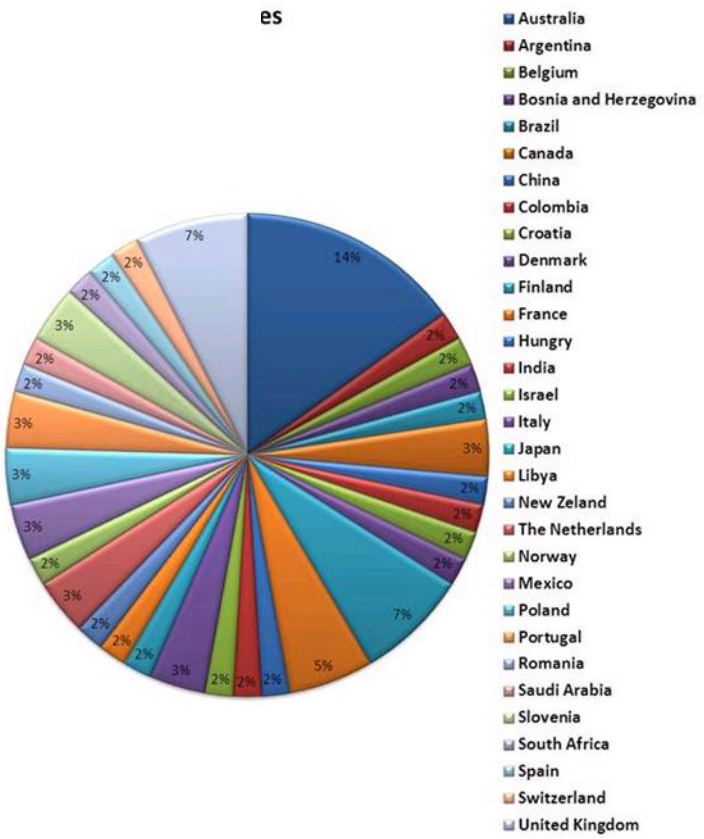


Figure 1 : Countries represented in the survey responses

Figure 2 shows the kind of companies that the participants work for.

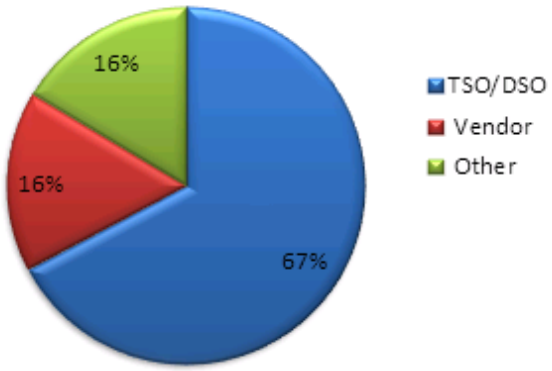


Figure 2: Survey responses per company type

Most of the participants work for Transmission- or Distribution- System Operators. Participants not working for TSO's, DSO's or vendors indicated that they work for a/work as:

- Consulting firm
- Research institute
- Generation company
- Telecommunication company
- Transmission company

- Power supply company

2.1.2 Survey summary and comments

The 58 respondents provided very detailed answers. These answers have been analyzed and a summary as well as the related comments are described hereafter.

Most used substation applications using IP and IP networks

When asked what the most used substation applications using IP and IP networks are, 81% of the participants indicated that they use applications for Network Management and Data Communication. On the other side, 71% of all participants indicated that IP is used for Inter Control Center Connections. The detailed results are shown in Figure 3

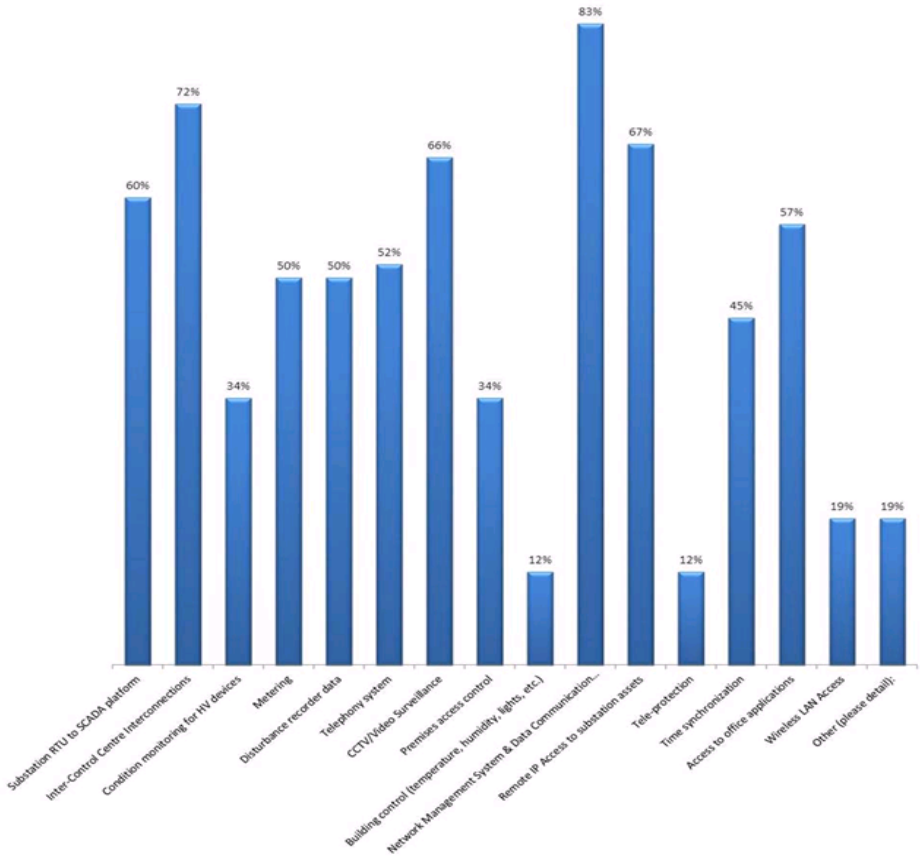


Figure 3: Most used substation applications using IP

In addition to the given list of application the following other substation applications using IP and IP Networks were mentioned:

- PMU (Phasor Measurement Unit)
- “Substation Protection and Control Systems”
- Station bus and Process bus applications
- Sequence of events recorder
- Dynamic system monitor
- Monitoring/ control & protection of IEC 61850 based substations

IP is widely used however, the building automation and the use of tele-protection is not widely used (only 12%).

2.1.2.2 The main challenges using IP in the substation environment

It was no surprise that the main challenge when using IP in the substation environment is security. 88% of the participants indicated that they see security as an operational challenge. Besides security, converting information communicated over legacy interfaces to IP (67%) and training personnel in using IP (59%) offer the biggest operational challenges. An overview of the operational challenges is shown in Figure 4

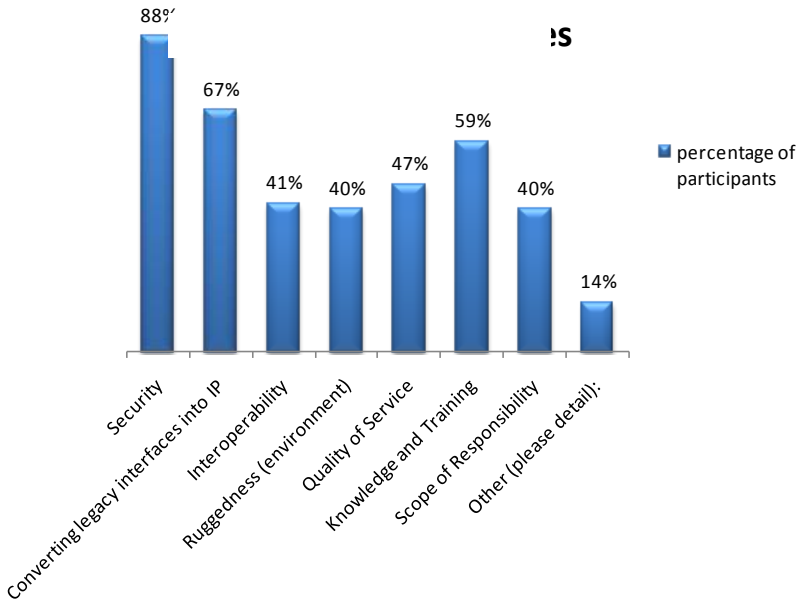


Figure 4: Main challenges for IP in the substation environment

Additional concerns that were expressed by the respondents include:

- Communication for current differential protection equipment over packet switched networks: strong requirements on delay (< 10 ms), path symmetry and jitter (< 250 µs)
- Enough security features in Substation devices
- Cost reduction in communications between substation and control: IP network vs. point-to-point redundant communication links
- Equipment:
    - The ruggedized IP hardware lacks features and perceived to be expensive
    - Compliant with IEEE1613 (Environmental Standards for Networking Devices Installed in Power Utility Substations) and IEC 61850 (Communication Networks and Systems in Substations) specifications that also supports current features like VLAN tagging and SFPs
- Dynamic routing
- Addressing scheme: IP address allocation/management
- Scope of Responsibility
- Project teams and human resources handling: Mix teams of Control Engineers, Protection Engineers and Communication Engineers is necessary

- All of these challenges can be migrated by using: leased lines
- Awareness of management, protection- and control-engineers

2.1.2.3 Main concerns with using IP protocol in substation applications

The previous question showed that security and knowledge of IP form the biggest operational challenges. This is also reflected in the answers to the question: “What are the main psychological barriers with using IP protocols in the substation environment?” The results are shown in Figure 5

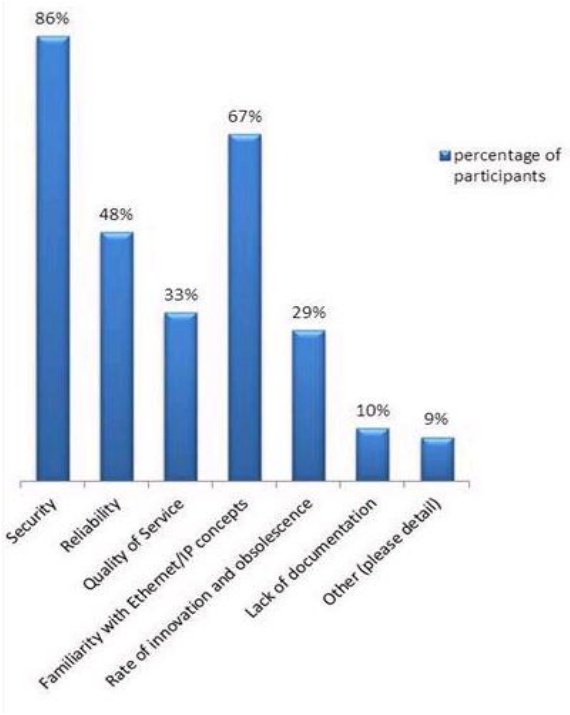


Figure 5: Psychological barriers

Other psychological barriers that were indicated by the participants are:

- Ethernet robustness:
    - Nondeterministic
    - There is a finite probability that packets containing critical data will not be delivered
    - Ethernet is subject to interruption from broadcast storms caused by malfunctioning equipment or routing table errors
- Lack of equipment that complies with real time timing requirements that are necessary for certain communication
- No psychological barriers

From the results of these two questions we can emphasize the training and awareness of Ethernet/IP technologies is critical to demystify it. On the other side security (physical network and cyber security) must be a top one priority from the beginning of network design.

2.1.2.4 IP compatibility of applications

As shown in Figure 6, almost 4 out of 5 participants indicated that not all of their applications are IP compatible.

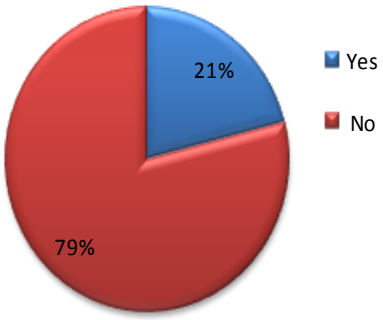


Figure 6: IP compatibility of applications

Participants indicated that the following applications are not IP compatible:

- Protection signaling, Metering, Unit Controllers and local HMI
- Counters, quality control (analog modems), will be used Ethernet convertors
- Tele-protection (possibility to migrate to MPLS or Ethernet network)
- Current differential protection (no migration predicted)
- Dial-up modems incompatible with VoIP and incompatible with packet data (like GPRS)
- Legacy substation equipment without IP or serial interfaces

Prediction of migration of operational communication into IP

As shown in Figure 7, just over half of all participants expect to have all operational communications go through IP within the next five years (5% already done, 13% in 1-2 years and 35% within 5 years). Two out of three of the participants expect that it will take more than ten years before all communication is migrated.

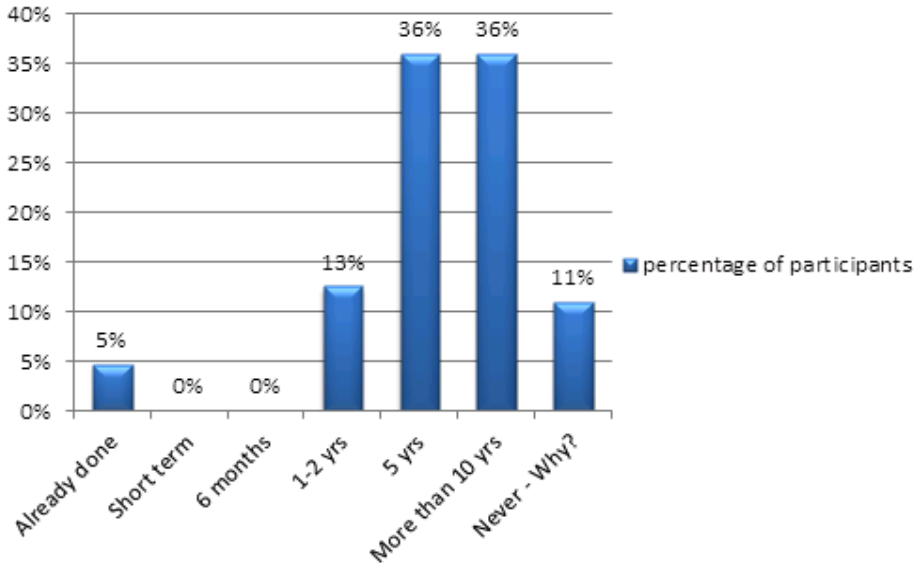


Figure 7: Prediction of migration time

Participants indicating that they expected that a full migration would never take place, gave the following explanations:

- Expecting something new to come before all communication is migrated to IP (example Next generation IP)
- Migration of time critical applications as tele-protection services is not foreseen to migrate to IP until reliable standards and proven products become available in the market
- There will always be applications where IP communication is not suited, either due to geographic or economic reasons
- Big investment

Some questions do arise:

- Is IP/Ethernet the only option for the future telecom network?
- TDM must continue?

How to deal with legacy equipment

64% of all participants see protocol conversion through a gateway as a good way to deal with legacy equipment. 59% see protocol encapsulation as a good solution and 40% of the participants think using separate networks for IP compatible and non IP compatible equipment is a good solution. This is shown in Figure 8

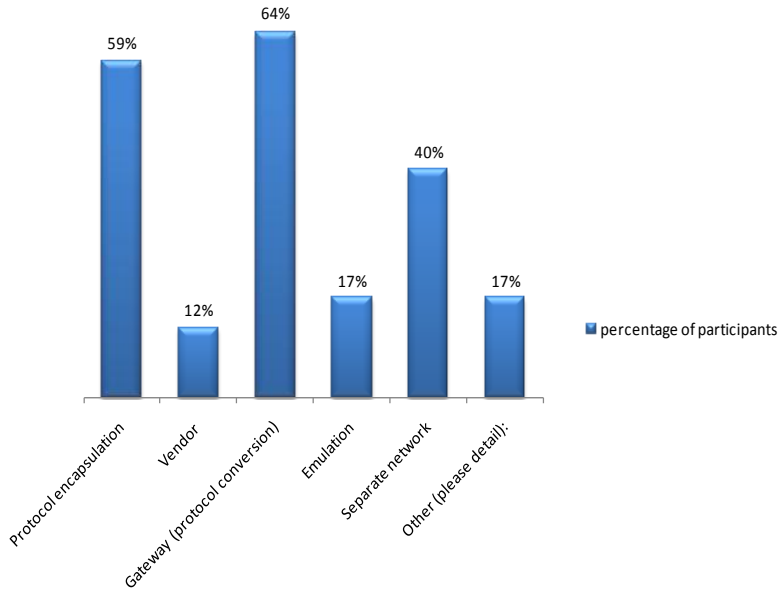


Figure 8: How to deal with legacy equipment

Other options that were mentioned as possible solution include:

Legacy equipment will be replaced in due time with IP compatible equipment

SDH and PDH used for non-compatible systems

SDH network as a backbone, which will carry traffic for both PDH (legacy) and IP systems

2.1.2.7 IP readiness of communications networks

Given recent developments in equipment using IP and the installation of IP capable networks in several project it is no surprise that 60% of the existing communication networks is ready for IP traffic. This is shown in Figure 9.

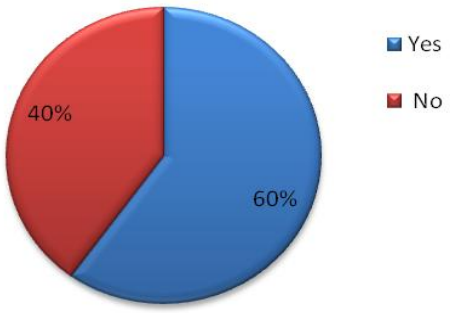


Figure 9: IP readiness of existing networks

Main reasons mentioned why actual network are not ready for IP, include:

- Existing network is being upgraded so that it will be IP ready
- Capacity / Cost
- Plans to roll out MPLS based real time network
- Some utility still use PLC equipment, IP based application requires IP access and Backbone based on broadband interfaces
- Last mile access telecommunications infrastructure needs to be upgraded to accommodate IP
- Low bandwidth, lack of Quality of Service
- IP is not widely implemented on the Transmission Network because of the cost of the Ethernet interface cards
- Many existing networks are based on TDM technology, but they are only partly ready or suitable for IP traffic
- Some small sites do not have Ethernet transmission possibilities
- Many legacy installations have a dedicated communications channel that does not support IP
- Would have to consider two types of networks, a corporate and other operative network […]
- The whole existing network is IP ready, except for radially connected station using PLCC link as last mile connectivity
- Analog equipment exists in some areas of the network
- Existing network is being upgraded so that it will be IP ready

2.1.2.8 Requisites and concerns for the telecommunication network

As shown in Figure 10, the existence of physical infrastructure and the availability of suitable transport technologies are the main requisites and concerns.

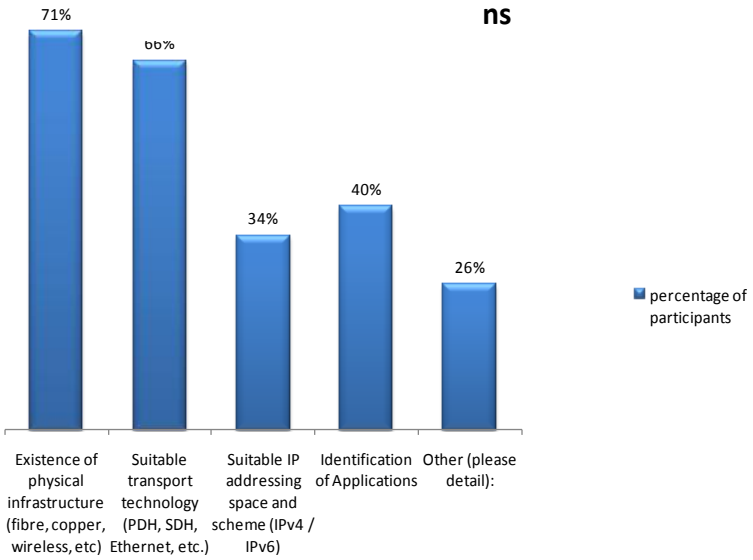


Figure 10: Requisites and concerns

Other requisites and concerns mentioned by the survey participants include:

- Segregation of SCADA & Protection from non-certified/authorised use
- A typical and strong communication requirements of current differential protections
- Training, QoS, Security Interface (firewalls, ACL's)
- Too many applications are today on mobile data
- Typical minimum system availability for SCADA and Protection services is 99.9%
- Identification of performance parameters for applications
- Network bottlenecks caused by mixed core of optical fibre and radio systems
- For the leased links (telecommunication service outsourced), because of the evolution of the technical offer, it is difficult to find a service equivalent to the previous technical offer
- Security using MPLS
- Ability to physically segregate operation traffic to ensure security is not compromised
- Security on the network, especially segregation of SCADA & Protection from non-certified/authorized use
- Security and availability of services

2.1.2.9 Most promising IP technology for secure IP communications

As shown in Figure 11, MPLS (IP over fiber) and SDH (Ethernet over SDH) are seen as the most promising technologies to provide secure and reliable IP communications.

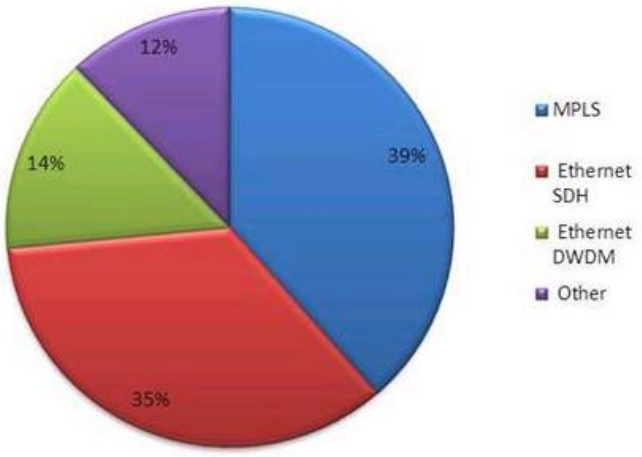


Figure 11: Most promising IP technology

Other options mentioned include:

- For security end-to-end encryption is the solution
- MPLS / IP (IETF) and MPLS / TP (ITU-IETF)
- MPLS (over optical fibre and lower capacity links such as SDH or PDH radio)
- MPLS (over DWDM)
- Point to point L2 Ethernet services delivered over SDH transport, MPLS provides excellent routing and failover capability but does add complexity and higher latency
- The most promising technology depends on the resources available:
    - Existing network architecture
    - Installed equipment
    - Path lengths
    - IP requirements, etc.
- Require physical segregation from traditional IT infrastructure

2.1.2.10 Should the IP network be reserved for operational service or also be used for corporate services?

On the question whether the IP network should be reserved for operational service or also be used for corporate services, the clear preference is have separate networks (either virtual or logical). Figure 12 shows, per option, the percentage of participants that selected the option.

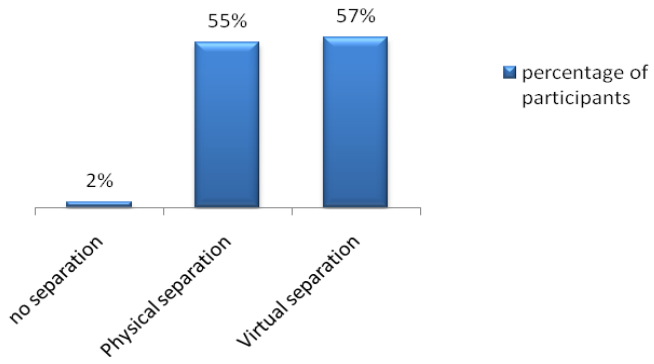


Figure 12: Shared or separate networks

2.1.2.11 Most promising technology to separate and provision different types of IP services

Finally Virtual Private Networks (Layer 3) are seen as the most promising technology to separate and provision different types of IP services, as shown in Figure 13

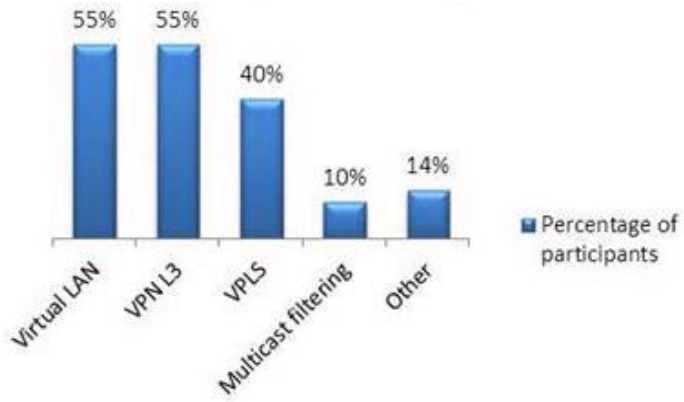


Figure 13: Technology to separate and provision different IP services

Besides the options given the following other options were mentioned:

- VPWS (Virtual Private Wire Service): encapsulation of legacy interfaces over IP services
- VLAN separation is good for service separation at the access layer but does not scale at the transport layer
- L2 VPLS (Virtual Private LAN Service) and L3 VPRNs (Virtual Private Routed Network) provide good transport layer separation and each filling a slightly different need.
- MPLS
- Physically separated networks
- We are not convinced that any of the technologies mentioned here will provide the necessary security

2.2 Conclusions from the survey

This section describes which challenges have to be taken on when applying IP based communication in a utility environment.

During recent years, there has been a continuous trend driven by the evolution of mainstream Telecom to have multiple services over IP (or IP convergence). Apart from the traditional data transport services, new services have arisen - such as voice over IP, video over IP, wireless IP (mobility). All telecom is moving to a multiservice environment where most of the traffic, independently of its nature or underlying application, is based on IP.

As a result of this, electric utilities are facing a new challenge where they have to manage the existing (traditional) IP applications, but at the same time many other applications which were not IP-native need to be migrated to operate in similar (or even the same) IP networking infrastructure.

Utilities are beginning to face this issue, as their grid infrastructure needs to evolve to cope with new operational requirements. The arrival of Smart Grids, Super Grids and Micro Grids imposes new requirements on the utilities' telecom networks, which need to be ready for the future, such as:

- Installation of bidirectional, communications enabled electricity meters in the end customer's premises
- Enabling active demand and participation of consumers in the power system market
- Need to improve the operations & maintenance of the electricity grid
- Real time protection and automation of both distribution and transmission infrastructure

For instance, SCADA applications continue to be one of the most important utility applications for the operation of transmission and distribution networks, and this application has been for many years and protocol generations outside of the IP world. Traditionally the utilities have had control over power generation plants and primary substations. Driven by new requirements such as SmartGrid applications there is a growing need to also control medium voltage installations, secondary substations and feeders. The control system must have a complete view of the whole electricity grid, and the telecom and networking applications must be able to fulfill this requirement. This requirement imposes complete new challenges for SCADA systems which in turn are being transferred to IP.

Another application example is that new regulatory frameworks in many parts of the world are forcing the electric utilities to start projects in order to see how they can provide bi directional communication to home metering devices. One of the main challenges however is the reachability of the meters. Fiber or copper may not be available and wireless technologies might have to be used. A common approach will be to install IED's in secondary substations that will gather all metering information and manage customer electricity demand. This implies that secondary substations will require bi-directional (IP) connectivity.

On the other hand, DSOs are also thinking of how they can automate their distribution grid. All primary substations are already automated in most utilities. Now it's time to increase the automation level of secondary substations.

From a pure telecom perspective, the following connectivity challenges are anticipated:

- In short term we need to provide connectivity to more electric installations to and from SCADA and integrate the legacy RTU and SCADA systems in the new IP network architecture
- In long term, to provide some of the services mentioned before, we will also require both, peer to peer (horizontal, substation to substation or IED to IED) and SCADA (vertical, substation or IED to central dispatch) connectivity in order to manage and control the infrastructure

Many other challenges are just popping up as a result of this process, such as how are the IP applications running on new installations going to access the utility backbone network? Should the utility invest in its own infrastructure or should it buy or lease a service from a 3rd party network carrier? Are all legacy applications and services to be migrated to IP for simplicity or is there some compromise? These questions require careful discussion at the utility taking into account different views and requirements.

3 Network Migration Process

New generation IP networks can be a promising solution to provide reliable and cost-effective services for substation applications. At the same time migration from legacy networks to IP based networks presents several technical and operational challenges to both concerned parties: carrier and end user1.

In order to meet these challenges, a rigorous migration process shall be developed; this process has to take into consideration the characteristics and requirements that will be discussed in the next paragraphs. The migration process is divided in three key phases:

- Pre-migration
- Migration
- Post migration

During each phase a dedicated action list and workflow must be managed.

Further information can be found in [Reference 2]

3.1 Lifecycle considerations

The following five aspects drive the lifecycle management of a power utility's telecommunication network:

1. Initial investments

Most EPU's have already an IP network. It is rarely deployed from scratch. In both cases we have to deal with the following parts and their investments:

a. Infrastructure:

EPU's usually have existing infrastructures, owned or leased. The existing infrastructures then have to be used to connect to the substations. See also 0.

b. Active devices

Active devices are needed to deploy transmission and data communication network based for example on SDH, MPLS, Ethernet devices (routers, switches, firewalls etc.)

c. Knowledge and support

The network has to be built and secured. This can be done through a vendor and / or an own staff. These services are managed through a data communication department for example or through the vendor.

2. Operation & maintenance

The cost is the main driver that directly affects the lifecycle management of equipment in the network. When selecting new technologies /equipment the following aspects should be considered:

- Establishment of cost limits for operation / maintenance activities.
- Analysis of the cost evolution regarding the operational and maintenance activities.
- Frequency of incidents and problems
- Availability of expertise personnel

[1] Carrier and end user can be two different departments within the power utility organization or two external parties.

- Availability of spare parts

These considerations directly influence the decision whether or not to implement the technology / equipment.

3. Failure & downtime:

Repetitive failures and downtime can damage the company's corporate image. Therefore it is necessary to maintain the monitoring of the quality of service within the network and to plan migration when the equipment cannot assure the required minimum availability.

4. Service innovation

Innovation of standards, new services and features is also an important aspect that can trigger the migration to new technology/equipment.

5. Obsolescence of technical support and experts (Human factor)

Network operational activities require the availability of technical support in "acceptable" time. Technical support can be internal or external based on company policy. When the technical support/expert (internal & external) becomes obsolete, it is very important to evaluate the cost and the effort to train new technical resources or to plan a migration to new technology / equipment.

A business case study should be conducted in the pre-migration design phase in order to justify the need of the migration to new technology / equipment based on the five aspects described above.

3.2 Service migration characteristics

Telecommunication network migration processes have characteristics that differ from other operational activities:

- Time dimension: Typically, a migration process contains several tasks and an associated timeline. Each migration process can take a "long" time to achieve a complete service migration.

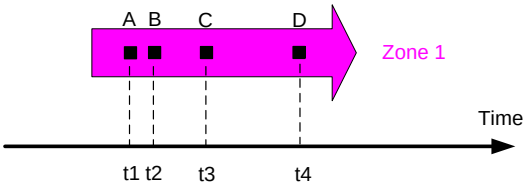


Figure 14: Example of service migration & time dimension

In Figure 14, the tasks "A", "B", "C" and "D" have to be executed in the associated timeline "t1", "t2", "t3" and "t4". Moreover, it is mandatory to respect the order and the sequence planned for each task.

- Space dimension: A migration process is generally applied in wide geographical zones (or batches). It is very important in the pre-design migration phase to identify the geographical zones where the migration shall be executed. Several criteria can determine the geographical zones and associated borders (data flow scheme, prioritization of users, alphabetical order…)
- Space time combination: The migration process shall clearly show the correlation between various zones and associated time line. In Figure 15, task "C" in zone 1, task "B" in zone 2 and task "A" in zone n have to be executed at the same time "tm"

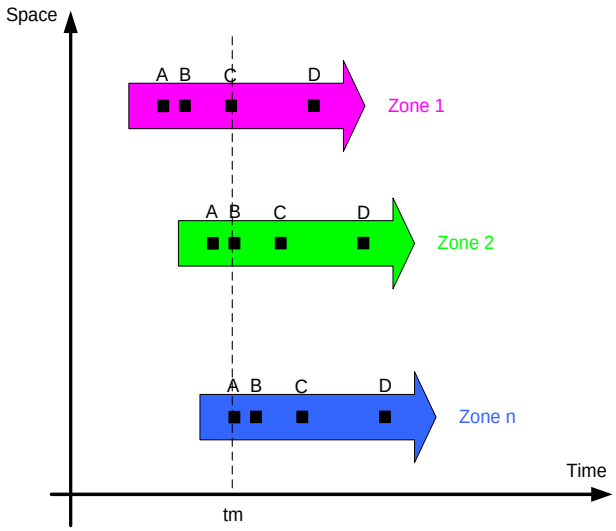


Figure 15: Example of service migration and spacetime

It is very important to keep in mind that the migration process is very critical for end user experience, both during and after migration phases.

3.3 A Possible service migration process

Several requirements have to be considered in migration design to have an integrated and consistent service migration process.

The migration process is critical, the service must be guaranteed all the time or in some cases the disturbance should be minimized to acceptable values.

This process requires an effective risk planning where several aspects can be identified that must be taken into account.

This planning can be done using a matrix with the following fields:

- Identification of the risk:
  - Description of the risk
  - Origin and cause
  - Probability to occur [1= low, 5=high]
  - Impact on the process [1= low, 5=high]
  - Importance [probability * impact]
- Mitigation plan:
  - Mitigation actions
  - Contingency plan
  - Definition of monitor indicators
- Execution plan:
  - Monitoring starting date
  - Monitoring finishing date

- Responsibilities

The service migration process can be divided into the following four phases:

1. Feasibility & business approval
2. Service migration design
3. Implementation & tests
4. Migration statement

The first step in any migration process is to find out if the intended migration is (financially) feasible. If the migration is thought to be feasible, a detailed migration strategy and plan can be made, and those who will be affected by the migration can be informed. Once the migration plan is completed, the migration can be implemented and tested. After the migration has been fully implemented and tested, the migration process and the effects of the migration should be evaluated. The evaluation results should be documented, so that the lessons learned from the migration can be used for future migrations. Figure 16 gives an overview of the service migration process. This overview is given in this brochure as an example; other model can be proposed depending on the project and the type of migration.

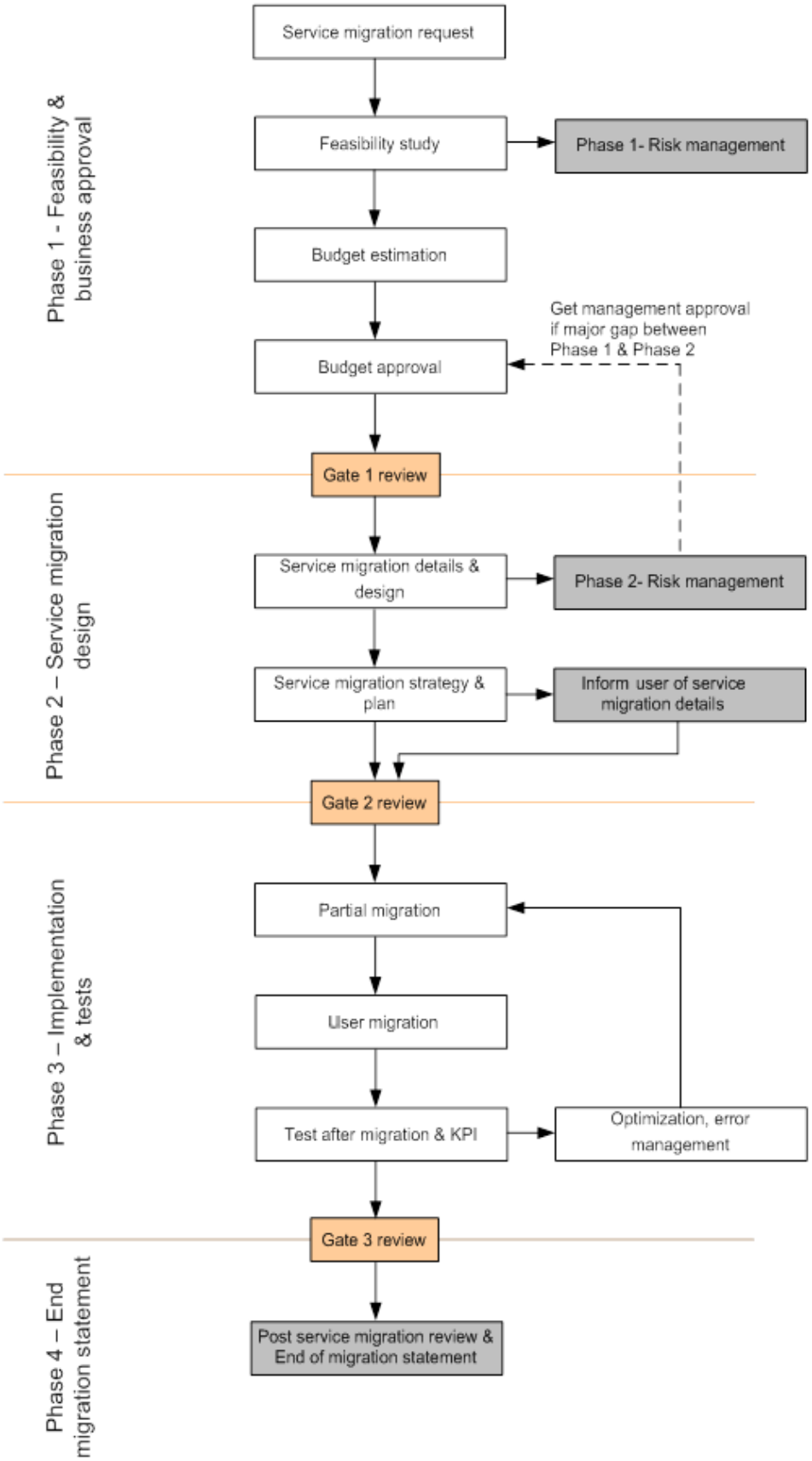

Phase 1 - Feasibility & business approval
Service migration request
Feasibility study
Phase 1- Risk management
Budget estimation
Get management approval if major gap between Phase 1 & Phase 2
Budget approval
Gate 1 review
Phase 2 – Service migration design
Service migration details & design
Phase 2- Risk management
Service migration strategy & plan
Inform user of service migration details
Gate 2 review
Phase 3 – Implementation & tests
Partial migration
User migration
Test after migration & KPI
Optimization, error management
Gate 3 review
Phase 4 – End migration statement
Post service migration review & End of migration statement

Figure 16: Example of service migration process

3.3.1 Phase 1 Feasibility & business approval

Service migration request

- Service migration could be required due to degradation of QoS in the network. It can be also requested by the Service Integrator due to development of new feature or due to obsolescence of equipment (or technology).

Feasibility study

- Identification of applications and end users to be migrated
- Estimation of migration impact on the service (downtime, shutdown window etc.), and checking with end user if the impact is acceptable

Budget estimation

- Estimation of resource requirement
- Estimation of cost and timescale of migration activities
- Estimation of return of investment after migration

Budget approval

- Project management shall present budget estimation and get budget approval from the appropriate authorities

[GATE 1 review]

At the end of Phase 1, a ”Gate 1 review” meeting shall be set up to decide if service migration can be implemented or to remain on the current service.

Once the migration project is approved, the budget and the resource can be allocated and the service migration design phase can be started.

3.3.2 Phase 2 Service migration design

Service migration detail & design

- Performing a site survey and a network audit is recommended and will assist in providing the inputs required to finalize migration design: physical assets, spare capacity, availability of existing frames, (ODF, MDF)
- Identification of acceptable downtime values for each application
- Check if both services (old and new) can work at the same time (to minimize migration impact), identification of opportunities and risk related to this
- Submission of all technical design documents for approval

Service migration strategy & plan

- Definition of geographical zones and batches; this can be based on dataflow exchange and priority of site and users
- Risk management: If critical services are to be migrated, a worst case scenario analysis must be carried out in advance in order to identify and mitigate weak points in the migration process. It is a key requirement that critical infrastructure must be kept up and running
- Contingency plan: Error handling and resolution in case of error occurrence has to be documented (step by step troubleshooting, roll-back procedures etc.)

- Planning definition for “implementation phase”, this planning details the execution of all migration tasks with related timescale. Each task has to be detailed and clearly described with responsibility definition
- Identification of KPI that measures the migration success criteria

Inform the users about service migration details

All migration details shall be presented in order to get formal approval for the following aspects:

- Technical design documents
- Risk management and service impacts
- Planning of ”implementation phase”

[GATE 2 review]

Once the migration design is approved, ”Gate 2 review” meeting can be set up in order to announce the beginning of ”implementation phase”.

3.3.3 Phase 3 Implementation & tests

Partial migration

- Identify available expertise in similar previous projects. After the available expertise has been identified, the operational teams which will drive network migration can be formed and the organization chart can be created.
- Set up documentation systems which can assist the operational teams to access plans, procedures, reports and other technical documents.
- Carry out all pre-migration work (if any) before the implementation of migration (e.g. logistic preparation, stations identification, labeling of circuit to migrate)
- Execute a partial migration. Partial migration consists of commissioning of the new telecommunication circuits without integration of end user interfaces
- Simulate end user interfaces, using dedicated tools and instruments to test the new circuit before real service migration
- Record all test results in specific documents
- Ensure continuous and fast communication with end user and periodical progress reporting

End user migration

- Once the partial migration is successfully completed, the migration of the end user can be performed based on the predefined planning in phase 2

Test after migration, optimization and error management

- End to end service test and performance measurement after migration, based on the previously found KPI´s.
- If major problems have been reported by KPI, it is necessary to optimize the migration methods and to redo the “implementation phase” until the correction of errors

[GATE 3 review]

Gate 3 review ensures that all planned service migration activities have been completed successfully and no tests or issues are pending.

3.3.4 Phase 4 End migration statement

Post service migration review & End of migration statement

- Monitoring of the service after the migration in order to check its stability, this shall be performed during predefined period (e.g. one or two months)
- Set up the post migration review meeting with end user to discuss the result of stability test
- If no objection regarding the results of stability tests; the service integrator can send the “As built” of technical documents (design, drawings, operator manual etc.). Consequently, the end user and the service integrator can sign the document proving the end of service migration

3.4 Legacy Serial to IP migration

In the past decades there have been myriads of applications in substations, ranging from SCADA, control, automation, maintenance, protection and others, which have relied upon protocols using serial connectivity over serial port RS-232 or RS-485 interface / links. These were point-to-point or point-to-multipoint configurations, with speeds of tens of kbit/s at best. The technology was simple, easy to debug and troubleshoot and reasonably reliable.

Substation applications have been run and managed in this way for some decades. As long as there were not additional applications or increased requirements for existing applications, there was no need to embrace a technology change.

Now, new substation automation techniques and approaches driven by new standards such as IEC 61850 have originated that technology change. New substations are built using IP-native protocols, and as a result of this many utilities face a common problem at the time of maintaining the existing infrastructure:

- Is it better to try to refurbish old substations from scratch and replace all functions and devices with modern ones, or to try to integrate legacy infrastructure and applications into the new all-IP substation system? Are the operational gains worth the extra investment?
- How to implement a centralized and automated control to all legacy devices like RTUs, protection relays and control IEDs using the IP / Ethernet network?
- Shall the existing legacy communication be moved to IP infrastructure at all? Or shall they be left running on the existing infrastructure, until their operational lifetime has expired and ‘proper’ IP solution can be implemented? Leaving the legacy data on existing infrastructure avoids the need for any conversion/integration on the level of data communication. But of course the question of integration then comes at the application level. Example: A SCADA system (Frontend) must support the handling of e.g. IP based data (IEC 60870-5-104) and existing serial data (IEC 60870-5-101)

These questions must be analyzed taking into account both operational and economic factors. In general, different paths can be observed depending on the application and sector, as seen in the survey results in chapter 0. However, many times the migration process is necessary, and some legacy systems must be integrated into the IP architecture. In these scenarios there are some common issues that have to be addressed in order to successfully integrate the infrastructure.

3.4.1 Considerations when migrating serial port based systems to IP/Ethernet interface

In addition to business and operational requirements, once a migration of a legacy application to IP has been approved, there are some technical issues that have to be carefully analyzed in order to ensure that the legacy application is going to run correctly over the new IP infrastructure. This is due to the differences in nature between packet-switching oriented networks (e.g. IP) and circuit switching or serial port based links.

Applications and protocols running over serial ports share a set of common characteristics due to the nature of the physical

- Negligible latency in comparison with the bit speed used (<100kbps), as is the case with a copper wire a few meters in length or optical fiber up to hundreds of meters in length. Then these applications may suffer when they are carried over an IP network with latencies in the order of several milliseconds or worse. If they have to traverse an IP router, the application may not work at all due to increased and random latency. So latency control is critical
- Strict timing requirements. The IP network may have an irregular distribution of latency (variance of the latency) depending on network congestion and actual traffic in each device. This may harm some applications that need strict inter-bit and inter-frame timings, initially designed for a serial port medium where this behavior does not happen or may be assimilated to a broken or damaged link
- Link Layer Control (LLC) mechanisms, which take care of error correction or detection and sequence control. Thus, some applications suffer heavily when encapsulated over the TCP protocol, which guarantees sequenced, error-free information delivery, usually at the cost of high latency and retries. UDP protocol is usually a better choice for the transmission of encapsulated legacy serial protocols, as generally it is better for serial-port based applications to receive a wrong frame in time, than to receive the correct frame too late, when link layer timers have expired
- Serial protocols often have a well-defined frame format, which must be analyzed by the devices making the serial-to-IP conversion. Whenever possible protocol frame fragmentation must be avoided, and it is often helpful - though more bandwith consuming - to encapsulate just one frame per transmitted datagram. This procedure ensures smooth protocol timing between frames. As a result of this, frame start and stop delimiters and frame length fields should be decoded by the IP encapsulator

As a rule of thumb legacy applications that match the following 3 criteria can be run smoothly when encapsulated over UDP connections in most legacy serial port oriented substation applications:

- There is a frame format correctly defined by characters or binary sequences at the beginning and end of the frame, avoiding ambiguities (predefined escape sequences, no possible ambiguities)
- There are predetermined maximum and minimum frame lengths, and where possible not too long frames are used, as this impacts negatively on latency. As an example, satisfactory results have been obtained for many tele-control protocols with a maximum frame value of 256 bytes
- There is an error detection mechanism in the protocol frame itself (CRC or similar) which allows for validation of the integrity of the protocol frame at both ends. This allows for filtering of error-containing frames before delivering them over the serial port

4 Defining the Network Architecture

From the functional point of view there are two types of communications services used by electric power companies:

- Corporate or enterprise services
- Operational services

The corporate services are used for the applications related to the Utility enterprise, market related activities and in some cases U-Telco activities (utility company being a telecommunications operator). The corporate services are not described in the document as the focus is only on the operational services.

The purpose of the operational services is to use telecommunications network and technology in order to maintain reliable, secure and efficient core operations of electric power utility. The list of typical applications realized with operational communications services is provided below:

- Protection and Control
- SCADA
- EMS/DMS
- Wide Area Monitoring Systems
- Operational Telephony Systems
- Substation Data Retrieval
- Remote Access to Devices and Asset Management
- Condition and Quality Monitoring
- Mobile Workforce Management
- Operational Cyber Security
- Operational Physical Security and Video Surveillance

Some of the applications listed above like protection and control (teleprotection or line differential protection) are well established functions practiced for many years that are critical to maintain safe and reliable operation of the electrical grid. However some of the applications are emerging functions that are becoming more and more important for improving utilities' efficiency and ensuring more intelligent decision making. These new applications include condition monitoring, mobile workforce management, etc.

Electric utilities have the choice to integrate operational and non-operational services in a combined communications infrastructure or run these services in completely separate networks. There are three possibilities how the different communications services can be realized :

- Operational and corporate services share the same network and there is no separation
- Operational and corporate services share the same network, that has logical separation with SLA (Service Level Agreement) management
- Operational and corporate services are implemented on physically separate networks

In large utilities the operational network is a combination of a Wide Area Network (WAN) and multiple Local Area Network Networks (LAN). The WAN network forms a communications backbone connecting together all major substations with the national and regional control centers. The LAN networks typically are contained within subststations and are interconnecting devices inside the substation perimeter and/or a number of remote devices located in its geographical proximity such as various sensors, controllers and smart meters.

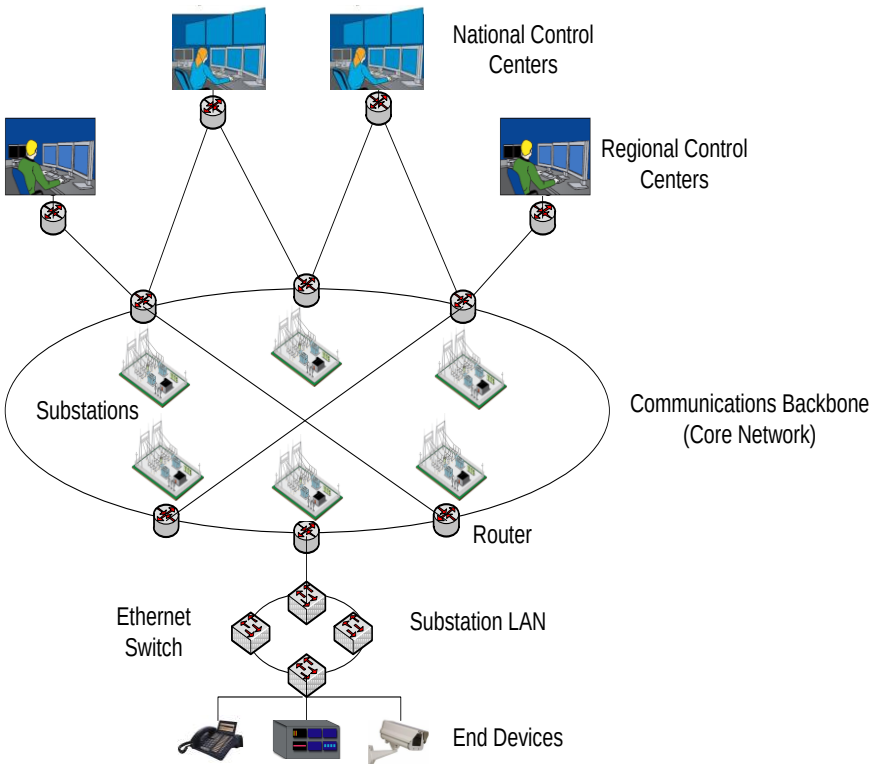


Figure 17: High Level architecture of the IP network for operational purposes

4.1 Scope and organization of responsibilities

Electric utilities have different missions, size, cover different geographical areas and have different resources and capabilities therefore there are various approaches for managing a utility's operational and corporate networks.

The corporate network is usually managed by the IT or telecommunications department. In most cases IT is separate from telecommunications but there are utilities that have one common department for all IT and communications systems.

The operational network is being used by telecontrol (SCADA) or protection and control departments and typically is being managed by an internal telecommunications department.

Nevertheless driven by both economical and organizational factors some utilities tend to outsource the management of corporate network and less frequently the management of the operational network. As a consequence the existing knowledge regarding the network and the technology disappears. In some utilities only part of the network and systems or only selected communication services are outsourced to external companies. Currently the trends of outsourcing operational communications services are being analyzed and several utilities are revisiting this strategy.

Additional information about organizational and management issues related to operational telecommunications services in the electric utilities can be found in CIGRE TB461, April 2011 .

4.1.1 Dealing with responsibility for operational networks

Within the utilities we find different ways of designing and managing the operational network. The design and management is influenced by

- The OPEX and TCO required
- The available skills and knowledge base
- The required service availability and resulting risk of outages.

From the organizational point of view the easiest situation is:

- when the whole operational network is managed by the utility itself, or
- when the whole operational network is completely outsourced to one or more third-party companies

Even if the whole operational network is outsourced the utility still requires a minimum knowledge of the underlying communication architecture in order to manage the Service Level Agreement with the outsourcing company and jointly coordinate migration plans or future additions of devices and services.

However in real life different hybrid or mixed-responsibility approaches can be adopted in order to optimize available resources and fulfill particular requirements and constraints:

- Only particular services or applications are procured or managed by third-party (e.g. mobile communications for field workforce or remote access to substation data retrieval, or video surveillance, etc.)
- Only services to particular sites or geographical zones are procured or managed by third-party (wireless or leased fiber links in certain areas, etc.)
- Only particular infrastructure layers or parts of the network are procured or managed by third-party (e.g. backbone transport services, etc.)

The situation can be even more complex when we consider that own personnel of the utility in charge of design and management of operational network can belong to different departments within the utility. Usually the utility personnel that designs and manages the operational network belong to:

- Telecommunications department
- Telecontrol- or protection and control department

In utilities that have more than one internal department dealing with management of operational network or operational services the split of responsibilities usually follows the example below:

- Telecommunications department responsible for backbone network and communications between substations and between substations and control centers
- Telecontrol- or protection and control department responsible for LAN network and communications within the substation

There is no best approach as it all depends on multiple factors already stated above such as available resources, knowledge, historical reasons, etc.

The fact that management of operational network in the utility is often split between telecommunications and telecontrol departments has historical reasons. Fifteen or twenty years back there were no data communications inside substations as all signals were hardwired between IEDs and between IEDs and conventional RTUs with the use of copper cables. Basically all the equipment inside the substation was considered part of the protection and control system. Even with the posterior introduction of standards based serial communications and more recently with Ethernet or IP based communications this process still remains globally unchanged in many utilities. Today the Ethernet switch that interconnects protection relays inside substation is facilitating transmission of IEC 61850 GOOSE messages carrying for example a permissive trip signal to open the high voltage circuit breaker. This Ethernet switch is in fact replacing a pair of copper cables used in the past for the same purpose and it is a key element for ensuring proper functioning of the system that is protecting the high voltage assets and facilitating a reliable supply of energy.

This explains why still many utilities put the frontier between what they consider belongs to protection and control systems and what belongs to telecommunications systems.

The recent interest in Smart Grid and trends to higher integration of electrical grid and information technology is putting pressure for such utility organization and systems where all communication enabled devices are monitored and integrated into a single information backbone. The goal of Smart Grid is to have all data from the electrical grid visible in a common bidirectional communications network and thus increase system reliability and efficiency while maintaining a certain level of security.

4.1.2 Organizational impact and human factor

There can exist significant differences in terms of mentality and technical skills between telecommunications engineers and protection and control engineers. The difference in mentality is based on the fact that protection engineering relates to personal and asset security and therefore requires a certain level of conservatism ensuring the continous use of well-defined fundamentals that had been practiced intact for dozens of years. The IT and Telecommunications technology is changing in a much faster pace than the protection and control technology. The product lifecycle is longer in protective relaying than in the IT/Telecom business. The difference in technical skills is obvious as each group is expert in its own domain.

Apart from the differences in skillsets and in mentality there can also exist organizational issues caused by certain level of duplicity, lack of established procedures or weak communication between employees of the same utility that work in different departments.

The major organizational challenges many utilities face today in regards to communications technologies and its impact on operational network are listed below:

- Difficulty being up to date with latest developments in IT and telecommunications technology
- Lack of multidisciplinary experts with combined knowledge of networking and protection and control (eg. IEC 61850 Standard, substations primary and secondary equipment, etc.)
- Weak internal communications between own employees and lack of well-established scope of responsibilities and procedures

New network deployment plans and implementation of new communications services can potentially be a motivation for the utility to create new multidisciplinary group or create a matricidal company organization with employees from multiple departments working together on a design and management of IP communications network and functionally reporting to the same project manager. It is recommended to identify such opportunities in an early stage and anticipate it. Knowledge and management of the network could be clustered within the company inside a so called “expert group” not necessarily within the same department.

4.1.3 Technical skills of network designers

Network design requires two conditions to achieve the network deployment objectives:

- theoretical knowledge of technology
- practical experience in the field

In addition to the IP knowledge there are new areas with their own specialties including:

- Data transport technology
- Cyber Security
- Remote access
- Traffic engineering
- Substation automation

The practical experience might be more important than theoretical knowledge, because it allows designers to have a general view of the network design and it allows also to avoid the deployment “traps”.

It is highly recommended that network designers work in parallel in the testing lab in order to cross check all the technical issues that may arise during the integration of equipment from different vendors. Before the network design is finalized pre-testing shall be run in the lab to mitigate the risks of interoperability issues, protocol incompatibility, etc.

4.2 Requirements and constraints for the communications network

The network design is one of the key elements in the communication infrastructure lifecycle. All existing communications networks can be divided into two categories:

- Networks that had been properly designed with predictable parameters
- Networks that had experienced spontaneous growth from several pieces without methodical design approach

Predictability is the most important challenge for the design engineers; it may take significant time and efforts at the preparation and design stages.

The IP communications network design shall satisfy the high level system requirements and the detailed design requirements. It is not possible to define a suitable network design without understanding all the functional and non-functional requirements of the system. The network design could be dictated by some of the application requirements such as the minimum latency or bandwidth needed for video streaming from surveillance cameras or deterministic channels for teleprotection devices. Establishing design principles will assist in resolving conflicting requirements (e.g. safety and reliability could have higher priority than cost of the equipment).

A communications network for utility operational purposes shall be designed taking into account several criteria and requirements, of which the most important are listed below:

- Grid topology and physical locations of substations
- Using the existing communications infrastructure
- Design of a scalable and flexible network
- Logical data flows and traffic patterns
- Performance requirements
- Proper IP addressing plan
- Support for legacy non-IP applications
- Interoperability and use of open standards
- Redundancy and resiliency
- Reliability and availability
- Time synchronization and accuracy
- Requirements for wireless technology
- Network management and monitoring
- Environmental and EMI immunity requirements
- Mechanical and physical media requirements
- Physical security and cyber security
- Maintainability, upgradability and lifecycle management

- Cost effective design and total cost of ownership

4.2.1 Grid topology and physical locations of substations

It is required that the communications network design takes into account the topology of the electrical grid and the geographical locations of substations as well as locations of different dispatching centers. Usually the fiber network is built over OPGW cables so that the basic telecommunication infrastructure reflects the power grid topology. This way the power grid deployment acts as a main constraint and driving force for physical architecture of the communications network.

It is recommended to create the map of the grid with all assets that need to be connected and to define logical data flows and communications services between the network nodes and try to fit these services into a telecommunication infrastructure. An example of fitting communication service to the electrical grid topology is to deploy telecommunications links for protection in parallel with the high voltage line, this can be implemented over OPGW or over a PLC link.

Power grids tend to be built with certain level of redundancy and the telecommunication design shall take advantage of this. On higher voltage levels the network topology redundancy is more explicit and part of the design could coincide with the power gird topology, whereas it is often not the case on distribution level where a more exhaustive logical design would be needed. Also on the distribution level, the utility may not have any own infrastructure and must rely on third party services

In case of substations located in remote areas the availability of communications infrastructure will condition the type of physical communications media and transport technology. In some regions it may not be feasible to deploy dedicated fiber optic links to substations and the only alternative may be the use of power line carrier or wireless technology, either cellular, microwave or satellite. In this case the multipoint character of wireless technology and its limitations should be considered when planning the services. For example if cellular technology is to be employed for point to point services a tunneling scheme could be employed.

4.2.2 Using the Existing Communications Infrastructure

The approach and constraints for implementing IP communications services will be significantly different for the utility companies that already have an existing communications infrastructure and for the companies that lack this infrastructure. In case there is an existing communications network based on non-IP technology there may be a strong argumentation to use this infrastructure and build on top of it IP networks or create a hybrid solution mixing native IP and non-IP networks. For utilities that don't have existing communications infrastructure the situation is different as IP networks can be built from the scratch using the latest technology based natively on Ethernet layer 2, IP, MPLS, VPLS, PBB, etc. Building a new communications infrastructure may be characterized by very high initial investment costs, especially in rural or low density population areas. In some cases the only alternative for physical transport layer may be the use own OPGW if available or own high voltage lines for Power Line Carrier (PLC). Also satellite links or long range microwave radio links can be considered.

Based on the results of survey from chapter 2, there is a significant number of companies that think Ethernet over SDH is the right approach for IP services. This is also dictated by the fact the utilities in many countries have made big investments in building own fiber optic network using SDH technology. For example in most of the European countries the TSOs have SDH networks spanning well their HV substations grid. It is obvious that there may be a strong requirement to capitalize on the existing infrastructure. Utilities are now the biggest user of SDH/PDH technologies. These technologies are being replaced in most cases by IP and Ethernet. Utilities have to take into account that the PDH/SDH market is mature. However, the technology is still promoted by many of the telecom manufacturers, indicating a prolonged life on the market. In addition, SDH/PDH is still among the most suitable solutions for critical applications such as differential protection.

4.2.3 Design of a scalable and flexible network

A scalable network can grow with new demands:

- Horizontally: accommodate increasing number of applications
- Vertically: accommodate increasing number of end devices (number of IP addresses)

A flexible network permits provision of new services without drastic modifications or redesign in its core architecture and while maintaining availability requirements. The network flexibility depends on the capability of the device, protocol or the technology to be adapted to different topologies: star, ring or mesh.

The network designer shall anticipate the following events:

- Addition of new substations, devices or users
- Addition of new applications
- Additional demand for bandwidth
- Appropriate location of edge nodes

Network scalability can be achieved by using a proper hierarchical network architecture providing enough spare capacity in the nodes in terms of bandwidth or spare ports and spare slots in switches, routers or multiplexers to allow for new connections or new communication modules to be added quickly.

Another way to achieve scalability is to use WDM or DWDM technologies in existing optical fibers. By using different wavelengths, it is possible to add multiple connections with high bandwidth. A few applications are adding (passive) connections or realize redundant connections.

It is necessary to create the list of all planned applications that will be utilizing the IP communications network. A good practice is to provide a list of potential future applications that are considered for the future. For example a utility may not have decided yet to deploy video surveillance cameras at all sites or to use phasor data measurement for wide area monitoring but it is important to make an assumption such services may be needed in the future and make necessary provision at the network design stage. The designers shall know company's mid-long term plans or considerations for example to roll-out next generation services or Smart Grid applications such as smart metering, demand optimization, large integration of sensors in the grid or renewable energy resources etc. that may put extra requirements for the communication network. All the possible applications shall be listed in the order of their criticality and description shall be given if logical or physical isolation is required between them.

Native Ethernet/IP networks still have scalability limitations, e.g. the required address space, address table sizes and convergence time in large networks. Therefore, utilities may consider using IPv6 to overcome some of these limitations.

4.2.4 Logical data flows and traffic patterns

An essential task of operational network design is to predict data flows and traffic patterns, and then plan the partitioning or segregation of traffic depending on the type of traffic.

Logical data flows are determined by the application and different devices and system exchanging information. For example SCADA applications can be conditioned by several regional dispatching centers acquiring data only from a limited number of substations or phasor measurement applications can be designed in a way that there are various data concentrators situated in strategic locations receiving streams of data from a determined number of sites and concentrating these data to fewer streams that are then forwarded up to regional or national dispatching centers. Once the data exchanges are known, traffic patterns emerge, for example voice over IP is characterized by similar throughput in both directions while SCADA or video streaming is utilizing much more link bandwidth in one direction only. Special care need to be taken for part-time or maintenance applications such as internet access or access to corporate resources from substations that can be provided for field crews.

The description of logical data flows and traffic patterns goes down to the level of knowing how many devices or IEDs are in each substation, what protocol these devices are using to communicate with other nodes/systems in the network and what is the typical and maximum bandwidth consumed by each device or each communication protocol.

4.2.5 Performance requirements

Each type of traffic or application to be carried by the IP network shall have well defined performance requirements or Quality of Service (QoS). QoS is the capability of a network to provide better service to selected network traffic over various technologies. Primary goals of QoS include bandwidth reservation, controlled jitter and latency and improved loss characteristics. Advanced QoS mechanisms permit queing, scheduling and traffic shaping.The list below shows an example of QoS requirements:

- Minimum throughput
- Maximum latency
- Maximum jitter
- Maximum packet loss ratio

After gathering the information of all potential IP applications and their traffic patterns the network designer shall define what are the performance requirements of each application/network device or each network node. This task may involve discussions with experts in particular areas for example control engineers that will define and design specific applications.

All these shall be carefully specified per application as it has impact on the network architecture and design. The designer must respect the required performance parameters in order to ensure required quality of service and proper functioning of applications.

More details on performance requirements are described in chapter 4.4 and can be also found in CIGRE TB WG D2.23.

4.2.6 Proper IP addressing plan

One of the main concerns when establishing an IP network is dimensioning the addressing space so that there are enough addresses for all hosts in the network, it fits into the company structure, is scalable and there is an optimal exploitation of the address space. The IP addressing plan is the fundamental key of IP network design success; it shall support the flexibility and growth of the network. Specifically if the responsibility for WAN and LAN infrastructure is distributed (see section 4.2.2), the coordination for the IP addressing plans is very important. It is essential to do the dimensioning of the number of elements to address and choose if IPv4 is suitable or if IPv6 is required.

Dealing with the extension of existing networks might require work-around solutions. This is discussed more thoroughly in chapter 0.

Nowadays IPv4 is the dominant internet protocol and IPv6 deployment is still limited, however it may be required that the IP backbone network design has IPv6 compatibility for the future.

4.2.7 Support for legacy non-IP applications

It shall be specified in the project requirements how many and what kind of legacy non-IP applications will need to be connected. For example in case of the serial devices all details about types and speed of interfaces such as RS232, RS485, RS422 will be used. What will be the serial protocols and what is their nature, e.g. synchronous vs. asynchronous etc. More about legacy serial to IP conversion can be found in chapter 3.5 of this brochure.

All applications and equipment with non-IP technologies such as PDH, SDH, X.25, G.703, C37.94 interfaces, V.35 modems, etc. need to be identified and technical details need to be gathered.

Based on the results of the survey from chapter 2 there is a significant group of users that will prefer to transport these applications using separate network because adapting them to IP may require specialized and costly equipment.

4.2.8 Interoperability and use of open standards

It is of vital importance that the network design is based on open standards to guarantee interoperability between multiple vendors. Depending on the utility experience and the region a basic set of standards to be used as a guideline shall be prepared. For example for the telecommunications equipment and transport technologies utilities may want to specify that ITU-T and IEEE standards will be used. For the communication equipment located in the substation environment that will provide direct access to device the IEC and IEEE standards and CIGRE reports shall be used. Open standards such as IEEE 802 series, IEC 60870 and IEC 61850 helps avoiding the situation where the utility is locked into one vendor solution.

4.2.9 Redundancy and resilience

In power utility applications it is common to use N+1 criteria for redundancy. It means that the system shall be tolerant to a single point of failure. For the network and communication equipment this criteria is applied selectively. Redundancy can be subdivided into hardware redundancy and network redundancy.

Hardware redundancy is a duplication of selected devices or selected components is these devices. It can be realized at the module (component) level and at the device level. Typical example for module level redundancy is power supply redundancy. An example of equipment level redundancy is router redundancy with VRRP (Virtual Router Redundancy Protocol).

Network redundancy is the ability of the network architecture to be resilient to failures. It is realized by redundancy protocols. Redundancy protocols implement mechanisms for fast recovery upon failures, avoiding loops and ensuring efficient and optimal data transfer through shortest communications paths.

Network redundancy protocols or network protection schemes ensure resilience to failures as redundant communications paths are available. However redundancy protocols are characterized by failover or recovery time which is the period when the data communication is not available as the switchover to the alternative path is being performed after failure link or device has been detected.

Each utility application is characterized by its availability and maximum tolerated outage or downtime. For critical substation automation applications the requirements are extreme in terms of latency and packet loss. Tripping information shall have a latency less than 4-6 milliseconds and no packet loss is accepted. Protection and control engineers are still reluctant to migrate such applications to IP or Ethernet technology. Availability requirements have direct impact on the redundancy protocol that should be used.

4.2.10 Reliability and availability

It may be required to know how often a component of the communication network will fail and how often a repair team must be sent to replace failed parts. Reliability and availability requirements are defined by desired MTTF and MTTR.

Manufacturers of electronics products use MTBF (Mean Time Between Failure) estimates as a measure of reliability and longevity assuming that systematic (or type-) errors have been eliminated before putting the devices in operation. MTBF is often requested by purchasers of equipment and is used to compare equipment from different vendors. It has to be noted that MTBF can be determined different ways with correspondingly different results.

There are three main methods for computing MTBF:

- Calculated or Predicted
- Assessment or Demonstrated
- Observed

Using the calculated method the MTBF can be predicted based on statistical failure rates of electronic components. The calculated method is most useful at the design stage when comparing design iterations. There are two popular methods:

- MIL-HDBK-217F developed by United States Department of Defense
- BELLCORE/Telcordia (used by Telecom industry)

MIL-217F is two to three times more pessimistic (i.e. 2-than Bellcore/Telecordia). Environmental conditions greatly matter when using either of the calculated methods and will produce dramatically different results. Often vendors publish calculated MTBF values under “Ground Benign” environmental conditions at 25°C. This is essentially an air conditioned office. Compared to “Naval Sheltered” at 25°C there is two to four times difference in results.

MTTR (Mean Time to Repair) is the average time required to repair a system. There are many factors influencing MTTR such as travel time to site for repair, detection time of failure, and replacement time of device. The first is specific to a given installation but the latter two are related to the device in question.

Availability = MTBF / (MTBF + MTTR) * 100%

Availability requirements may include specific rules for backup and recovery plans as well as for provision of power autonomy such as batteries, UPS systems (Uninterruptable Power Supplies) or diesel generators).

Definitions of availability models and calculation methods for communication networks can be found in:

- IEC 62439-1 Clause 7

- IEC 60870-4 Performance Requirements, section 3.3

4.2.11 Time synchronization and accuracy

Precise time synchronization is required for IP communication devices for example in order to do event correlation and have common time reference.

Substation applications and IEDs also have time synchronization needs. For most SCADA applications the requirement is 1 millisecond accuracy in order to have chronological sequence of events with millisecond granularity. Until relatively recently the time synchronization of electronic devices in power systems has been realized via dedicated wiring used for distribution of GPS, IRIG-B or 1PPS signals. However with the proliferation of Ethernet NTP or SNTP started to be widely used in substations. Typical NTP/SNTP implementations in normal network conditions provide the accuracy of 2-3 milliseconds; even a tuned network running NTP can achieve accuracy only in the millisecond range.

There are specific applications like IEC 61850-9-2 Process Bus or Synchrophasors that require 1 micro second accuracy of the time signal. For these applications IEEE 1588 time synchronization protocol should be considered. It provides the same accuracy as IRIG-B or PPS but has the advantage of using IP network and elimination of dedicated cabling.

While designing the utility communications network high precision time synchronization IP based protocols shall be considered as they can provide system wide synchronization method and bring potential cost savings by elimination of GPS receivers from many substations. The constraint for IEEE 1588 network is that in order to preserve the micro second accuracy all the network devices shall support this standard.

Another alternative to ensure high accuracy of time synchronization is the use of Synchronous Ethernet (SynchE).

To avoid the necessity for high precision time protocols over the backbone, a hybrid approach may also be used. Major substations may still be equipped with time sources (e.g. GPS based) and distribute the synchronization signal on LAN level through a time protocol.

4.2.12 Requirements for wireless technology

The use of wireless technology may be required for several reasons, for example due to geographical constraints such as long distances to sites, lack of wired infrastructure or where it is economically not feasible to deploy fiber connections. On the other hand utility may want to use wireless technology as backup connection to an existing communication links. Therefore wireless communications shall permit transmission of IP traffic.

There are multiple aspects of wireless technology for consideration. Regulatory issues for private deployments can limit the application because the wireless spectrum availability is specific to countries or geographic areas. Technical aspects of wireless technology that will condition the network design are:

- Throughput
- Range
- Latency and jitter
- Security
- QoS (Prioritization)
- Uplink biasing

4.2.13 Management and monitoring of network equipment

It is a common requirement to have the ability to perform remote online network management and monitoring. Typical tasks accomplished by management and monitoring systems are:

- Service and devices monitoring including alarms and fault indications
- Correlation of events
- Performance monitoring
- Device firmware and configuration file management
- Network topology automatic discovery and maintenance

SNMP is a commonly used protocol and has multiple versions. Nowadays most of the modern network equipment implements SNMP versions 2, 2c and 3. It is important to specify a minimum requirement in terms of SNMP version as well as a minimum subset of standard MIBs supported by the devices in the network. Network management systems may have other features such as syslog retrieval, etc. There are big differences in functionality, scalability and price of network management systems (NMS systems). The price of small NMS software capable of monitoring up to few hundred devices may vary between few hundred up to few dozen of thousand dollars. An enterprise level NMS system that is scalable and capable of monitoring thousands of devices, has large third party support and has large possibilities of integration with other corporate information systems may cost up to several hundred thousands of dollars. When migrating to IP networks a company may want to either use a dedicated NMS for devices in the operational network or may want to use a centralized NMS system to manage networks.

For configuration of network equipment the NETCONF (RFC 4741) protocol can be considered. NETCONF is a relatively new standard and has more powerful features than SNMP, which for many years has been successfully used for monitoring of devices but rarely for their configuration. NETCONF provides mechanisms to install, manipulate, and delete the configuration of network devices. It is based on XML language and also provides mechanism for support subscribing and receiving asynchronous event notifications.

For topology and device discovery in layer 2 networks the LLDP (Link Layer Discovery Protocol) can be used.

4.2.14 Environmental and EMI immunity requirements

High voltage substations are characterized by presence of different types of electromagnetic phenomena. These phenomena can be continuous or transient and will heavily impact functioning of electronic devices such as communication network equipment. In short, communication devices for utility applications shall have extremely robust hardware design to properly operate under the influence of interferences and harsh conditions. Unfortunately, when these phenomena occur, communication is required most.

To name just a few of these phenomena we can mention inductive load switching, opening disconnectors, lightning strikes, electrostatic discharges from human contact, radio frequency interference due to personnel using portable radio handsets, ground potential rise resulting from high current fault conditions within the substation, etc.

Communication devices are often installed in enclosures or containers located few meters from high voltage apparatus. A power transformer or a circuit breaker may generate very heavy vibrations and electromagnetic field. It is a good practice to specify that all networking equipment shall comply with EMC specification as per IEC 61850-3 or IEEE 1613 standards. IEEE 1613 goes one step further than IEC 61850-3 by defining “Class 2” operation which requires that, during the application of the type tests, the communication device must experiment:

- No communications errors
- No communications delays
- No communication interruptions

Substations may be located in the desert, in areas with presence of corrosive substances, underground or even in maritime environments on offshore platforms. Therefore it is recommended to specify strict requirements for immunity to high levels of dust, chemical substances, pollution, salt, humidity and abrupt temperature changes. For immunity to chemical or corrosive substances some vendors offer an option of so called “conformal coating” which is a special protective layer that will be covering all electronic circuit boards and is applied to the whole device during the manufacturing process. Devices that are going to operate in maritime environment shall have special robust design preventing corrosion caused by salt, high humidity and bird guano, if mounted outdoor.

4.2.15 Mechanical and physical media requirements

There might be special hardware and mechanical requirements for network devices for utility applications. Apart from the rugged hardware design immune to unfriendly environment it may be required that devices cannot have any rotating or mechanical moving parts such as fans, CD-ROMs, rotating hard disks, etc. Another requirement may be for a specific form factor such as DIN rail mounted devices, 19 inch rack mounted devices or small form factor in case there is limited room. This may happen in wind platforms, underground substations or pole mounted installations that are characterized by very limited space. If the communication network is going to span different locations inside the substation, such as remote containers with RTUs, IOs (input/output module) and signal acquisition modules in the switchyard then fiber optic communications port will be required to protect communications against interferences. Some end devices like IP phones or IP cameras can only be powered via Ethernet ports, which is called PoE (Power over Ethernet) standard. PoE is specified in IEEE 802.3at and IEEE 802.3af. The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power to each device, the updated IEEE 802.3at-2009, also known as PoE+ or PoE plus provides up to 30 W of DC power to each Ethernet port. If there is a need to connect PoE devices in the substation or in the control room the designer shall make sure the Ethernet switches chosen comply with the required PoE standard. Power budget calculations shall be performed and in some cases Ethernet switches may require external power supplies to ensure the necessary power is provided for all PoE equipment.

4.2.16 Physical security and cyber security

The introduction and implementation of physical and cyber security measures and tools at the utilities, will also place important requirements on the communication architecture that needs to be addressed during the design and implementation phase of the IP network. Physical security measures could for instance introduce video surveillance at the substations that would impose requirements for more bandwidth, the use of quality of service etc. on the network infrastructure. Cyber security requirements will also greatly influence the design of the communication infrastructure. This can include segmentation of the network into security zones, use of VPN technologies, use of security tools like firewalls, use of encryption (IPSec), use of network access control systems (IEEE 802.1X), best security practices of configuring the network equipment, ensuring all company’s portable devices have encrypted hard disks, etc.

A detailed description of physical and cyber security issues is out of the scope of this document and has been described in other Cigre technical brochures, nevertheless selected issues are mentioned in chapter 5.

4.2.17 Maintainability, upgradability and lifecycle management

The network lifecycle milestones shall be known before proposing the design; this can help the designer to propose a future-proof network architecture. The key aspects are to avoid obsolescence of technology and obsolescence of equipment. It is also important to know the trends and potential evolution of applications that will use the network.

Future firmware and hardware upgrades must be considered. The devices shall permit easy way of upgrading the firmware or configuration settings. Configuration software with feature of bulk download or upload of firmware or configuration files to multiple devices simultaneously shall be considered.

Modular design of devices and use of SFP ports shall be considered. Hardware upgrade process is easier with devices that offer modular design. Until now scalability was mainly accommodated in the backbone devices, however nowadays it is not limited only to SDH equipment or big core IP routers. Today also smaller routers and layer 2 Ethernet switches are manufactured with field-replaceable and even hot-swappable hardware modules. Replacement or addition of new communication card or power supply takes in such devices only few seconds and reduces outages and maintenance costs. Future-proofing of the network may be improved by selecting equipment with built-in support for protocols and features that are seen as future trends for example IEEE 1588 time synchronization that permits much higher accuracy than NTP protocol.

4.2.18 Cost effective design and total cost of ownership

The network cost is conditioned by the project available budget and it is a fundamental aspect that directly impacts the choice of the network design. Economical calculations have to be done for the items listed below:

- Total equipment and infrastructure costs
- Engineering and deployment costs derived from the complexity of the network design and configuration
- Support, maintenance and replacement costs

Support and maintenance costs are typically not easy to forecast. This is not only due to technical concerns but is also related to the utility's strategy and policy to either have an internal team for support and maintenance or to have this task outsourced to an external contractor.

Appropriate number of equipment and service suppliers is important for the cost of ownership. Having too many suppliers means that a utility needs to maintain spare parts for several types of devices as well as may have to pay software maintenance fees for several applications. On the other hands having too few suppliers may lock the company to one-vendor solution and could lead to a forced acceptance of excessive prices for equipment and services. Interoperability and, if possible also interchangeability, of standard types of devices is a recommended requirement.

Rugged communication equipment specifically designed for electrical substation environment has normally higher cost than IT grade devices used in office or data center environments. The expected equipment life time of telecom/IT equipment in utility environment is much higher than in public telecom environment. A higher cost for utility grade equipment may therefore be acceptable. However given the nature of the utility applications it shall be assumed that communication devices in substations no matter if in direct proximity to high voltage apparatus or inside control building will be used for mission critical applications and therefore the hardware shall have extremely robust design.

One of the cost key aspects in an electric utility network is how to establish the long distance connection. Long distance connections can be especially costly when the existing infrastructure and physical media choices are limited.

Redundancy and high availability have direct influence of solution cost. Some applications or network layers may be accepted with lack of complete device or component duplication, this would allow cost reduction of the solution.

If the utility decide to outsource provision of Wide Area Networks (WAN) or service it shall carefully review the service contract as the WAN network service and maintenance fees can easily become the major portion of total cost of ownership of the communications infrastructure.

4.3 Guidelines and Engineering Process for Designing an IP Communications Network

The network design shall satisfy high level requirements and shall ensure understandable, reliable, efficient and cost effective architecture. Establishing design principals will assist in resolving conflicting requirements (e.g. redundancy and reliability could have higher priority than cost).

The communications network design shall follow an engineering process with well-defined tasks. Following a methodical process the designer increases chances to end up with appropriate network design. Depending on the company's policy or designer's experience the engineering process can be defined as a project checklist, a guideline document or a formal flowchart.

4.3.1 Engineering process

The engineering process of utility communications network goes through several steps. The figure below shows a generic approach to utility network design. With small modifications it can be applied both to substation LAN network and also to the WAN network

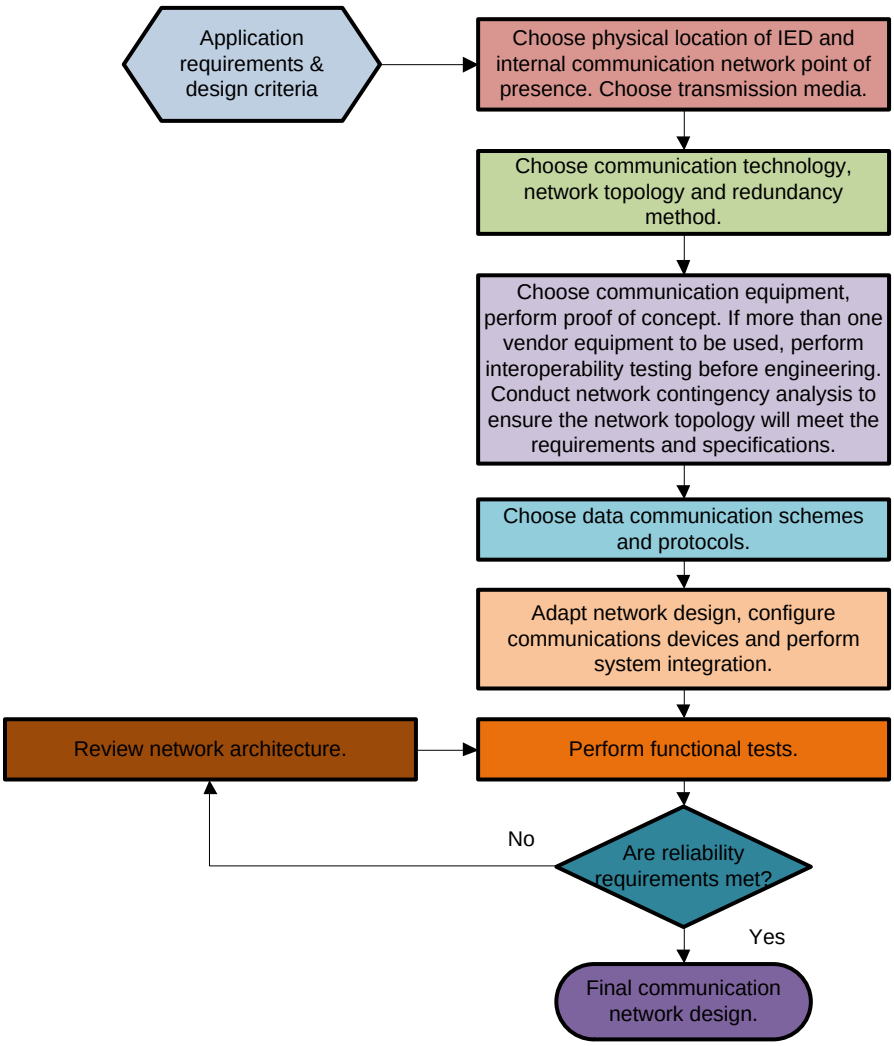


Figure 18: Generic engineering process for designing utility communications network

The following list describes the recommended checklist during the IP network engineering process:

1) Determine the list of applications
2) Determine performance parameters for all applications
3) Identify network constraints:
    - Identify solutions cost constraints
    - Identify scope of responsibility for planning, operation, support and maintenance
4) Determine if support for legacy technologies is required
5) Based on the previous constraints, fix the target values for performance parameters
6) Propose high level network design:
    - Define IP addressing plan
    - Select new or modify existing WAN technology

- Select new or modify existing type of equipment in each part of the network

7) Compare high level design with network constraints. If the constraints are not met then review the high level design

8) Propose detailed network design that covers all technical details

9) Perform technology training and educational sessions for the staff involved in deployment, operations and maintenance of the new solution

10) Realize proof of concept and perform lab tests to check device and vendor interoperability, communications protocols, etc.

11) Establish progressive deployment planning with rollback procedures

12) Discuss the network design with the people or company who will be in charge of the network deployment

13) Prepare the final bill of material with detailed order codes of all the communication equipment

14) Start network deployment and/or migration

4.3.2 Technical Aspects to Consider

Once the application requirements and constraints are known the designer shall go through a list of technical aspects of the IP technology to determine the detailed technical requirements. The following list contains possible discussion points and existing technologies that will help to define detailed technical requirements of the utility IP network:

High level design:

- IP Addressing plan – Type of IP addresses, subnetting, summarization
- WAN technology – SDH, Ethernet, IP routing, MPLS, PBB
- Network topology – Star, redundant star, ring, multiple rings, mesh
- Routing protocols – OSPF, RIP, BGP, etc.

Availability and performance:

- Power autonomy – use of batteries or UPS (Uninterruptable Power Supplies)
- Dual-redundant power supplies – Higher reliability with power-load balancing Fiber optic media – Immunity to EMI resulting in reliable communications in the backbone
- Gigabit ports - Optimum throughput for a high-speed network backbone
- Link aggregation - IEEE 802.3ad provides the ability to aggregate several Ethernet ports into one logical link (port trunk) with higher bandwidth, it is an inexpensive way to set up a high speed backbone to improve network flexibility
- Port rate limiting – Limiting unicast and multicast traffic. Helps managing network bandwidth and providing edge security for denial of service (DoS) attacks
- Multicast layer 2 filtering – static filtering tables or dynamic GMRP/MMRP protocols to optimize layer 2 multicast like IEC 61850 GOOSE or Samples Values inside substation LAN
- Multicast layer 3 filtering - IGMP Snooping allows creation of multicast filters and limiting IP multicast traffic streams (i.e. video surveillance) to specific hosts on the network
- Layer 2 redundancy protocols - RSTP/MSTP (IEEE 802.1Q-2005) provide loop elimination in redundant topology and automatic failover
- Layer 2 bumpless (sometimes referred to as "high availability-") redundancy protocols - PRP/HSR (IEC 62439) provide zero-time failover and duplication of traffic simultaneously over redundant path

- Layer 3 redundancy protocols – VRRP provides automatic and transparent failover for redundant routers
- Class of Service and traffic prioritization - QoS/CoS (IEEE 802.1p) provides better performance and lower latency for critical applications
- Monitoring and management – SNMPv2c/SNMPv3 allows monitoring and diagnostic of port interfaces, CPU utilization, alarms, events, and other aspect of networking devices

Security:

- Traffic Segregation - VLANs (IEEE 802.1Q) allows segregation and securing network traffic.
- Firewall and IDS (Intrusion Detection System) – block unwanted traffic from entering the network, detect intrusions and abnormal situations in the network such as attempts of cyber attacks
- Secure data tunneling – VPN, L2TP, IPSec, GRE protocols provide secure data tunneling to remote locations over unsecure communications channels
- Port based network access control – IEEE 802.1X allows lock down ports to unauthorized users
- Authentication – Radius or TACACS provide verification of users credentials, authentication and granting access to network
- Access Manager – specialized centralized solution to authenticate users and provide security audit trials
- Encryption – AES, DES, 3DES, RC4, etc. data encryption
- Password management – multi level user passwords, role-based security, established policies for password length, strength and expiration, central repositories of passwords, etc.

4.3.3 Defining the IP Addressing Scheme

A proper and consistent IP addressing plan is essential for efficient network design and optimized performance of applications. Careful allocation of IP address blocks is useful for creating routing tables of manageable sizes by taking cognizance of the fact that the excessive size of routing tables increases processing latency of IP routers.

The main steps that a network designer has to go through when defining the IP addressing plan are:

- Decide if public or private addresses are to be used
- Decide if IPv4 or IPv6 protocol addressing is to be used2
- Decide the class of IP addresses and type of subnetting

Subnetting is a technique of dividing a block of IP addresses into smaller segments (or chunks) called subnets. Subnetting permits logical division of the network based on organizational reasons, preservation of IP address space, enhancing cyber security and controlling of network traffic to preserve bandwidth.

In order to decide on the type of subnetting the following steps must be followed:

- Determine the entire IP network size
- Determine the criteria for subnetting, eg. separate subnets per geographical location vs. separate subnets per service or application etc.
- Determine the desired number of network segments
- Determine the maximum number of hosts in the largest subnet

The following formulas can be used to determine the address class and subnet for given requirements:

2 IPv6 protocol is not commonly found in substation devices at this stage.

(1) *Required number of hosts in the subnet* $=< 2^H - 2$, *where H is the number of host bits in the network mask*

(2) *Required number of subnets in the network* $=< 2^S$, *where S is the number of subnets bits in the network mask*

(3) *S + H = < maximum number of host bits for a given address class*

Practical example of subnetting

As an example we consider a utility with the following requirements:

- use private class C subnets
- have a minimum of 5 subnets
- have subnets with at least 1000 hosts

Using formula (1) we will calculate the minimum number of host bits in the network mask that will allow a network segment of at least 1000 network hosts:

$1000 =< 2^H - 2$ *according to formula (1)*

$H = 10$

$1000 =< 2^{10} - 2$

Using formula (2) we will calculate the minimum number of subnet bits in the network mask that will allow a network of a minimum 5 different subnets:

$5 =< 2^S$ *according to formula (2)*

$S = 3$

$5 =< 2^3$

Private C class allows IP address range of 192.168.0.0 – 192.168.255.255, the number of host bits is 16. Finally the condition from formula (3) has to be met:

S + H = < maximum number of host bits for given address class

3 + 10 = < 16

In our example formula (3) and all other conditions are met. As a result the utility could use one of the following private IP class C addressing spaces:

192.168.0.0/19	subnet 255.255.224.0	(8 subnets with maximum 8190 hosts each)
192.168.0.0/20	subnet 255.255.240.0	(16 subnets with maximum 4094 hosts each)
192.168.0.0/21	subnet 255.255.248.0	(32 subnets with maximum 2046 hosts each)
192.168.0.0/22	subnet 255.255.252.0	(64 subnets with maximum 1022 hosts each)

The example of IP addressing in one subnet for the address space 192.168.0.0/22 is shown below:

192.168.128.0 (11000000.10101000.10000000.00000000) Class C private subnet address
192.168.129.0 (11000000.10101000.10000001.00000000) Class C private subnet address
192.168.130.0 (11000000.10101000.10000010.00000000) Class C private subnet address
192.168.131.0 (11000000.10101000.10000011.00000000) Class C private subnet address
---
192.168.128.0 (11000000.10101000.10000000.00000000) Supernetted Subnet address

255.255.252.0 (11111111.11111111.11111100.00000000) Subnet Mask
192.168.131.255 (11000000.10101000.10000011.11111111) Broadcast address

If in the above example the requirement would be to have at least 100 different subnets with at least 1000 host then class A would have to be used instead of class C addresses.

Variable Length Subnet Masking (VLMS)

In real life the IP network may have subnetworks with different numbers of hosts. The subnetting example shown above is based on single-level subnetting where the address space is equally divided to subnets based on the size of the greatest number of hosts. This may be inefficient in case many subnets have significantly fewer hosts than the biggest segment. The solution to this problem is Variable Length Subnet Masking (VLSM) which is a technique that allows the dividing of the IP address space into subnets of different sizes. VLSM can be seen as multi-level splitting of the same major class of addresses, eg. iterative subnetting of higher level subnets. VLSM is more complex than single-level subnetting but allows more efficient allocation of IP addressing space to better match requirements of the network. Variable length subnetting implies the use of IP routing algorithms that support VLSM. This is known as CIDR (Classless Inter Domain Routing) and is supported by dynamic routing standards such as OSPF (Open Shortest Path First).

There are multiple software tools that can assist network designer with creating an IP addressing plan. Some of these tools are free online applications, for example:

- IP Subnet Calculator, http://www.subnet-calculator.com/
- VLSM (CIDR) Subnet Calculator, http://www.vlsm-calc.net/

Practical recommendations

- Consider future growth of the network however be reasonable as reserving excessive space for subnets may complicate addition of new services
- When designing an internal corporate network using IPv4, use private IP addresses if possible. A private network is a closed network within a company and if needed, it can still be connected to the Internet using a NAT (Network Address Translation) device or a proxy server
- For large networks or when a large number of hosts must be supported, consider implementing a class A private addresses (address range of 10.0.0.0 – 10.255.255.255 with 16,777,214 possible addresses)
- When segmenting the address space address blocks with the size of power of 2 (thinking in binary) are preferred in order to avoid address space fragmentation and to provide a simple evolution path, route summarization and to facilitate the implementation of Access Control Lists
- Use adjacent subnetting and avoid “holes” in the addressing plan and wasting of IP addresses
- Consider using Variable Length Subnet Masking (VLSM) for efficient allocation of suitably-sized address blocks
- Consider using supernetting (route summarization). This permits aggregation of a group of routes (IP subnet) into a single route. The benefit of supernetting is the reduction of routing table size. This is easily achieved by planning the address allocation in advance
- The IP addressing plan shall be carefully documented with details of all address blocks showing for example which IP addresses have been statically allocated to which devices, which IP addresses are dynamically allocated by DHCP, which IP addresses are unallocated, etc.
- Consider security constraints and Access Control Lists

4.3.4 Network Segmentation with VLANs

VLANs (Virtual LANs) are specified in IEEE 802.1Q as a mechanism that allows logical segmentation of the network into separate virtual broadcast domains. VLANs help segregate and secure network traffic and also permit prioritization of traffic according to IEEE 802.1p.

VLANs can be also seen as mechanism for facilitating the implementation of cyber security rules since hosts can only access other hosts on the same VLAN. Inter-VLAN traffic can be controlled using routers and Access Control Lists. Another benefit of VLANs is that broadcast traffic in one VLAN is isolated for the others.

In utility communication networks, typical services that are allocated to different VLANs are:

- Protection and control
- RTU communication
- Video surveillance
- Communications device management
- Voice over IP
- Synchrophasors

Separating these functions 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. Secure access to different VLANs by personnel is easily controlled at a central router demarcation point.

Practical recommendations

- In order to define a VLAN of a different size inside the network a similar approach to variable length subnet masking (VLSM) shall be used
- It is necessary to keep in mind that use of VLANs is going to impact the whole structure of the network, but the benefits often far outweigh the perceived added complexity

4.3.5 Determining Bandwidth Requirements

The bandwidth is an important aspect that designers must take into consideration because it has a direct impact on the Quality of Service. The key element for bandwidth definition is to know the bandwidth required for each application. Mainly, the traffic of each application (eg. from the substation to the control center) is carried through WAN links. Therefore network designers shall determine the WAN capacity in order to guarantee an efficient transport within the network.

Below, are given generic designing rules related to bandwidth (Min_Bdw = minimum bandwidth, Max_Bdw = maximum bandwidth) and WAN capacity calculations:

- $\sum$ (Min_Bdw) ≤ WAN capacity, where $\sum$ (Min_Bdw) means the total minimum bandwidth for all application passing through the WAN link
- For each application, Min_Bdw ≤ Max_Bdw ≤ WAN capacity
- For best effort applications, Min_Bdw = 0 (bit/s) and Max_Bdw = WAN capacity
- $\sum$ (WAN capacity) ≤ Physical_Bandwidth, where $\sum$ (WAN capacity) means the total capacity of all WAN links passing through physical link

Traffic prioritization (or classification) is used to avoid any random behavior in case of congestion, especially in case of bandwidth unavailability. Generally, the lower priority traffic will be marked first or dropped based on the policy mechanism that is defined in the network element.

There are several types of traffic prioritization, for example:

- IEEE802.1p for Ethernet
- DiffServ for IP
- EXP bits for MPLS

Examples of bandwidth requirements of selected applications are shown in Table 1 in chapter 4.4.6 and more detailed information can be found in CIGRE TB D2.23.

Practical recommendations

- If possible try to have similar capacity in all routes, this will facilitate future traffic engineering
- Every critical node in the network (eg. backbone node) shall have at least two independent routes to the rest of the network
- The number of common links for two different routes shall be minimized
- Consider defining a specific segment for the WAN links with 2 addresses, with enough address range to grow
- For new deployments consider 1Gbps links in the backbone as a starting point
- Consider using link aggregation protocol (IEEE 802.3ad) to increase available bandwidth by aggregating multiple links together
- For substation LAN 100Mbps links to connect IEDs may be sufficient for most of the applications, however 1Gbps links shall be considered for the interswitch connection especially if IEC 61850-9-2LE Process Bus or video surveillance applications are going to be used

4.3.6 Determining Latency Requirements

Latency can be defined as the amount of time it takes a packet to travel from source to destination. In legacy substation architectures, where all the data and signal interchange was resolved by means of hard-wiring, the users and applications were not latency aware, as in practice there was no network. Signals were received instantaneously by the devices which had to take care of them.

However, in modern substations running SCADA/Control applications over IP networks with latest generation protocols such as IEC 61850, the network introduces some latency that needs to be addressed. Protection relays and other equipment are not hardwired, but critical data comes over a network which is shared among many devices.

Some applications are very sensitive to transmission delays and latency jitter, such as RTU protocol communications. These problems can be avoided by proper network design and transmission technology selection. Depending on the type of network and the lower layer technologies upon which the IP network is built, the behavior in terms of latency will vary significantly.

Packet switched networks have several sources of latency:

- Transmission media latency
- Transmission equipment latency (e.g. Ethernet switch or router):
    - Store-and-forward
    - Switch fabric processing
    - Frame queuing

For wired connections all of these latencies except for queuing are deterministic and yet the effects of frame queuing can also be calculated providing one knows the nature of all sources of traffic on the network.

Transmission media latency in wired networks is typically very small for fiber optic based systems however it can be rather high in wireless links.

Medium	Time to traverse a link.
CAT-5 and CAT-6 cables	0,55 µs per 100 m (5,5 µs/km)
Glass-Fibre cables (Corning smf28)	0,49 µs per 100 m (4,9 µs/km)
Free air (wireless)	0,33 µs per 100 m (3,3 µs/km)

Table 1: Latency values for ISO/IEC 8802-3 frame to traverse the physical medium

Store and forward refers to the basic operating principle of an Ethernet switch. The term is descriptive of its actual operation: the switch stores the received data in memory until the entire frame is received. The switch then transmits the data frame out the appropriate port(s). The latency this introduces is proportional to the size of the frame being transmitted and inversely proportional to the bit rate.

The internals of an Ethernet switch are known as the *switch fabric*. The switch fabric consists of sophisticated silicon that implements the store and forward engine, MAC address table, VLAN, and CoS, among other functions. The fabric introduces delay when executing the logic that implements these functions. The switch fabric latency in utility grade hardened switches is typically in a range of few micro seconds.

Ethernet switches use queues in conjunction with the store and forward mechanism to eliminate the problem of frame collisions that used to exist on broadcast Ethernet networks. Queuing introduces a non-deterministic factor to latency since it can often be very difficult to predict exact traffic patterns on a network. *Class of Service* (CoS) introduces a priority scheme to Ethernet frames to help mitigate queuing latency. It is a best-effort service, however, and cannot guarantee quality of service, since multiple frames at the highest priority level must still be queued relative to one another. Another consideration is that if a lower priority frame has already started transmission, then that frame must be completed before the switch may begin transmitting the higher priority frame.

Calculating with absolute certainty the worst case latency for any Ethernet frame can be challenging. More details on this topic and examples of latency calculations for wired networks can be found in [Reference **2**]

The table below provides typical latency values for IP links over different media, observed in utility applications.

IP Network connection	Typical latency (ms)
IP link over wired Ethernet LAN inside substation (no routers)	<1-10
IP link over wired IP WAN (intermediate routers)	20-100
IP link over proprietary point-to-point wireless Network (latency of a single hop)	10
IP link over proprietary point-to-multipoint wireless Network (latency of a single hop)	30
IP link over UMTS network	200-300
IP link over VSAT network	400-600
IP link over GPRS network	400-1000
IP link over TETRA network	1500-2000

Table 2: Typical latency values for IP links

As it can be derived from Table 2, latency values for certain IP link types make them unsuitable for time sensitive applications, whereas others are perfect for applications not requiring strict timings.

As network resources are finite, the latency of a given IP network can be dependent on the level of utilization (or congestion) of the network resources. As a result of this, it is necessary to manage them carefully by means of traffic prioritization with layer 3-4 policies, so the applications that really need priority are the ones that get it, and thus ensure lower latency for them. A network management principle states that “if everyone uses high priority, no one actually gets it” [R. Seifert, ”The Switch Book].

Service	Data Rate (Kbit/s)	Service Requirement Maximum Latency (ms)
Voice (1 channel) 3	2.4-100	< 100
Telecontrol 4 SCADA ICCP Control WAN	 0.05 – 64 9.6 – 64 Typical 2048	 < 1000 < 1000
Teleprotection 5 Blocking Permissive Intertrip	 < 64 < 64 < 64	 < 4 < 5 < 8
Line Differential Protection 6 EHV (Extra High Voltage) HV (High Voltage) MV (Medium Voltage)	 < 64 < 64 < 64	 < 5 < 10 < 40
Video Surveillance	256 – 4096	< 1000
Other operation data	1.2 – 100	< 1000

Table 3: Operational Services Latency Requirements

Values in the table are given in

[Reference **3**].

Practical recommendations:

- For time critical applications (e.g. teleprotection signaling), select a technology with low latency such as switched L2 networks or hardware based routed L3 networks (use L3 switches instead of routers)
- For applications which are sensitive to channel asymmetry, choose a transmission technology that allows creation of bi-directional paths (such as SDH), where transmit and receive follow the same path and thus experience the same delay

3 Connection time is also important for operation applications.

4 The communication channel latency has been taken as typically 1/10th of the application response time.

5 Despite that teleprotection has bandwidth requirement of less than 64kbit/s today it is more and more common that teleprotection devices have native 2Mbit/s output channels in order to interface directly to SDH equipment.

6 Differential protection is also very sensitive to differential delay between transmit and receive time (channel asymmetry variations). If the latency is constant then it doesn't have big effect on line differential protection. The most important for differential protection is that variations in latency (jitter) should be small.

- For applications which require deterministic jitter, the use of IP technology that supports jitter buffers or other technology helping to secure deterministic jitter is recommended. Jitter buffers introduce clock stamps in data packets and help asynchronous Ethernet become synchronous. It is worth mentioning that jitter buffers add delay to transmission channel.
- Use QoS and prioritization methods for time critical traffic to help minimize latency

4.3.7 Determining the Type of Physical Media

Different types of media can be used in the IP network; the most important are copper cable, optical fiber cables and wireless links.

- Local Area Networks:
  - Optical Fiber
  - Copper
  - Wireless WiFi or WiMAX
- Wide area networks
  - Optical Fiber
  - Copper
  - Power cables (Power Line Carrier)
  - Wireless: RF Mesh, Cellular, Point-to-Point, Point-to-Multipoint, WIMAX, LTE, etc.

The table below provides an overview of the most commonly used physical media. The maximal length of the link and the bandwidth depend on different parameters and constraints and are given here as an example. Please note that the bandwidth limitation evolves rapidly with technological progress.

Medium	Max. length	Bandwidth	Typical Interface
Copper	10 - 15 m	64 kbps - 44 Mbit/s 7	V.35
Copper	4 - 15 km	< 50 Mbit/s	xDSL
Copper	55 - 100 m	10 Mbit/s – 10 Gbit/s	
Fiber Multimode	500 - 2000 m	10 Mbit/s – 100 Mbit/s	
Fiber Multimode	550 m	1 Gbit/s	
Fiber Single Mode	Up to 100 km	> 10 Mbit/s - 40 Gbit/s	
Narrowband	Up to 80 km	9.6 - 64 kbit/s (1)	Wireless
RF Mesh (included IEEE 802.11 WiFi)	500 m – 12 km	Up to 55 Mbit/s (1)	Wireless
Broadband point-to-point	Up to 120 km	50 – 1000 Mbit/s (1)	Wireless
Proprietary Broadband point-to-multipoint	Up to 100 km	Up to 1 Mbit/s (1)	Wireless
Standards based Broadband point-to-multipoint (IEEE 802.16d or 802.16e WiMAX)	Up to 30 km	Up to 13 Mbit/s (1)	Wireless

Table 4: Most commonly used physical media

For copper based Ethernet the most used nowadays are Category 5 Enhanced (Cat-5e) and Category 6 (Cat-6) cables. The rugged version STP (Shielded) of FTP (Foiled) are often used in substations. A study

[7] All wireless technologies are characterized by a trade-off between range and throughput. Also line-of-sight propagation has direct effect on available throughput and maximum range a prerequisite

done by EPRI in 1997 looked at the susceptibility of shielded and unshielded Cat-5 cable to electrical fast transients which are a common EMI phenomenon in substations. The results indicated large communications frame loss; up to 75% frame loss for -2kV transients on Cat-5 cables.

Once a decision is made for where to use fiber, there are still decisions to make regarding the type of fiber, connectors and transceivers. There are two basic types of fiber: multi-mode and single-mode. The former can use inexpensive LEDs to impart light onto the cable but has bandwidth and distance limitations: 2km at 100Mbps, and 550m at 1Gbps. The latter requires a higher quality laser light but allows almost infinite bandwidth and distances exceeding 100km. Multi-mode fiber is generally suitable within the substation for the majority of applications and is often used today.

Practical recommendations for the substation LAN

- Use copper cat5 or cat6 cables only inside racks and protection cabinets that are installed inside buildings. RJ45 connector is recommended however it is not very robust and has limited EMC/EMI tolerance. If needed a more rugged M12 connector can be used.
- Use fiber optic cables for all inter switch links also always when deployed outside buildings (eg. crossing the switchyard or interconnecting outdoor equipment). In substation LAN multimode fiber shall be sufficient as typically has maximum length of up to 500-2000 meters. Recommended cabling is 50 µm (50/125) fibres, with LC connectors for interswitch links. SFP technology shall be considered as flexible way for future modifications or upgrades.
- For Gigabit links copper cabling and 1000BaseTX is not advised as many copper 1Gbps transceivers are characterized by long link loss detection times (up to 700 ms), this may cause large failover times even if RSTP protocol is used and thus making it not suitable for critical application such as tripping over IEC 61850 GOOSE in station bus.
- For Gigabit links, the use of LAN 1000BASE-LX optical fiber cabling with LC connectors is recommended
- WiFi or WiMAX can be used however the amount of metal or concrete structure elements may have impact on wireless propagation. Careful site survey and radio planning is recommended. WiFi or WiMAX service is recommended as useful means for providing connectivity for field force for commissioning, testing and maintenance purposes.

4.3.8 Choosing Wireless Technology

There are multiple wireless options available:

- Public cellular networks:
  - 2G, 3G and 4G (LTE)
  - IEEE 802.11 (WIFI)
- Private wireless networks:
  - Data over Voice UHF/VHF/Trunked systems
  - Microwave Broadband Wireless systems
  - Mesh wireless systems
  - IEEE 802.16 (WiMAX)
  - ZigBee
  - TETRA
- Satellite networks

Different applications will imply different technology. For example interconnection of sensors, meters, reclosers or capacitor banks in medium voltage networks require small throughput. On the contrary a wireless backhaul link to a regional control center or a transmission substation may require dozens Mbps of throughput and very low latency.

Utility backbone based on Ethernet or SDH technology may have islands connected via broadband wireless point-to-point links. It should be specified what throughput and technology shall be transferred over wireless, for example fast or gigabit Ethernet or multiple E1/T1 circuits. In case of the necessity to transfer Ethernet data it is recommended that the wireless system has native Ethernet support to avoid extensive mapping over TDM circuits. This will result in higher throughput and lower latency.

The question of using public carrier networks or a private wireless network is important from the point of view of reliability, availability, security, ownership and control over the network and finally CAPEX and OPEX.

Public carriers have evolved to meet many needs of power utilities and require limited capital expenditure. Public carriers provide moderate throughput, pervasive coverage, acceptable latency, and adequate security features. However, the need for additional security, channel availability during emergencies, and the ability to pass significant data in the uplink remain concerns.

Broadband standard based technology such as IEEE 802.16e (WiMAX), is deployed in licensed, lightly licensed, and unlicensed bands. It provides flexibility of deployment in areas where regulatory allocation of frequencies is limited. The ecosystem of solutions available is larger and not limited to a single vendor.

Initial deployment costs may be higher in case of private infrastructure than for public infrastructure. However in the long term private infrastructure may result in lower OPEX and more reliable operation as it is under full control of the electric utility.

Practical recommendations:

- For wireless links connecting two sites and to carry a single application such as teleprotection between two substations microwave long range, low latency point-to-point technology is recommended
- For multipurpose architecture and simultaneous support of various IP based applications a point-to-multipoint technology such as IEEE 802.16d or IEEE 802.16e shall be considered
- To ensure reliability, security and channel availability during emergencies the use of private wireless infrastructure is preferred over a public infrastructure

4.3.9 Defining Routing Strategy

IP routing directs packet forwarding across multiple networks from its source to its destination. The purpose of routing protocols is to communicate information about all network paths used to reach a destination and to determine from those paths, the best path to reach a destination network. Routing protocols enable routers to create forwarding tables that correlates final destination with next hop address.

The following list describes basic concepts related to routing:

- Autonomous System (AS) - is a group of networks under a single administrative control. An autonomous system can be a utility company for example. To distinguish one autonomous system from another, an AS can be assigned a unique number from 1 to 65,535. The Internet Assigned Numbers Authority (IANA) is responsible for assigning these numbers
- Interior Gateway Protocol (IGP) - is a routing protocol that handles routing within a single autonomous system. Examples are well-known RIP, EIGRP, OSPF, IS-IS (Intermediate System-Intermediate System)
- Exterior Gateway Protocol (EGP) – is a routing protocol that handles routing between different autonomous systems. Nowadays Border Gateway Protocol (BGP) is the most popular EGP protocol. It is used to route traffic between different autonomous systems that are spread across the Internet backbone

Routing protocols can be divided into two top level categories:

- Distance vector protocols: the routers learn routing information from directly connected neighbors. The principle of these protocols is that all routers periodically inform their neighbors of topology changes
- Link state protocols: use the Shortest Path First (SPF) algorithm to find the best path to a destination. Every node constructs a map of the connectivity in the network, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical hop from it to every possible destination in the network. The collection of best next hops will then form the routing table

Practical recommendations:

- For new deployments consider using link state routing protocols rather than distance vector protocols
- For private networks IGP protocol should be considered. If connection to Internet is required then it could be handled by proxy server, NAT or a VPN scheme
- If there is a need to have a routing protocol within a larger (>10 routers) system, then OSPF is a popular choice enabling easy implementation. In addition, it provides a relatively fast recovery mechanism while supporting a hierarchical network structure.
- Use hierarchical network design with a backbone and several sub networks
- When possible keep the number of sub networks low. For mid/large size TSO with 200-400 substations a number of sub networks lower than 10 is a good starting point
- Consider the physical communications structure and when possible follow the layout of the transmission grid network. If there are natural transmission rings, these can be grouped into a regional sub network
- Consider company organization, eg. geographical locations of maintenance centers, separate operational areas or regions, etc.
- Create a backbone routing “Area 0”. In this backbone include Headquarters and main important centers like Operation and Maintenance Centers
- Create several routing “non-backbone areas”. These areas can match the regional sub networks and shall have similar size
- Connect sub networks to the backbone with at least one level of redundancy
- Configure DHCP server in the substation LAN router. Ensure DHCP is enabled on designated ports only, isolate these with specific VLAN and ensure authentication is required to access the network. DHCP on substation router allows maintenance staff to automatically obtain IP address for maintenance laptops connected to the network when needed

4.3.10 Choosing Network Hierarchy and Transport Technology

A good practice for obtaining an efficient network design is to build the network topology based on a hierarchy of multiple layers, for example:

- Access network layer
- Distribution network layer
- Backbone network layer

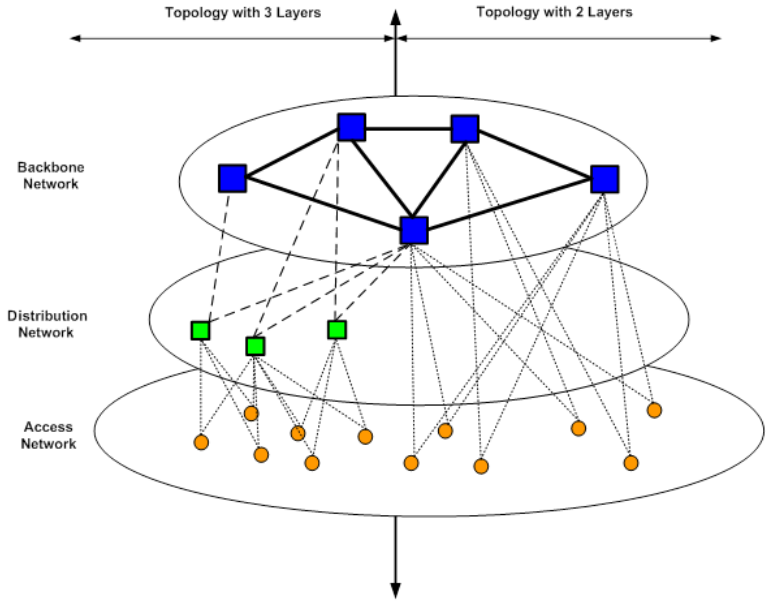


Figure 19: Example of layered network hierarchy

Access Network

The access network is composed of equipment that performs the role of concentration points of all (or some) applications in the substation. It's the edge of the network where end devices are connected.

Distribution Network

The distribution network is the intermediate layer between access and backbone networks, the following are selected functions of the distribution network layer:

- Termination of Ethernet connections for access network (e.g. VLANs)
- Implementation of policies for QoS (traffic control, prioritization, etc.)
- L3 traffic routing (if applied)

Backbone Network

The backbone Network provides high-speed and efficient transport to satisfy the high requirements of end users and applications. The backbone needs to fulfill requirements for QoS, reliability, etc. As this is the core of the network, it has to provide the highest availability of the three network layers described here. The technologies and type of equipment that can be deployed in backbone network are detailed in the next section.

As shown in Figure 19, we can use this hierarchical model in two ways:

- Network hierarchy based on 2 layers
- Network hierarchy based on 3 layers

The two layers hierarchy is suitable for medium size networks. In this case network devices in access layer can be connected directly to the backbone network equipment. Therefore, there is no interest to insert the intermediate distribution layer between access and backbone networks. This hierarchy can also be proposed for some mission-critical applications that have more demanding latency requirements.

The three layers hierrachy is suitable for medium size and large networks. Splitting a large network into three independent hierrachical levels permits more optimized asset and data management.

Each of the layers described above may be implemented with different network topology, for example linear, star, mesh or ring. The following factors are key for selection of the logical network topology:

- The available underlaying physical topology
- The required level of traffic redundancy
- The technical possibility of builiding a particular topology with selected transport technology

Several technologies are available to carry Ethernet/IP based applications; however few of these technologies can meet requirements of power utilities, especially to carry mission-critical applications. The most important technologies available for IP Backbone networks are:

- Ethernet
- Ethernet over SDH
- IP-MPLS – IP
- MPLS–TP
- PBB
- PBB–TE

Practical recommendations

- Depending on the network size choose two or three layers hierarchy
- For access layer use devices with Layer 2 switching capabilities, consider non-Ethernet interfaces for legacy applications
- For distribution layer use IP routers and/or layer 3 switches
- For backbone technology consider physical separation of critical applications from non-critical applications. Physical separation is generally speaking more secure and more reliable than virtual separation however it is usually more expensive

4.3.11 Determining Redundancy Protocols and Mechanisms

Once the network topology and transport technology is defined the network designers have to choose the appropriate redundancy protocols to satisfy network redundancy requirements. Different redundancy protocols may apply to different layers or different parts of the communications architecture. Considering different nature of the communications inside electrical substations and in backbone network that connects substations and control centers it may be useful to separate network redundancy into two categories:

- Redundancy in the substation LAN network
    - RSTP Protocol
    - PRP Protocol

  - HSR Protocol
  - VRRP Protocol
- Redundancy in the WAN network
  - SDH Protection Mechanisms
  - RSTP Protocol
  - IP Routing Protocols
  - IP-MPLS with TE
  - MPLS-TP Linear Protection Switching
  - PBB-TE Linear Protection Switching

Substation LAN networks are implemented in vast majority using layer 2 Ethernet technology. The most widely deployed layer 2 redundancy protocol in these networks is RSTP (Rapid Spanning Tree Protocol). The failover time when using an optimized implementation of the standard RSTP protocol can be in the range of 5 milliseconds per hop with the maximum number of 40 hops.It means that in a large substation network formed by 40 Ethernet switches the worst case of a single communication link failure results in a failover time of 200ms. Apart from link failures also failures of Ethernet switches have to be considered. The worst case of switch failure is the case when the switch acting as “root bridge” fails. In this situation the behaviour of RSTP protocol is non-deterministic and the network outage can last several hundreds of milliseconds or even few seconds.

The most critical applications inside substation LAN have the requirement of zero-packet-loss and no outage time at all. For these applications high availability redundancy protocols like PRP or HSR shall be used. PRP (Parallel Redundancy Protocol) and HSR (High Availability Seamless Ring) are defined in IEC 62439 standard and facilitate truly zero-time-recovery as all traffic is transmitted by each node simultaneously via two independent network interfaces.

For the edge routers connecting substation LAN to the WAN network VRRP or HSRP redundancy protocols are used. HSRP originally was a proprietary protocol and later on has been specified in RFC 2281. VRRP is implemented by larger number of manufacturers as it is a non-proprietary alternative to HSRP. The latest specification of VRRP is contained in RFC 5798.

WAN network redundancy protocols depend on the transport technology. If IP technology is used redundancy protocols will vary if the network is realized on L3 or L2.

Ethernet over SDH (EoSDH)

If the WAN transport technology is Ethernet over SDH network redundancy is accomplished by any of SDH protection mechanisms with switchover time typically below 50ms:

- SubNetwork Connection Protection (SNCP) / Path Protection on VC-x level
- Multiplex Section Protection (MSP) on a point-to-point SDH section
- Multiplex Section Shared Protection Ring (MS-SPRing) on ring networks

Additionally EoSDH can make use of the Link Capacity Adjustment Scheme (LCAS), where the only virtually concatenated containers can take different routes through the network and LCAS adjusts to the actual available bandwidth if one path should fail.

Pure L2 Ethernet and L3 IP networks

Redundancy in L2 WAN network is typically realized with RSTP protocol where the failover time depends on the topology. RSTP failover time in WAN network is typically below 1 second however in case of root bridge failure it can be up to several seconds. Redundancy in L3 network can be realized by any IP routing protocol (e.g. OSPF) and the switchover times is in the range of several seconds.

MPLS

In IP-MPLS the topology reconfiguration in case of a network node failure uses L3 re-routing functionality and does therefore not offer fast protection switching. Only the addition of Traffic Engineering (TE) to IP-MPLS allows to setup backup path in advance for faster switching times. MPLS-TP offers a range of fast protection switching mechanisms. ITU-T G.8131 describes MPLS-TP Linear Protection (currently for T-MPLS but the upcoming next release is expected to cover MPLS-TP as well).

PBB / PBB-TE

PBB relies on the standard L2 protection mechanism RSTP, with the known limitations in switching times. PBB-TE provides end-to-end linear path protection according to IEEE802.1Qay with sub-50ms switching times.

Practical recommendations

- Substation LAN Layer 2 switches with redundant power supply are recommended

5 Technical details

There are several, options to propose network architecture for IP based applications. The following are described in this section:

- Ethernet switching technology (Layer 2 Ethernet switched network,)
- IP routing technology (Layer 3 Routing - RIP-2, OSPF, etc.)
- MPLS-TP and IP/MPLS technologies
- PBB and PBB-TE technologies

This section describes these technologies in some more details. The section also describes cyber security considerations and inter-substation communication acc. to IEC 61850.

5.1 Network Technology Descriptions

5.1.1 Ethernet Layer 2 Networks (Switched networks)

Layer 2 networks, also referred to as Data Link Layer or DLL networks are networks that operate on layer 2 of the 7 layer OSI model. The three main functions of the Data Link Layer include framing mechanisms, addressing and error detection. Addressing and frame forwarding is based on MAC addresses (Medium Access Control) i.e. hardware addresses. Layer 2 addresses are thus also not assigned by any network designers but given by the hardware manufacturer, which means that logical structuring in a network is not possible based on Layer 2 hardware addresses.

Ethernet Layer 2 networks do not include any routing procedures, i.e. no routing protocols are exchanged between L2 devices (switches). Forwarding decisions are purely made on locally available information. An Ethernet switch per default broadcasts a received frame on all available outgoing ports. However switches provide a local learning mechanism, where the source address of incoming frames is registered and mapped to the incoming port. For future frame transmissions this destination address is known and only forwarded on the registered port.

Ethernet Layer 2 Networks offer connectionless services. Connection control has to be handled by higher layer protocols such as TCP (Transmission Control Protocol).

The following figure depicts the basic frame format of Ethernet frames.

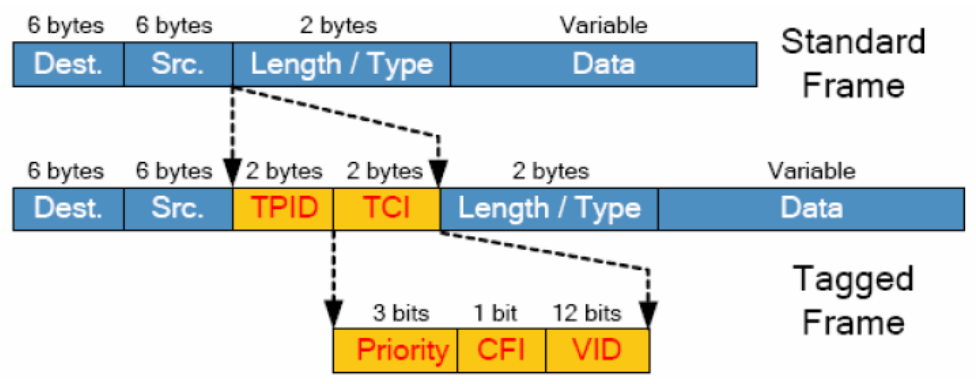


Figure 20: Ethernet Frame Formats

The standard frame is defined in IEEE 802.3, with the extensions for VLAN tagged frames being defined in 802.1Q:

- Tag Protocol Identifier (TPID), typically set to 0x8100 to identify tagged frames
- Tag Control Identifier (TCI)
  - Priority Code Point (PCP). 3-bit field to assign priorities
  - Canonical Format Indicator (CFI)
  - VLAN Identifier (VID): Virtual LAN identifier

With Telecom operators, pure Layer 2 technology is not used for transport networks. With utilities this might however still be an option. A typical application is IEC 61850 traffic, where GOOSE and SV traffic (see [Reference 5]) is based on layer 2 communication. Layer 2 networks can also be an option for SCADA system in distribution networks.

5.1.1.1 Quality of Service (QoS)

As Ethernet is basically a shared media (best effort policy), it's very difficult to provide hard Quality of Service. In Layer 2 networks, QoS very much depends on the network load and the network engineering and is difficult to predict.

Ethernet switches support Class of Service (CoS) functionality based on priority settings. CoS has been introduced with IEEE 802.1Q. As described above, the VLAN tag includes a 3-bit priority indication (PCP).

The 3 bits available for the VLAN priority allows for 8 different priority levels based on IEEE 802.1p as described in the table below..

CoS	Application/Traffic
0	Best Effort Data
1	Background Data
2	Spare (undefined)
3	Excellent Effort
4	Controlled Load
5	Video
6	Voice
7	Network Management

Table 5: Ethernet CoS

Today many Layer 2 Ethernet Switches also support traffic prioritization based on Differentiated Services Code Point (DSCP). DSCP is a priority indication in the IP header. This does however not mean that switches operate on Layer 3, but they are capable of checking the priority information in the IP header (in the Ethernet payload) and prioritize the Ethernet frames based on this information

5.1.1.2 Scalability

Pure Ethernet Layer 2 networks face a number of challenges regarding scalability:

- Size of MAC address table
  In very large Layer 2 networks, the MAC forwarding tables in the switches may become very big. Depending on the deployed hardware the total number of addresses or the number of addresses per port may be too big to handle
- One broadcast domain
  A Layer 2 network builds one broadcast domain. If the network is too big, broadcast traffic may contribute too much to the traffic load
- No logical structuring
  As MAC addresses are assigned randomly it is not possible to bring a logical structure to the network (as compared to IP networks, where this is possible). This complicates the design of big networks
- Limit in number of VLANs
  With the 12-bit VID field, it is possible to define up to 4096 VLANs. Depending on the number of sites, customers and services that have to be distinguished, this may become a limitation

The following helps, to overcome some of the Ethernet scalability issues:

- Use of Q-in-Q mechanism (double tagging) for better structuring of customers/services. Q-in-Q is defined in IEEE 802.1ad.
- Design a mix of Layer 2 and Layer 3 networks, where the layer 3 components (routers) allow to structure and separate different Layer 2 domains
- Introduction of other Layer 2 technologies like Provider Backbone Bridging (PBB) – see other section of this document for details

5.1.1.3 Maturity

The basic concept of Ethernet was introduced by Xerox in the 1970s. IEEE Standards started to deal with Ethernet in the 1980s. Since then a huge number of IEEE standards has been elaborated around the Ethernet technology. Today it is the most widely used Layer 2 network technology and can be viewed as mature.

Networks up to 10 Gigabit Ethernet have already been standardized, and IEEE is currently working on 40 and 100 Gigabit Ethernet standards.

5.1.1.4 Management

Management in Layer 2 systems works mainly on the equipment level, but not on the network level. It is thus not possible to monitor every end-to-end service. The configuration and performance management can be supported by L2 NMS (typically through SNMP).

Further reading about the topic of Ethernet Transport Networks: See [Reference 4].

5.1.2 Ethernet Layer 3 Networks (Routed networks)

The network layer, IP layer 3 enables us to define scalable networks. With minor modifications and limited resources it is possible to expand the network.
The IP- numbering structure has to be well designed to suit the organization future growth. The routing protocols can aggregate the different subnets to define a scalable and reliable network. The subnets form then a ‘Broadcast Domain’. Per default broadcasts are blocked by routers.

Scalable IP networks are often designed following the next model:

- Core layer: This layer (also called Backbone) is designed to provide a reliable and high available transport
- Distribution layer: This is a campus backbone and provides interconnections to different parts of the networks and services
- Access layer is the access to the local resources and users

In smaller implementations, we may only see the Core and the Access layers.

5.1.2.1 Quality of Service (QoS)

The following architectures are used to cope with the issues of Quality of Services (QoS) for some applications such as VoiP and video:

Differentiated Service (DiffServ)

DiffServ uses the six most significant bits of Type of Service (ToS) field in the IP packet header; it is called DiffServ Code Point (DSCP).

Per Hop Behavior (PHB) is applied by the conditioner (for the traffic) at the Edge Router according to pre-determined policy criteria. There are four main PHB standards under DiffServ mechanism:

- **EF** Expected forwarding (RFC 3246): EF minimizes latency and jitter and provides highest level of QoS
- **CSx** Class Selector (RFC 2474): where x corresponds to the IP Precedence value (The three most significant bits of ToS)
- **AFxy** Assured Forwarding (RFC 2597): where x corresponds to the IP Precedence value and y corresponds to the Drop Preference value;
- **BE** Best Effort

DiffServ doesn't support End to End QoS control, but it is controlled by an administrative contract and Service Level Agreement (SLA).

Integrated Service (IntServ)

IntServ is based on resource reservation process (RSVP protocol for example). There are three classes of services in IntServ:

- Guaranteed Service (RFC 2212): IP Packets will arrive at designed delivery time without packet loss
- Controlled Load Service (RFC 2211): No guaranteed delivery time of IP packets, but with minimum of packet loss ratio
- Best Effort: No guaranteed delivery time

IntServ supports End to End QoS control (dynamic control) that it is initialized by the application layer.

IntServ is more difficult and complex to implement compared to DiffServ

5.1.2.2 Scalability

L3 designs include a number of features that provide scalability

- Network segmentation: Internal substation, WAN links to aggregation routers (SS-SS, SS-CC). Subnetting allows to structure the network

- L3 allows interconnection between several LANs, therefore to extend the number of hosts
- Use of NAT allows to reuse same IP address range in several LANs
- For higher number of required IP address, IPv6 will support better scalability

5.1.2.3 Maturity

L3 Routing based on IP is a mature technology; the IP standardization was in the mid Seventies. Most new transport technologies rely on IP. The current version is IPv4 (1984). The new version IPv6 is not yet implemented at large scales.

5.1.2.4 Management

Management in Layer 3 systems works on the equipment level, but not on the network level. It is thus not possible to monitor any end-to-end services. However the configuration and performance management are supported by L3 NMS (typically through SNMP).

5.1.3 Provider Backbone Bridging (PBB) / Provider Backbone Bridging –Traffic Engineering (PBB-TE)

Native Ethernet networks present a number of limitations that may seriously impair the performance of some services. The most relevant being the lack of service performance control and the limited scalability due to the MAC addresses learning explosion that can be experienced in large flat networks and that may create unexpected traffic loads.

The new set of Ethernet standards addresses these drawbacks by defining a method of isolating client Ethernet LANs from the service network implemented using Ethernet technology. The new working principle is simple and straightforward since it consists in adding a new Ethernet MAC header to the client Ethernet frame. Thus, the client Ethernet frame is tunneled through the service network.

The working principle of the service provision WAN is further simplified by disabling the MAC address learning procedure and setting fixed forwarding tables that define the routes that tunnels will follow to cross the WAN. This facility paves the way to the implementation of traffic engineering and formal QoS support. Furthermore, backup disjointed tunnels can be defined to support self-healing services.

The new architecture is based on the following standards:

IEEE 802.1ah. Provider Backbone Bridge (PBB). Defines the provider backbone broadcast domain working principles, as well as the format of the header added to cross the provider backbone

IEEE 802.1Qay PBB Traffic Engineering. Dynamic MAC learning procedure and spanning tree algorithms are disabled. Instead, forwarding based on the static forwarding database (FDB) entries is implemented. The FDB is configured by the management centre which is responsible for the establishment of loop-free tunnels. Broadcast and multicast frames of the client LAN are encapsulated and unicasted through the associated tunnel. Path protection is provided by configuring a disjoint redundant path. This configuration has to be done from the management centre.

ITU-T G.8032 Ethernet Ring Protection (ERP). It provides the mechanism to recover service in a ring.

Provider Link State Bridging Protocol (PLSB): To provide dynamic routing in PBB, a link-state protocol based on Intermediate System to Intermediate System (IS-IS) protocol is proposed, in which the IP address identifiers in IS-IS are replaced by Ethernet MACs. Another advantage of PLSB is that a single control protocol is used.

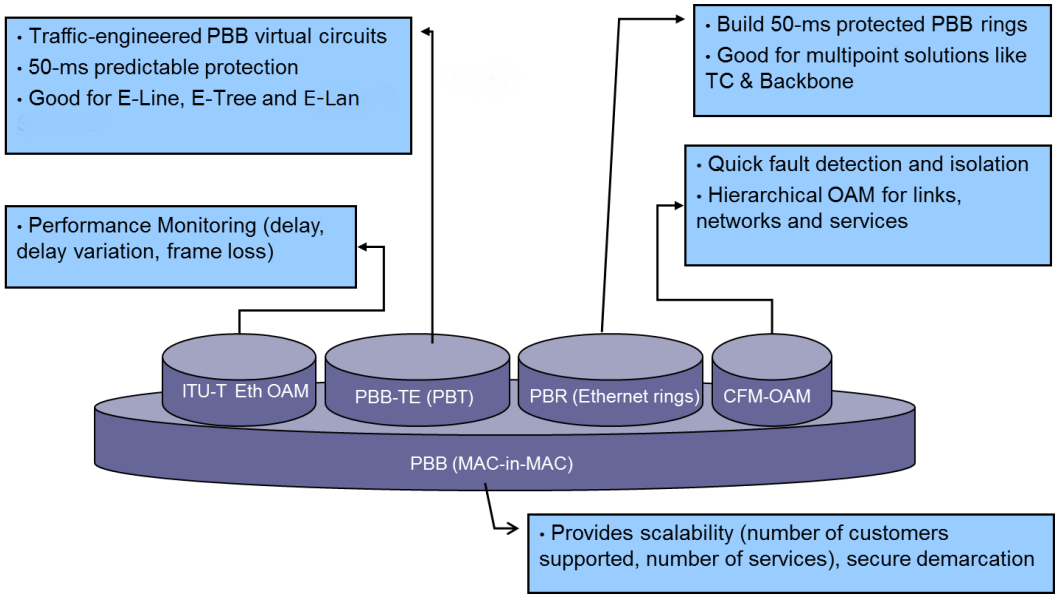


Figure 21: Provider Backbone Bridging

The key advantages of this new approach are:

- **Service unification and transparency.** PBB provides isolation between substation LANs and Ethernet WAN even though they use the same protocol
- **Quality of Service.** Traffic Engineering together with admission control and scheduling in every node may provide a quasi-deterministic transport service over the PBB Ethernet core. Inside the PBB core, the symmetry of the path can be guaranteed, which provides connections with the same latency in both directions
- **Improved service resiliency.** The standard ERP and the capability of managing redundant path recovery mechanism allow recovering a path in less than 15 msec
- **Improved OAM facilities.** Ethernet layer has been complemented with network management services and functions that provide the same level of functionalities than existing networking technologies

The PBB Header

Provider Backbone Bridging (PBB) operates in exactly the same manner as IEEE 802.1ad (Q-in-Q). However, instead of operating on Customer and Service MAC addresses, a new Backbone MAC (B-MAC) address is used. The B-MAC is added or removed at the edge of the PBB network. Outside of the PBB area, the packets are forwarded using the standard header.

PBB uses Multiple Spanning Tree Protocol (MSTP) to establish rooted broadcast domains in the network, with each domain associated with a Backbone Virtual LAN (B-VLAN). Unknown MAC addresses are only broadcast within the given B-VLAN.

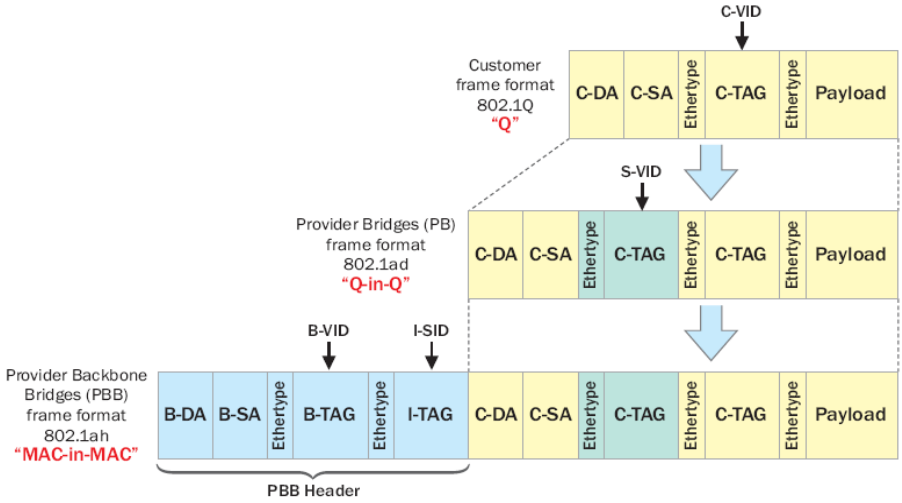


Figure 22: PBB Header

C-DA: Customer Destination MAC Address
C-SA: Customer Source MAC Address
S-VID: Service VLAN ID
C-TAG: Customer VLAN ID

B-DA: Backbone Destination MAC Address
B-SA: Backbone Source MAC Address
B-VID: Backbone VLAN Id
I-SID: Service ID

PBB-TE

One of the drawbacks of PBB technology was the use of Spanning Tree Protocol (STP) as a control plane. Despite of STP endeavors to remove loops by closing ports and links, the use of STP wastes resources.

STP is also slow to recover from changes that take place in the network and to recalculate the optimal paths in the network.

PBB-TE removes STP entirely, The Network Management distributes the forwarding tables to each node allowing that the network becomes symmetrical and deterministic. Also broadcasting and flooding of unknown MAC addresses was removed. This Management directed routing procedure also allows the feature of sub-50 ms path switching.

The combination of PBB and PBB-TE thus provides both point-to-point and multipoint connectivity. PBB and PBB-TE can be run on the same network from the same Carrier Ethernet switch, at the same time. The combination of PBB and PBB-TE is similar to the combination of MPLS label switched paths (LSPs) and virtual private LAN service (VPLS).

5.1.3.1 Quality of Service (QoS)

The possibility to dynamically refresh the routing tables from the System Manager allows a lot of possibilities actually and in a close future in which the traffic congestions could be inferred before they occurs, and the traffic rerouted using fuzzy logic or other self-learning algorithms

Traffic Engineering together with admission control and scheduling in every node may provide a quasi-deterministic transport service over the PBB Ethernet core. Inside the PBB core, the symmetry of the path can be guaranteed, which provides connections with the same latency in both directions.

5.1.3.2 Scalability

With the I-SID, PBB also improves the scalability of Ethernet, which previously was restricted to 4,094 service instances due to the limited 12-bit VLAN field. The 24-bit I-SID now supports up to 16 million service instances. This effectively separates services from transport with services identified by the I-SID and the "transport" indicated by the B-VLAN broadcast domain.

5.1.3.3 Maturity

IEEE 802.1ah (PBB) was released in 2008, IEEE 802.1 Qay (PBB-TE) was released in 2009.

PBB-TE might play an important role for guaranteed, connection-oriented data transport in the aggregation and transport portion of telecom operators networks. However it is currently hardly discussed in the utility environment and currently not widely implemented at telecom operators. The PBB protocol was initially designed by Nortel Networks before submitting it to the IEEE. The future of this technology is uncertain as Nortel and also other manufacturers recently cut investments in PBB.

5.1.3.4 Management

IEEE 802.1ag / ITU-T Y.1731. Service layer OAM and Connectivity Fault Management. This standard defines the messages used to upgrade Ethernet with OAM functionality. The main features included are: Tunnel continuity check, Alarm Indication Signal, performance monitoring, etc.

For PBB-TE the Forwarding Database (FDB) is configured by the management centre which is responsible for the establishment of loop-free tunnels. All the entries are static and not introduced by any dynamic protocol.

The traffic paths can be defined manually or automatically from the Network Management System.

5.1.3.5 Service Types

PBB supports point-to-point, point-to-multipoint and any-to-any service. This enables the provision of Ethernet LAN (E-LAN) and Ethernet Line (E-LINE) services as specified by the Metro Ethernet Forum (MEF).

5.1.4 MPLS-IP

MPLS-IP stands for Multi-protocol Label Switching. MPLS-IP is a packet forwarding technology that is capable of carrying any L3 protocol. This is what the term multi-protocol refers to. MPLS-IP is capable of tunneling L3 packets inside the MPLS-IP network using MPLS labels.

The MPLS-IP label is a fixed 4 byte identifier added to the packet by the ingress router between the data-link layer (Layer2) and the network layer (Layer3) and is used by all routers along the path to switch the packet to its destination without the need for any routing table (Layer3) look-ups. MPLS-IP is considered a **layer 2.5** technology.

The figure below illustrates the structure of the label. One or more labels are pushed on the packet at the ingress router forming a label stack. The first label is called the top label or the transport label; other labels are used by different MPLS applications if needed.

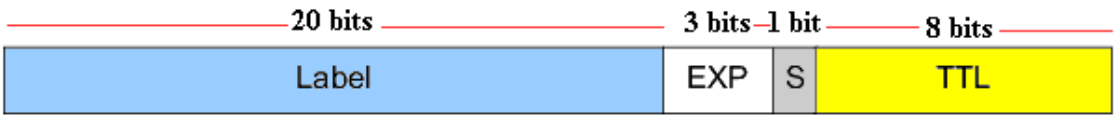


Figure 23: MPLS-IP Label structure

The list below provides basic terminology used in MPLS-IP:

- **Label**: label value, 20 bits
- **EXP**: Experimental bits, Name is changed to Traffic class, 3 bits
- **S**: bottom of stack, 1 bit
- **TTL**: Time to live, 8 bits
- **Label Edge Router (LER)**: Operates at the edge of the MPLS network (ingress/egress) and makes forwarding decisions based on the IP header information of the packet.
- **Label Switch Router (LSR)**: the routers in the middle of the MPLS network which forwards MPLS packets based on label information
- **MPLS a Label Switched Path (LSP)**: is established to carry out the traffic along specified paths between two LERs
- **CE Router**: Customer Edge Router
- **PE Router**: Provider Edge Router
- **P Router**: Provider Router

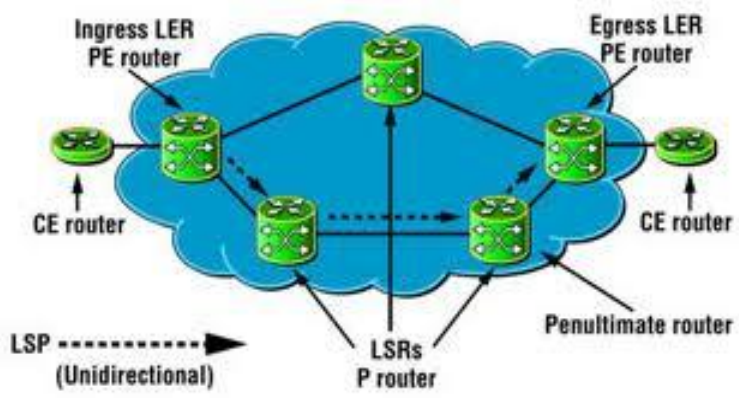


Figure 24: MPLS-IP network example

Benefits of MPLS:

- Layer 2 transport - new standards allow service providers to carry Layer 2 services including Ethernet, Frame Relay and ATM over an IP/MPLS core
- Layer 3 routing occurs only at the edge of the network, and layer 2 switching takes over in the MPLS core
- Integrates layer 2 switching and layer 3 routing by linking the layer 2 infrastructure with layer 3 routing characteristics
- Label switching networking technology that forwards packets over multiple, underlying layer 2 media
- Permit the network routers to exchange packets with a simplified header
- Large scalability, can reach a very complex topology without traffic congestions
- Very high availability when using mesh paths

5.1.4.1 Quality of Service (QoS)

Quality of service (QoS) is defined as the ability of a network to recognize different service requirements of different application and to comply with SLAs negotiated for each of the application services, while attempting to maximize the network resource utilization. QoS is absolutely essential in a multi-service network, in order to meet SLAs of different services and to maximize the network utilization.

With MPLS QoS, there are two approaches to mark traffic for controlling QoS within an MPLS network. That means, when IP traffic enters an LSP tunnel, the Class of Service (CoS) bits in the MPLS header (EXP) are set in one of two ways.

a) EXP-Inferred LSP (E-LSP)

In the first way, queuing information is encoded into the experimental (EXP) field of the MPLS header.

Since the EXP field allows eight different CoS markings, the marking is used as packet's CoS value. Here, different packets might receive different markings depending on their requirements along the path. This approach is referred to as experimental bit inferred label switched paths (E-LSPs), to indicate that QoS information is inferred from the EXP field. Here below an example showing the mapping of IP DiffServ classification with five MPLS classes (Real time, Critical data, Video, bulk and best effort)

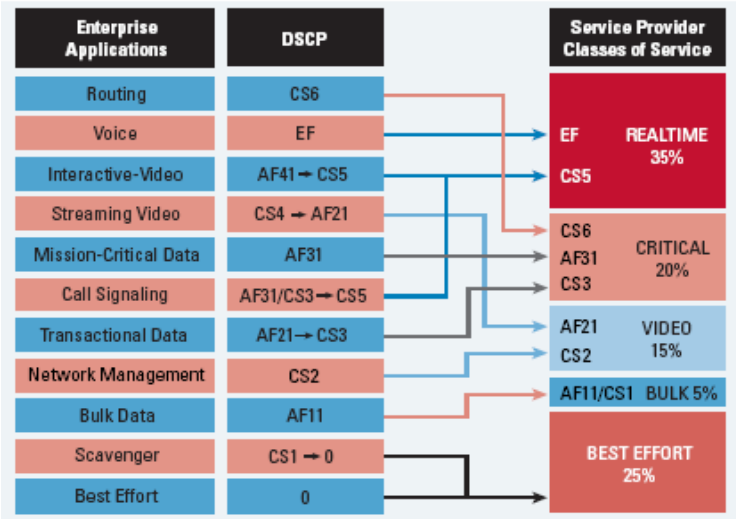


Figure 25: Example of MPLS E-LSP [www.cisco.com]

b) Label-Inferred LSP (L-LSP)

In the second method, the label associated with MPLS packet specifies how a packet should be treated, and all packets entering the LSP will be marked with a fixed CoS value. This means that all packets entering the LSP receive the same class of service. This approach is known as label inferred label switched paths (L-LSPs), to indicate that QoS information is inferred from the MPLS label.

5.1.4.2 Scalability

As mentioned in the introduction to this paragraph, the size of the MPLS-IP label is 20 bits, therefore any MPLS-IP node in the network can supports up to 1 million different services per physical link.

5.1.4.3 Maturity

The IETF formed its MPLS Working Group in January 1997, and protocol specifications began publication a few years later. Moreover, some Telecom suppliers have more than 20 years MPLS-IP history. This provides an important maturity to MPLS-IP comparing with other protocols (e.g. PBB, PBB-TE). Suitability for mission critical traffic is currently not secured.

5.1.4.4 Management

Network Management System for MPLS-IP supports the following features:

- Configuration management (service provisioning etc.)
- Fault management (alarm monitoring etc.)
- Performance management

5.1.4.5 Service types

Metro Ethernet Forum (MEF) has defined three Ethernet services: E-Line, E-LAN & E-Tree.

E-Line is based on point to point Ethernet Connection, this can be used like Circuit Emulation service.

E-LAN is based on multipoint to multipoint topology with more than two users, this topology can be considered like an extended LAN service.

E-Tree is based on single root to multipoint service, this topology is mainly used for multicast service (e.g. IPTV).

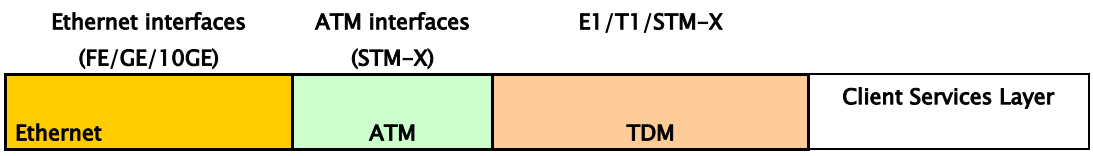
MPLS-IP supports MEF services E-Line/Virtual Lased Line (VLL), E-LAN/Virtual Private LAN Service (VPLS) and E-Tree.

5.1.5 MPLS – Transport profile

Multiprotocol Label Switching - Transport Profile (MPLS-TP) is an extension to IP/MPLS to support the existing traditional transmission models (Time-Division Multiplexing – TDM) and to emulate the 'Pseudo wire-connections' technology.

It is based on Generalized MPLS (GMPLS) and MPLS protocol as defined within the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU-T). The goal is to extend MPLS with "Operation, Administration and Maintenance (OAM)" and emulate the existing transmission models such as SDH/SONET. Circuit-switched services are here emulated using packet-switching with fixed bandwidths with similar requirements as within SDH/SONET:

- Guaranteed QoS.
- Traffic engineering
- Reliability (sub 50ms re-routing)
- Legacy support
- Scalability
- Bi-directional path



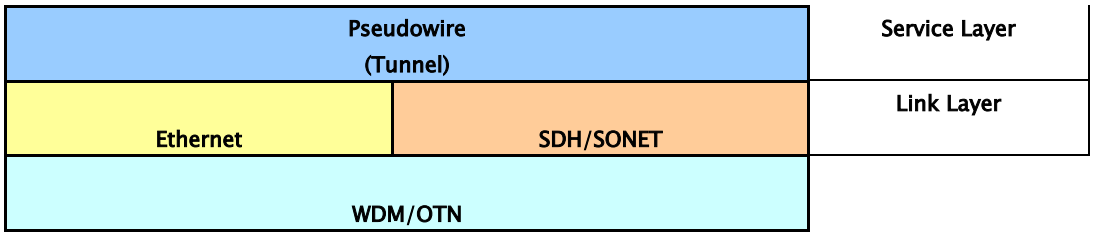
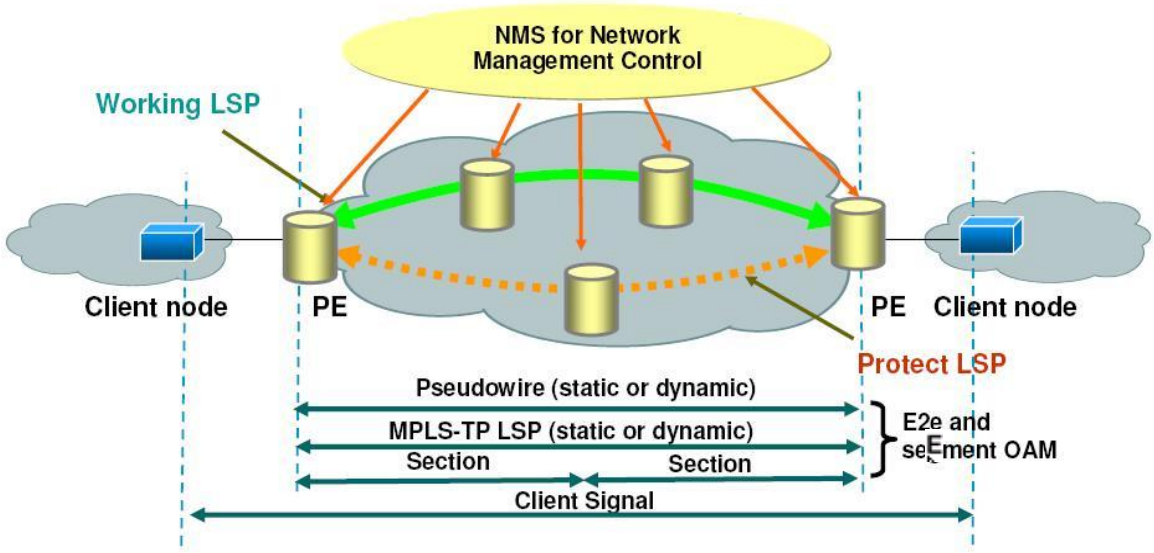


Figure 26: Layer Architecture

MPLS-TP provides thus an End-to-End connection-oriented Pseudo-wire, across different technologies and media. Its implementation is simpler. It defines an extension to MPLS. Non relevant MPLS features are removed.

MPLS-TP focuses on the transport domain and omits the IP-routing complexity. This results in faster learning curve of the network managers.

This technology (at the moment of this brochure writing) is new, moreover its implementations and further technical deployment are still expected at the moment.



.

Figure 27: MPLS-TP network example

Protection Mechanisms

MPLS-TP support different protection mechanisms as in the traditional transmission technologies, for example SDH/SONET.

- Linear Protection:
  - Dedicated 1+1 (2 active paths)
  - Dedicated 1:1 (one standby path)
  - Shared 1:N (One standby path for many active paths)
- Ring Protections

The recovery time is very fast for a packet switching environment. It is for both linear and ring protection is less than 50 ms.

Bi-directional path

MPLS-TP uses always the same path for both the transmit and receive paths. This is also the case with the protected path. This can be interesting for the potential use for tele-protection.

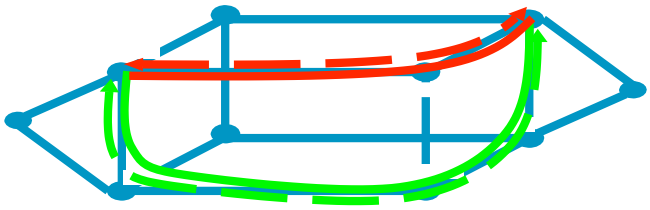


Figure 28: MPLS– TP Protection scheme example

Red: Primary path

Green: Backup path

Benefits of MPLS-TP

MPLS-TP delivers an interesting step forwards in the new technology development:

- Transport technology using Ethernet as Packet/Transport medium
- Transport of different protocols: L2 (Ethernet, FR, ATM etc.) and L3 (IP)
- Delivers Connection oriented services
- Compatible with existing MPLS-IP
- Support for QoS, Guaranteed frame delay, and frame delay variation.
- Supporting high availability (sub 50 ms protection switching)
- Use of the same path (Bi-directional: transit and Receive follow the same path)
- Lower cost (OPEX and CAPEX); you get more Mbit/s per dollar, per port
- Learning curve is faster than the learning curve for MPLS

5.1.5.1 Quality of Service (QoS)

This network as in the TDM environment supports fully guaranteed QoS for all delivered services assuring:

- End-to-End differentiated services (Class of Services)
- Connection oriented
- High reliability

5.1.5.2 Scalability

Like MPLS-IP, MPLS-TP's label size is 20 bits, therefore any MPLS-TP node in the network can supports up to 1 million different services per physical link.

5.1.5.3 Maturity

Most network operators and various equipment manufacturers are investing in this technology. Operators want to use it for service transport and for mobile data backhaul.

Standardization work is still ongoing, specifically in the field of OAM.

As MPLS-TP is a new technology and not deployed at a large scale yet, it is difficult to describe its possible impact on the EPU's. The technology is however very promising.

Some possible applications for the EPU's are:

- Migration form SDH/SONET maintaining a part of this existing SDH/SONET infrastructure
- Implementation of tele-protection because of the similarity of the services of MPLS-TP and SDH/SONET. At the moment is there no information available about this subject

5.1.5.4 Management and Provisioning

Operation, Administration and Maintenance (OAM) are a key component of MPLS-TP technology; this in a similar way as in the traditional TDM-technology. Standardization in the field of OAM for MPLS-TP is however still ongoing. Delivered features:

- Alarm notification
- Failure detection and localization
- Path recovery
- Performance monitoring, including delay and loss monitoring
- Monitoring end-to-end QoS
- Monitoring if the guaranteed frame delay and frame delay variation
- Support of SLA: Bandwidth allocation, Delay variation, Automatic Failure recovery and Packet drop rules

Static provisioning is default by a central Network Management System (NMS). Dynamic provisioning is possible via Control Plane.

5.2 Transport Technology Comparison

The table below compares the main characteristics for each technology. The convergence time values reflect the optimum which can be achieved with the given technology:

Technology	Service	Connection-Oriented	QoS	Legacy Interfaces	Convergence Time
Ethernet	E-LAN	No	Simple (IEEE 802.1p)	No	> 50 ms (RSTP[1]) < 50 ms (proprietary protocols)
Ethernet over SDH	E-Line E-LAN	Yes (for E-Line) No (for E-LAN)	Guaranteed (for E-Line) Simple (IEEE 802.1p for E-LAN)	Yes	50 ms for E-Line > 50 ms (xSTP) for E-LAN

Technology	Service	Connection-Oriented	QoS	Legacy Interfaces	Convergence Time
MPLS- IP	E-Line E-LAN	No	Complex (Traffic Engineering, DiffServ over MPLS[8])	Yes	50 ms (FRR)
MPLS-TP	E-Line E-LAN	Yes	Complex (Traffic Engineering, DiffServ over MPLS)	Yes	50 ms (FRR-TP)
PBB	E-LAN	No	Basic (IEEE 802.1p)	No	> 50 ms (xSTP)
PBB-TE	E-Line	Yes	Complex (Traffic Engineering)	No[9]	50 ms
Layer 3 routing	N.A.	No	Complex DiffServ	Yes	> 1 sec

Table 6: Transport Technology Comparison

5.3 Cyber Security considerations

5.3.1 Overview

Physical security is out of scope of this document however from the IP communications perspective it is worth mentioning that video surveillance applications are becoming more popular in substation applications. Many utility companies install large numbers of video cameras to monitor the assets and have online real time access to the video streams they generate. Apart from classical monitoring and detection of undesired presence some of these systems implement sophisticated features such as image processing algorithms that may predict a potential faulty situation in a high voltage equipment. The company may chose native IP or analogue cameras, in the later case integration into IP network will require specialized encoders. Depending on a variety of parameters such as encoding algorithm, image quality, number of frames per second, etc. a single video camera may generate very high data rate (higher than 1Mbps) so it is important to specify all these parameters to properly design the network.

Cyber security requirements shall specify all means of protecting electronic access to electrical grid substations. Basic requirements may include that remote access have to be protected by encryption, VPNs, IDS (Intrusion Detection System), firewalls, Application Gateway Services and passwords.

Over the last several years, it has become apparent that better tracking and monitoring of access to the substation control network is needed. In the United States, the NERC-CIP set of standards provide a cyber-security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. NERC-CIP mandates that provide guidance and requirements for electric utilities to become more accountable and secure. Who accesses, for how long and to what end devices was access granted. These are needed for identifying who did what and when and places the information readily into the administrator's hands.

[1] Convergence time in an optimized implementation of RSTP is in the range of 5 ms per hop, in case of a maximum size topology allowed by IEEE802.1Q-2005 which is formed by 40 hops the convergence time upon link failure is 200 ms

[8] Diffserv over MPLS allows mapping IP Class of Service with MPLS Class of Service.

[9] Only Ethernet interface is supported; however there is a draft study to support Legacy over PBB-TE.

Application Gateway Services, which can also be referred to as Application Access Management, is a fairly new group of tools and functions which utilize current tools such as Firewalls and Radius or TACACS (Terminal Access Controller Access Control System) authentication and adds additional features that automate the manipulation of Firewalls to allow access based upon a very narrow rules dynamic. The operation description is fairly simple; authenticate the user and laptop/PC, identify the device to be accessed, authenticate the access and punch holes in the Firewall that are assigned to the discrete IP address of the device and the necessary TCP/UDP port numbers. Firewall rules are automatically created that correspond to the required functions, the technician does his work and then logs out of the access manager. The access manager then removes the rules it just created, thereby removing any holes that could have been left open to allow unauthorized access. The network is then locked down again from the outside until another request comes in for access.

Some utilities may have requirement that the operational network is isolated from the service network and remote access to devices in the operational network is only possible from dedicated terminals that lack any physical ports like USB interfaces, CD-ROMs etc. The only way to copy data to these specialized terminals is via dedicated access management servers.

5.3.2 Network security segmentation

A utility has many different services and applications running in their environment based on IP communication. Many applications that previously did not use IP are now being converted to use IP based communication. These services and applications have different demands for the underlying infrastructure and the network design, based on their needs for quality, resources, response times, jitter etc.

One important issue is the security needs that the services and applications are placing on the network design. A utility may have IP based services and applications like SCADA (IEC-60870-104, IEC 61850), Inter Control Centre traffic (ELCOM-90, TASE.1 or TASE.2), telephony traffic (Voice over IP), video surveillance, unified communication and other administrative applications. These applications have different needs for security and may have to be separated from each other by some sort of security measure. For example, a utility does not want SCADA based traffic to float in the same network (segment) as the administrative based traffic because that could expose this traffic to a huge amount of users.

There should be some sort of classification of the different types of services and applications used in the environment based on the consequences of a security breach and the importance of the service. If there is a security breach on the SCADA system this could potentially have very serious consequences for the utility. Usually one classifies the services and applications in different security zones where the services with the highest consequence of a potential security breach and highest importance are placed in the zone with the highest security protection. Traffic between each zone have to pass some sort of security measure like firewalls, IDS/IPS etc. to check if the traffic should be allowed to pass from one zone to the other based on the security policy implemented at the utility.

Figure 29 gives an example of how the security zone model is layered from the unprotected Zone 0 (Internet) to the highly protected critical systems in Zone 4. In the zone model below, DMZ Zones (Zone 1 External DMZ and Zone 3 Internal DMZ) have been implemented, to increase the security in Zone 2 and Zone 4. In the zone model one could impose rules like:

- Applications and systems are not permitted to initiate direct connections from a zone that is 2 levels below the zone one should reach. All traffic should be terminated in a DMZ through terminal servers, replicated servers etc. As an example all traffic from the administrative network should go through a server in Zone 3 to reach resources in Zone 4. In this way should the resources in Zone 4 get a higher level of protection against attacks from sources from a lower security zone

- Applications and systems are permitted to initiate direct connections, where the destination end point is in a security domain that is no more than two levels below the source end point

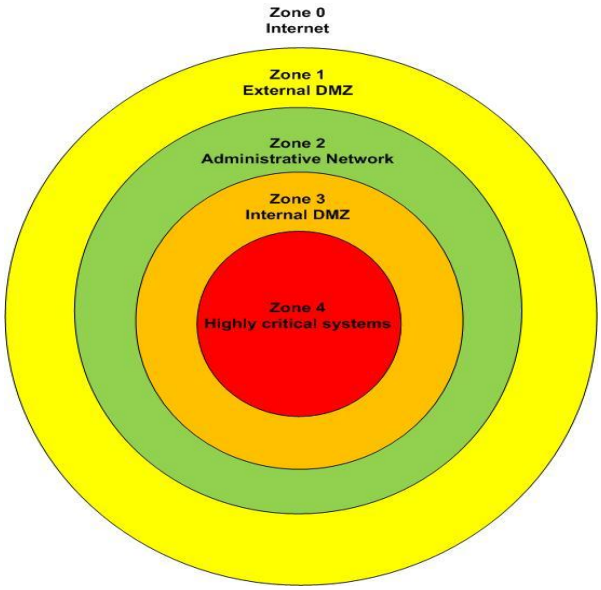


Figure 29: Security Zones

In a schematic example of how this could be implemented at a utility is shown. Traffic initiated from the Internet goes through servers in the external DMZ, and traffic initiated from the enterprise Zone 2 can access resources in Zone 0 directly if the traffic is allowed by the security measures between the zones. Services and systems in Zone 4 are not allowed to access resources in Zone 0 directly. As the figure indicates, this zone based structure also applies to sub stations. The security appliances between security zones are usually placed at central locations (control centres), so there should be no direct connections between the different security zones at a substation. This security structure has a huge impact on how to design the IP network, both centrally, and at the substations.

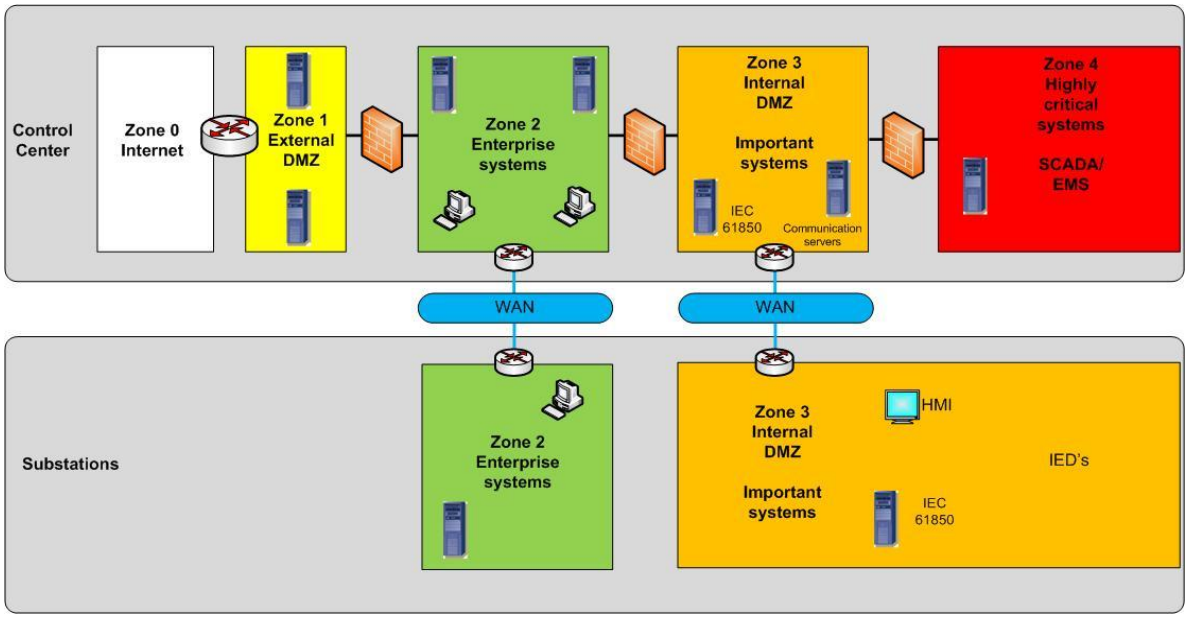


Figure 30: Security Zones Example

To keep this separation between different security zones and to have further internal separation in a security zone (sub zone) due to other reasons, one has to separate the IP based communication into separate networks. This separation can be done by building networks with dedicated equipment (separate routers and switches for each network) or by using some sort of virtual separation (Virtual Private Networks) like MPLS/VPN, IPSec, VRF Lite, VPLS etc. A combination of the two could also be an option where one network has separate equipment and other networks use the same physical equipment with some sort of logical separation of the traffic.

A possible way of implementing security zone separation is to create a multi layered network. Network security is more efficient when it is layer-distributed. That means any hacker needs more time and more work to penetrate this kind of secured network. A firewall is a very good security element, but this is not enough to protect a network, this layer of security must be double-acting by another security layer. Every security layer must be implemented independent one of the others. One single layer compromised does not mean that entire network is compromised.

References on the subject of security zones/domains from other Cigre reports are:

Cigre WG D2.24 EMS Architectures for the 21st Century (Chaper 10)

Cigre WG D2.22 Treatment of Information Security for Electric power Utilities

Cigre WG D2.31 Security architecture principles for digital systems in Electric Power Utilities

5.3.3 Security rules

8 Security Ground Rules

1. Access Control
   - Ensures access by authorized personnel & devices only
   - Protects against unauthorized use of network resources

   Mechanisms:
   - Simple log-in/password

- Access Control Lists (ACL)
- Role Based Access Control provides different levels of access control to guarantee that only authorized individuals & devices can only access information

2. Authentication
   - Confirms the identity of communicating entities (e.g., end-users, network elements)
   - Ensures validity of claimed entities
   - Provide assurance that an entity is not masquerading
3. Non-repudiation
   - Prevents an individual or entity denying having performed an action
   - This will ensure the availability of documentation in case of an incident.
   - Logs
   - Role based access control
4. Data Confidentiality
   - Protects data from unauthorized disclosure
   - Ensures data content cannot be understood by unauthenticated entities

   Mechanisms
   - Encryption (3DES, AES)
   - Access control lists
5. Communication Security
   - Ensures information only flows between the authorized end points
   - Ensures information is not diverted or intercepted as it flows between these end points

   Mechanisms
   - VPNs (IPSec)
   - MPLS tunnels
6. Data Integrity:
   - Ensures the correctness or accuracy of information
   - Ensures data is protected from unauthorized modification, deletion, creation & replication
   - Provides an indication that this has occurred

   Mechanisms:
   - IPSec HMACs (e.g. MD5, SHA-1)
   - Cyclic redundancy checks
7. Availability:
   - Ensures no denial of authorized access to network elements, stored information, information flows, services, application
   - Disaster recovery solutions are included in this category

   Mechanisms:
   - Redundancy & back-up
   - Business continuity

- Services with SLAs

8. Privacy:
   - Provides protection of information that might be derived from network activities

   Mechanisms:
   - Encryption of IP headers (IPSec VPNs)

5.4 IEC 61850 beyond the substation perimeter

When IEC 61850 was first released, it was intended for information exchange between IEDs within the substation perimeter and therefore was focused on the substation automation systems. Control Centre to Substation Communications and the communication between substations in such cases relied on the use of specific telecontrol and teleprotection protocols such as DNP 3.0, IEC 60870-5-101 or IEC 60870-5-104, G.703 or proprietary solutions.

Since the release of the first edition of IEC 61850, many IEC 61850 based substation automation (SA) systems have been successfully implemented worldwide. It was clear from the very beginning that the concepts of IEC 61850 could also be applied to applications outside the substation. Such applications that go beyond the substation perimeter can be divided into two levels: Substation to Substation communication and Substation to Control Center communication.

5.4.1 Substation to Substation Communication

Because both the data and the communication in the SA systems are standardized, it should be relatively easy to interconnect (several of) these systems. Interconnecting different SA systems opens up possibilities for new functionality, such as:

- Automated transfer tripping
- Distance protection
- Differential protection
- Automated fault locator systems
- Wide area protection
- Wide area control
- Remedial action schemes
- Synchrophasors
- Etc.

When interconnecting two different SA systems, the following should be taken into account:

- Interoperability
- Communication delays
- Security

These issues are addressed in technical report IEC 61850-90-1 “Use of IEC 61850 for the communication between substations”. This report combines relevant information for substation to substation communication from IEC 61850 and related standards and reports.

The current mechanism for inter-IED communication within the same substation relies on Multicast over layer 2 (Ethernet), and up to now most of the substation networks are built as layer 2 networks (switched Ethernet) within the substations, with layer 3 connectivity from the substation to the control centre (i.e. router at the edge of the substation). This will imply that if low latency connectivity between substations is required, either

they will have to be linked at layer 2, or the necessary inter-substation data will be carried over layer 3 (IP) but with special latency control.

The goal of linking substations with IEC 61850 is to be able to exchange information for teleprotection and other applications. However, if there were concerns on the reliability of layer 2 networks and devices for inter-substation communication, in this case the network grows in size, complexity, number of services supported, and several different architectures are available. Thus network reliability (as a whole system, as individual network devices, and as network design) is a critical issue, dependent on many parameters.

5.4.2 Substation to Control Center Communication

For the communication from substations to the control center many utilities are using standard or proprietary telecontrol protocols which will not disappear over night even though newer, more advanced solutions such as the Common Information Model (CIM) exist which use MMS over TCP/IP to communicate with the outside world. So when applying IEC 61850 in substation one of the most common requirements is for the communication with the control center to have some kind of gateway from IEC 61850 to the existing telecontrol protocols such as DNP 3.0, IEC 60870-5-101 or IEC 60870-5-104. This is why IEC TC57 has developed IEC 61850-80-1 “Guideline to exchange information from a CDC based data model using IEC 60870-5-101/104”.

The idea behind this guideline is to define a standardized solution for a gateway between these IEC standards. It includes a mapping architecture in order to map MMS services and data objects from IEC 61850 to their counterparts in IEC 60870-5-101/104. The technical specification also includes a conceptual architecture of the gateway. The conceptual design of the gateway is shown in Figure 31.

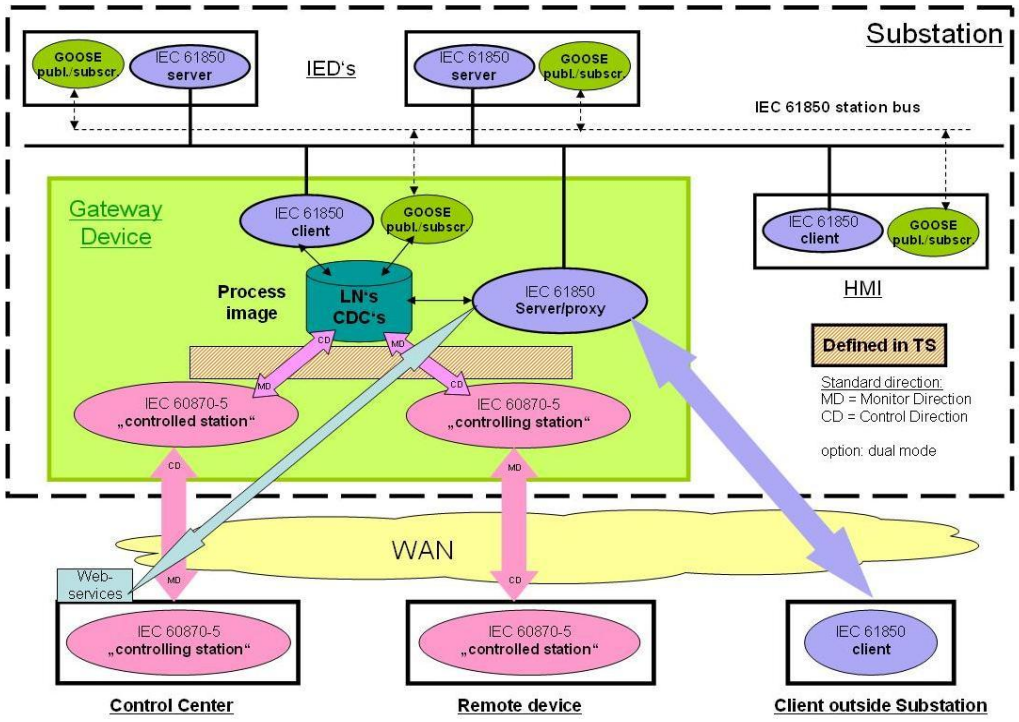


Figure 31: Conceptual gateway IEC 61850-IEC60870-5-101/104

Although the technical specification allows for the use of standard gateways, the end goal for the communication between control center and substation is a seamless access to all information without the use of gateways. This is why 61850-90-2: "Use of IEC 61850 for the communication between control centers and substations" is being developed within IEC TC57.

Two approaches have been defined where the control center has access to the model as defined in IEC 61850:

- Through a proxy and/or with direct access to the IED
- Through the creation of a “control center view” by the substation gateway

Both approaches have the advantage that the control center is decoupled from the physical substation implementation. This not only alleviates security risks, it also allows for a more flexible solution. If the information for the control center needs to be modified only one interface needs to be changed in the gateway and the physical infrastructure of the substation remains unaltered.

6 Case Studies

This chapter describes case studies from utilities around the world that have implemented communication architectures for IP-based Substation Applications. The case studies described in this chapter are not intended to reflect the best possible communication architectures are meant to provide insight into why certain implementations were chosen in specific situations. All case studies have been created from April to August 2010.

The case studies are divided in the following sections:

Introduction
This section describes what work was done and why the work was done.

Description of the communication system
This section describes the communication system that was developed.

Characteristics and requirements of the communication system
This section describes the utilities requirements for the characteristics and other requirements for the communication network.

Work plan to realize the needed system characteristics and requirement
This section describes the utilities work plan to realize the required system characteristics and other requirements.

Research and investigations used to define the communication system used
This section describes how the utility came to the decision to use the chosen communication system.

Applications used and their characteristics
This section describes the applications that are used in the communication system and what their characteristics are.

Operational and responsibility experiences (use of in/out source)
This section describes the utility's operational experiences with the communication. When applicable, it also describes what part(s) of the communication network has been outsourced.

Conclusions and recommendations
This section describes the conclusions that the utility has drawn from the implementation and use of the communication network. This section also describes the utility's recommendations for other utilities that are going to go through a similar process.

6.1 Case Study Energinet.dk

The task we set out to complete was to IP enable the 400 kV substations in Energinet.dk electrical transmission grid. The driver for the project was the implementation of a new SCADA system and the strategic choice to move RTU communication to the IEC 60870-5-104 protocol between the SCADA main system and the RTU in the substation.

6.1.1 Description of the communication system

The communication system is a routed system with SDH as the main transmission system. Hence it consists of optical fibers, SDH multiplexers, IP Routers and ethernet switches.

At that point Energinet.dk already had a network of multiplexers on all the stations involved, so it was given that it should be used. Then we just needed to add a layer 3 functionallity on top in the form of routers. See Figure 32 for the router concept.

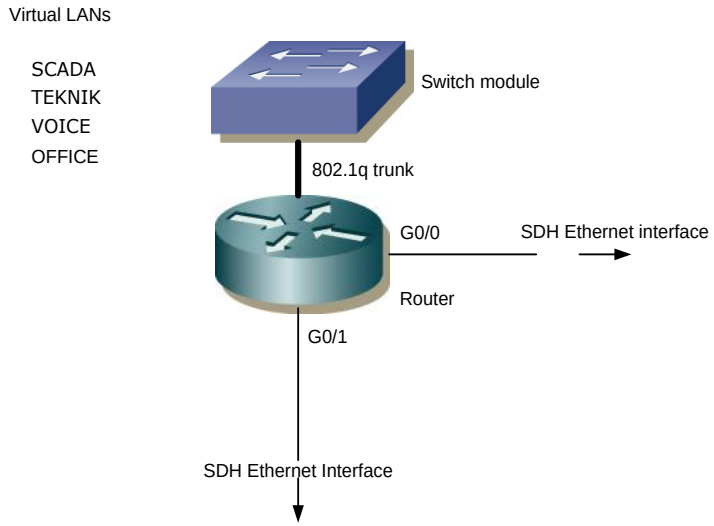


Figure 32: Router Concept

VLANs and the number of Ethernet ports provided in the substation are shown in the following table.

VLAN	Name	Comment
100	SCADA	VRF – ”scada” 5 ports
101	OFFICE	VRF – ”office” 17 ports
102	VOICE	VRF – ”voip” 10 ports
103	TEKNIK	VRF – ”teknik” 15 ports
104	MANAGEMENT	

105	Spare	Not implemented

Table 7: Number of Ethernet ports per VLAN

6.1.2 Characteristics and requirements of the communication system

From the beginning we wanted this network to have some specific characteristics:

- High fault tolerance
- Support for QoS
- Support for multiple networks in the substation
- Have the ability to scale

High fault tolerance was achieved by letting each substation have two WAN links and letting a routing protocol select the best path through the network. We chose the routing protocol OSPF since it is an open protocol which can be trimmed for relatively fast convergence. Other protocols that were considered are IS-IS and EIGRP. EIGRP is a Cisco propriety protocol and hence not open. IS-IS was a serious candidate and just as good as OSPF but since the network engineers had more experience with OSPF it was preferred. Ideally we wanted a hardened and rugged router made to operate in an unmanned and harsh environment. This proved difficult to archive with the products on the market at that time. So we ended up selecting a "not so rugged" router with a redundant power supply. To increase the availability of the router solution it is offered as a one router configuration or a two router configuration on the substation level. See Figure 33 for the two router configuration.

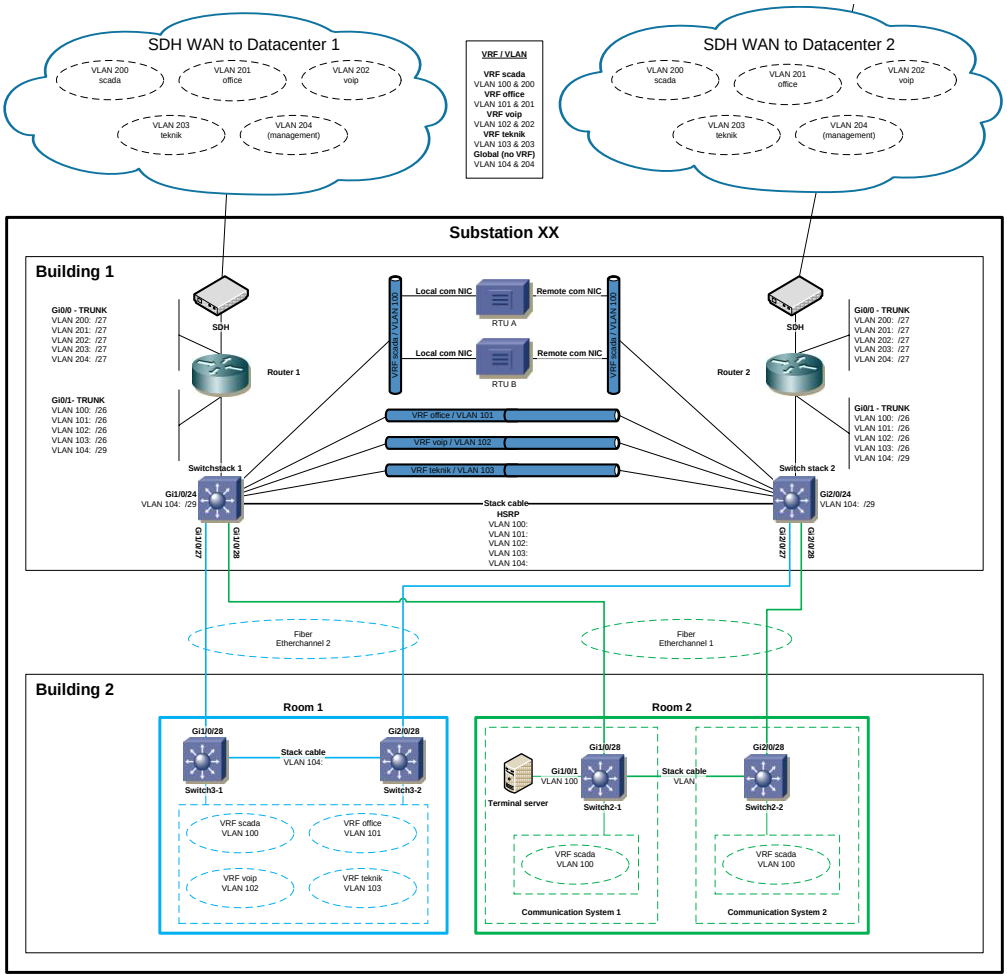


Figure 33: Two router configuration

6.1.3 Work plan to realize the needed system characteristics and requirements

The process of gathering requirements and working with constraints was the first step. Some requirements were already given to us since our SCADA project required support for the IEC 60870-5-104 protocol. Getting other requirements meant interviewing relevant technical personnel as well as the management to uncover their needs.

It was evident that it was very difficult for these people to provide meaningful requirements since most of them did not have any idea of what they might want to put on a network like this in the future. So the result was quite meager at that time. Later, when it became obvious to everybody what such a network could be used for many ideas came crawling out of the box. Recommendation: leave space for growth.

The next task was to provision and compile the following documentation:

- Executive summary
- Design requirements
- Design solution
- Network diagram

We experienced some resistance against the network design. Some resistance came from respected and experienced engineers within the organization.

They would typically argue something like this:

- It is unsafe to run different types of traffic in the same network.
- SCADA traffic will suffer packet loss because other traffic will take up the whole bandwidth.

This called for a process where the project involved higher management to be ambassador for the new technology and several meetings where the design details could be questioned, explained and discussed hence bringing comfort to those who were insecure of the technology.

6.1.4 Research and investigations used to define the communication system used

EM resilience. Since our preferred router was a Cisco router we asked Cisco to document any compliance to any EMC standards. It turned out that it was difficult to obtain such information. We were curious about how the router would withstand strong electromagnetic fields such as those found in a high voltage substation. This led us to conduct our own EM test on the router. Exposing the router to increasing bursts of EM fields while forwarding IP packets, we observed its behavior. It turned out that the packet traffic became slower and slower when the size of the EM field increased. We could not make the router stop, restart or shutdown and we considered this behavior to be satisfactory.

Lab test. Then we conducted a lab test with a prototype of the system. Simulating the WAN links it was verified that the router and the routing protocol performed as expected. The lab test was successful and gave valuable input for timer settings and what to expect from the real system.

Pilot test.

After completing the lab test is was time for a pilot test involving the following steps:

1) Specify and build the Pilot configuration
2) Develop a test plan
3) Conduct the test and evaluate the results

The pilot test configuration involved two substations with redundant RTU configuration. See Figure 34.

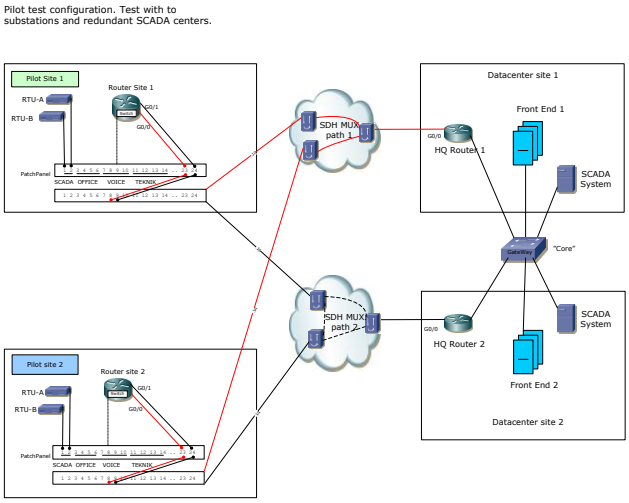


Figure 34: Pilot test configuration

The Pilot test was successful hence the next task was to plan the full scale build and implementation. Since we tested well in the Pilot test there were no technical surprises with the design when it was rolled out full scale.

6.1.5 Applications used and their characteristics

The following applications are available in the substation:

- SCADA (IEC 104)
- Voice
- Protection relay logs
- CCTV
- Office applications, mail and file access
- Building security
- Phasor measurement unit

Vlan	Name	Bandwidth	Type
200	SCADA	2Mb/s	Guaranteed
201	OFFICE	20Mb/s 10	Best Effort
202	VOICE	2Mb/s	Guaranteed
203	TEKNIK	2Mb/s	Best Effort
204	MANAGEMENT	2Mb/s	Best Effort
205	Spare	20Mb/s	Best Effort

Table 8: Bandwidth assignment

[10] Note that the bandwidth for the Office network is a shared bandwidth. 8 stations share this BW.

6.1.6 Operational and responsibility experiences (use of in/out source)

At the moment the network has been in operation for almost two years.

The network is monitored with HP Node manager and can be polled for status and send SNMP traps. In this time we have seen two malfunctions in the system. One fault was a failing system board in a router and the other was a faulty fan module.

6.1.7 Conclusions and recommendations

- Gathering requirements may not lead you to the right set of requirements alone.
- Add common sense and room for growth if you have the budget.
- Develop the IP plan in the beginning of the project. This, because you will be with this plan for many years to come and users will be needing IP addresses early also. Test the IP plan for scalability.
- Spend time developing a good test plan. The knowledge provided by this is your future baseline.
- Spend time developing a security concept. It will be your problem in the future.

6.2 Case Study TenneT

TenneT is Europe's first cross-border grid operator for electricity. With approximately 20,000 kilometres of (extra) high voltage lines and 35 million end users in the Netherlands and Germany we rank among the top five grid operators in Europe. Our focus is to develop a Northwest European energy market and to integrate renewable energy.

6.2.1 Description of the communication system

The IP networks are components of the TenneT Telecommunication system. The IP networks are layer 3 networks whereby the SDH network delivers the serial communication lines to routers and layer 2 networks whereby Ethernet interfaces will be delivered over SDH.

For each IP application there is a separate IP network in the substation, between substations and central offices and between control centers, Some IP applications share the Ethernet and some don't for this moment.

There are three types of IP networks between substation and central office:

- Office Automation network, this IP network gives access to office application software and also gives access to the EMS. On substation level it is possible to consult the EMS for status and alarm information. It is not possible to switch disconnecters and circuit breakers
- PV-access network, this IP network facilitates the communication between Energy Suppliers in the Netherlands
- Security, camera's, building security etc. This is a pilot project in several substations

Communication between TSO's and DSO's on Control Center level

- ICCP network

IP Communication only substation level

- Disturbance recording; On substation level IP. Communication between substation level and central office analogue
- Substation Control System IEC 60870-5-104 (only in branch house). Outside the branch houses the communication is serial IEC 60870-5-101

IP Communication on control center level

- Voice over IP. The system is not operational yet and we expect it to be operational in September 2010. At this moment there are some problems in the redundancy of the network. If there is an outage of one LAN segment the IP Phones don't work properly. Figure 1 t shows a schematic view of the network topology

When the system is in operation, we will think about introducing voice over IP in the substation in combination with a private GSM network on substation level (pico cells).

6.2.2 Characteristics and requirements of the communication system

This paragraph only describes the characteristics and requirements of the Voice over IP network. There are many requirements for Voice over IP networks, Quality of Services requirements but also security requirements. We need a fully redundant IP Telephony System for telephony communication with the substations. See figure Figure 35. In case of a problem in one of the LAN segments (e.g. because of a broadcast storm) all telephone functions from the disturbed LAN segment should be taken over by healthy LAN segments.

Some important QoS requirements:

- Loss of packets < 3% packet loss ratio
- Delay of packets < 150 ms
- Jitter < 1ms
- Echo's
- Codec ITU-T G.711
- Relevant ITU-T recommendations

Some security requirements:

- Using firewalls between Voice over IP network and other kinds of networks;
- Security of MAC addresses
- No possibility to tap phone calls
- Encryption

The figure below shows the system architecture:

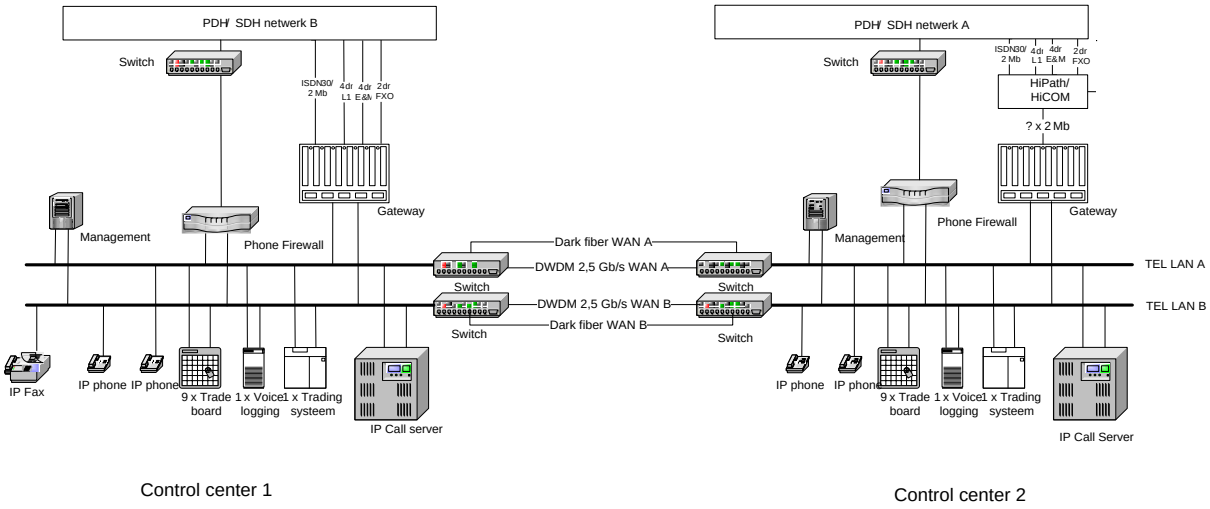


Figure 35: System architecture

6.2.3 Work plan to realize the needed system characteristics and requirements

This paragraph only describes the voice over IP system.

We started to think about Voice over IP three years ago for replacing an old trading system by introducing a new telephone system for one of our control center locations. The first step was to make a choice between traditional telephony and Voice over IP. The telephone market is growing for Voice over IP and shrinking for traditional telephony so the choice was made for Voice over IP. Also interviews with business people and technical people led us to choose for Voice of IP.

Arguments to choose for Voice over IP:

- Shrinking "traditional" telephony market
- Opportunity to remove approximately twenty old public automatic branch exchanges
- Online monitoring status IP Phones and connections
- Integration office automation with voice over IP

The next step was to make a design and requirements, in figure 1 you can find the design of the network which was enclosed with our specification.

Documentation and tools

For engineering we use ITU-T recommendations for the typical non-high voltage applications on IP, such as Voice over IP and office automation etc. For typical high voltage applications, we use IEC standards and also ITU-T recommendations. Experience from other companies and technical people are very important to make a good set of specifications.To control the typical non-high voltage networks with switches and routers we use the program HP Openview. Local switches for Disturbance recording and substation automation systems don't use specific application software on control center level. These switches are not monitored online.

6.2.4 Research and investigations used to define the communication system used

Probably next year we start a study to investigate the possibilities of one type of interface in the substations on telecom transmission side for all high voltage applications such as substation automation and protection. Methods which will be used are:

- literature research, Cigre papers, IEC standards, ITU-T recommendations
- investigate experience from other TSO's and DSO's
- investigate experiences from telecommunication / network suppliers
- investigate experiences from suppliers which delivers protection relays and substation automation equipment
- research possibilities telecom communication equipment and network equipment

6.2.5 Applications used and their characteristics

Office automation network:

- Three 2 Mb/s rings with routers and serial telecommunication lines over SDH approximately 9 substations per ring
- Several point – point connections with leased lines between substation and office location

PV access network:

- Two fully redundant 8 Mb/s Ethernet rings over SDH with five substations

ICCP network

- ICCP network between DSO's and TenneT
- For the communication with between TenneT and each DSO there is a separate 2 Mb/s ring with routers and serial telecommunication lines over SDH

Voice over IP network

- Two fully redundant 100 Mb/s Ethernet (figure 1), between the control centers dark fiber and 2,5 Gb/s Ethernet interface over DWDM directly coupled to the switches
- Capacity of the Ethernet rings to the substations must be defined

Disturbance recording substation on substation level

- 100 Mb/s Ethernet. No redundancy

Substation automation on substation level

- 100 Mb/s Ethernet. No redundancy.

6.2.6 Operational and responsibility experiences (use of in/out source)

Voice over IP system

Our IP Telephony System is not operational yet, the factory acceptance tests are already passed with remarks. Site acceptance tests will be started if the remarks from the FAT are solved. The major problem to be solved for SAT is to maintain all specified basic telephone functionalities in case of a failure in one of the LAN segments.

All other IP communication networks

These IP communication networks are stable and work correctly.

6.2.7 Conclusions and recommendations

In case of the Voice over IP system, we had several problems during the project with redundancy on network level but also on application level. In our opinion is the energy market with his strong requirements for telephony suppliers a nice market and is hard to fill in the requirements of redundancy. Redundancy concepts/requirements used in industrial automation networks are hard to realize in Voice over IP networks.

Remmendations:

- Spend time on the design of the network, especially concepts for redundancy
- Make a good test plan
- Test the network and applications in a non-operational situation
- Specify how the components must react during failures in the network but also in case of failures in the components themselves

6.3 Case Study REN

REN (Rede Energética Nacional), the Portuguese Transmission System Operator (TSO) responsible for the 400, 220 and 150kV electrical grid and the high pressure natural gas transmission network, owns a private telecommunications network responsible for data and voice services.

The evolution of telecommunication technologies, the demands for communication standards, integration of Information Technologies and the requirement of business continuity and disaster recovery plan, required the evolution of RENs network in terms of bandwidth and unified data telecommunication technology.

Ethernet/IP technology was chosen to fulfill this objective and a nationwide project was developed to implement an IP / MPLS network.

6.3.1 Description of the communication system

The implementation of REN data network, also designated as Security Services Network (SSN), was done in several phases:

- In the first phase the SSN was implemented in 27 electrical substations, 2 Dispatch Centre sites and in the Disaster Recovery Site (DRS)
- In the second phase the SSN was expanded to 32 new substations and to RENs headquarter building
- In the third phase the SSN was expanded to 19 electrical substations and the implementation of an IP network in the gas stations was started
- For new substations the SSN is considered from beginning as a basic telecom / IT requirement.

To implement the SSN some of the base requirements were to have a structured IP address scheme, the availability to implement traffic engineering, quality of service and network scalability in order to integrate future expansions to further sites and services. In order to accommodate all requirements the option was to implement a layer 3 network with layer 2 distribution in each site.

6.3.2 Characteristics and requirements of the communication system

The SSN is based on a MPLS core formed by 7 nodes with the responsibility of routing the different VPNs and to which the access sites are connected. In the access sites the IP/VPNs are terminated and the switching equipment is used for local distribution of Ethernet services in different VLANs.

The core network is based on a “hub and spoke” topology, as shown on Figure 36.

The connections between the core sites are established in layer 1 optical Gigabit Ethernet links (1000-SX) provided by internal transmission platforms based on DWDM technology.

The connections between access layer and core layer are provided by dedicated SDH Ethernet layer 1 links (EoSDH with GFP protocol) from the private telecommunications network.

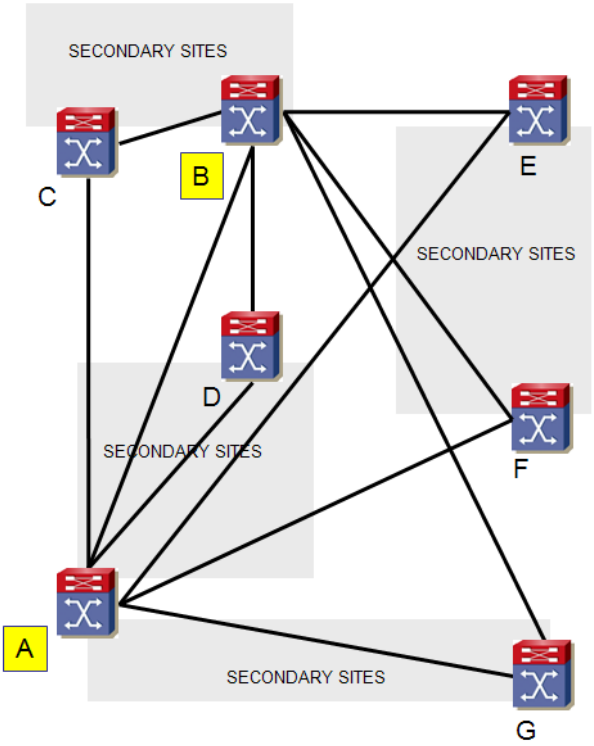


Figure 36: SSN Core Network

The core network was designed considering a geographical distribution of the secondary sites between each node, 4 areas were defined. The main requirement was that each secondary site must have a redundant connection. This means that each secondary site is connected to 2 different core nodes.

In a hierarchical point of view the MPLS network is composed of routers for different functions as shown in Figure 37

- Provider (P) – Equipment with high availability and performance having the responsibility of switching MPLS labels. This equipment does not have clients connected directly
- Provider Edge (PE) – Point of interconnection between core routers and access routers/switch. In this level the VPN/IP is terminated and traffic policing and classification is applied
- Client Edge (CE) – Client router/switch to distribute the different VLANs

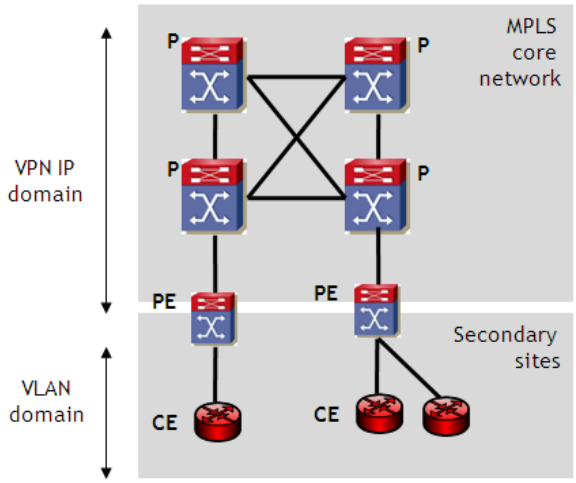


Figure 37: MPLS Network

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

- For IGP (Interior Gateway Protocol) core routing protocol, OSPF (Open Shortest Path First) is used
- For MPLS label distribution, LDP (Label Distribution Protocol) is used
- Between the PEs, MP-BGP (Multi-Protocol Border Gateway Protocol) is used to distribute and announce client routes

In the SSN three distinct layers can be identified (3 tier model), each with specific functions.

- Core: responsible for the packet forwarding, has high availability and specific strategies of QoS. In this layer specific transport technologies are used to provide high availability and performance
- Distribution: interconnection between core and access layers
- Access: provides services to users. Traffic mapping for QoS DiffServ can be done in this layer

Other networks are connected using a Firewall

The main characteristics of this network are:

- Layer 3 VPN MPLS services to provide isolated different types of service
- Layer 2 VLAN in the access and distribution layer. This layer is dedicated to internal services, typically Substation - Substation and Substation - Dispatch Center communication
- Private IP addressing plan dedicated to SSN devices, “10.0.0.0 /8” was used. This network was divided in logical networks (subneting) according to the following specification:

  -Type 1 addresses - clients:
    - Second octet defines the site
    - Third octet defines the client
    - Fourth octet defines the client device/equipment
    - SSN IP address: 10.<site>.<client>.<client equipment>

  -Type 2 addresses - internal IP addresses:
    - Loopback of core sites

  - Subnet for WAN links
  - Connection between core equipment in the same site

- Type 3 addresses - central systems:
  - DMZs for central systems in the datacenter

- Requirements for the network equipment:
  - Core equipment is completely redundant in terms of power, fan system, service modules and software controller cards
  - The access layer equipment is mostly adapted to harsh substation environments by using special switches in strategic points (ruggedized switches)
  - Synchronization for network equipment using Network Time Protocol (NTP). The NTP server (primary and secondary) receives the Stratum 1 clock signal from an atomic clock and spreads to the network
  - Optical Ethernet interfaces were widely used in substations to interconnect equipment between buildings and rooms in order to avoid electromagnetic problems
  - Ethernet electrical interfaces were used inside each room where the active switching equipment is installed. CAT6 SFTP (Shielded Foiled Twisted Pair) cabling was used
- The GbE and Ethernet links are supported by internal DWDM/SDH private telecommunications network. Several requirements were taken into consideration in the plan in order to assure redundancy of communications
  - Path redundancy avoiding routing overlapping.
  - Equipment independencies
  - Shortest path planning
- Security requirements:
  - The different services are supported by dedicated VPN IP in the core / distribution and by VLAN in the access layer. This option provides the required traffic isolation, quality of service schemes and prioritization
  - Centralized Firewall and IDP / IPS to control SSN traffic installed in the Datacenter sites
  - Remote Authentication Dial in User Service (RADIUS) provides the authentication service used to identify users allowed for internal network administration (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)
  - Storage for network logging for maintenance reasons in the System Log (SYSLOG)
  - Creation of DMZs (Demilitarized Zones) for LAN security
  - Multi-level user passwords for network management
  - Extension of password protection capability using SSH/SSL, in order to add encryption of passwords and data as they cross the network
  - Disabled the equipment management through HTTP and Telnet access
  - Utilization of port security, MAC addresses identification, control and port policy in each switch port
- Centralized management systems with real time monitoring and supervision in RENs telecommunication Network Operation Center (NOC)
  - One centralized management system for switching and routing network equipment
  - VoIP management system
  - Video over IP management system

- Firewall management system
- IDS (Intrusion Detection System) /IPS (Intrusion Prevention System) management systems
- RADIUS management system
- Network monitor to monitors availability and usage of the network including the occupation of Gigabit and Ethernet links

- Integration with umbrella supervision system for visualization of alarms in the central telecommunications NOC. This solution also permits the event correlation between SSN events and telecommunication transmission network events, providing an integrated vision of the service

6.3.3 Work plan to realize the needed system characteristics and requirements

The process of implementation of the SSN was divided into phases, actually the 2nd phase is finishing and 3rd phase is being launched.

Typically the process has the following steps:

- Gathering of requirements: internal and external surveys, interviews, and standards review
- Launch a Request of Information (RFI) process
- Laboratory tests, Proof of Concept (PoC)
- Project and specification design
- Launch a Request of Proposal and Quotation (RFP + RFQ) process
- Implementation
- Commissioning and acceptance
- Passage to Ready for Operation Status (RFOS)
- Service migration and configuration
- Service report analysis and key performance indicators evaluation (continuous process)

6.3.4 Research and investigations used to define the communication system used

The construction of the SSN followed one process divided into several phases:

- Benchmark with other utilities
- Market study to evaluate the most promise technologies
- Functional specifications were all technical requisites are detailed

During this process several additional actions are developed in order to gather additional inputs:

- Gathering of requirements: internal and external surveys, interviews with “client” departments.
- Standards review (ITU, IETF, IEC, etc.) and applicable CIGRE documentation
- Consult international opinion makers
- Launch a Request of Information (RFI) process
- Laboratory tests, Proof of Concept (PoC) with the most promise technologies
- Lunch pilot test with real traffic, if the technology is completely new

6.3.5 Applications used and their characteristics

This convergent network provides integrated services of voice, data and video to 36 clients (internal and external), such as:

- SCADA/EMS (RTU communications – protocol 104)
- Power system equipment monitoring and management
- Remote access to protection equipment
- WAN links – LAN interconnections
- IP telephony
- Video and security surveillance
- Video conference
- Management of telecommunication systems

Corporate LAN access.

6.3.6 Operational and responsibility experiences (use of in/out source)

From the point of view of operational activities the actual focus is on outsourcing. For the SSN it was used the following outsourced activities:

- Physical site installation
- Expansions of the network
- Implementation of management system
- Corrective and preventive maintenance
- Daily operation: service configuration, remote maintenance, etc.

The internal team controls the activities of outsourcers and evaluates the service report analysis and key performance indicators in a continuous process basis.

6.3.7 Conclusions and recommendations

The SSN network provides IP VPN services with standardized interfaces and high bandwidth communications between substations and corporate installations, where is present, in order to reduce communications operational costs with high performance.

SSN is being expanded to new points of presence and be used gradually for internal Ethernet/IP services: LAN/WAN implementation, SCADA, utility data applications, access from substation location to corporative applications (ERP, 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.

6.4 Case Study EDP

EDP (Energias de Portugal), The Portuguese DSO, responsible for the 60, 30,15, 10kV an Low Voltage.

EDP owns a fiber optic network of more than 6500km, owns a PDH network with 500 nodes, a SDH network with 100 nodes, and 84 microwave links.

To deliver new generation services in substations, EDP decided to implement a IP network.

In phase 1 implemented 33 nodes without any backbone.

In second phase will implement more 30 nodes over fibber, and will use a IP/MPLs backbone from a Telecom Operator.

6.4.1 Description of the communication system

For the design of first phase of the network, the existing SDH network and the existing fiber optic network were considered in the next topology:

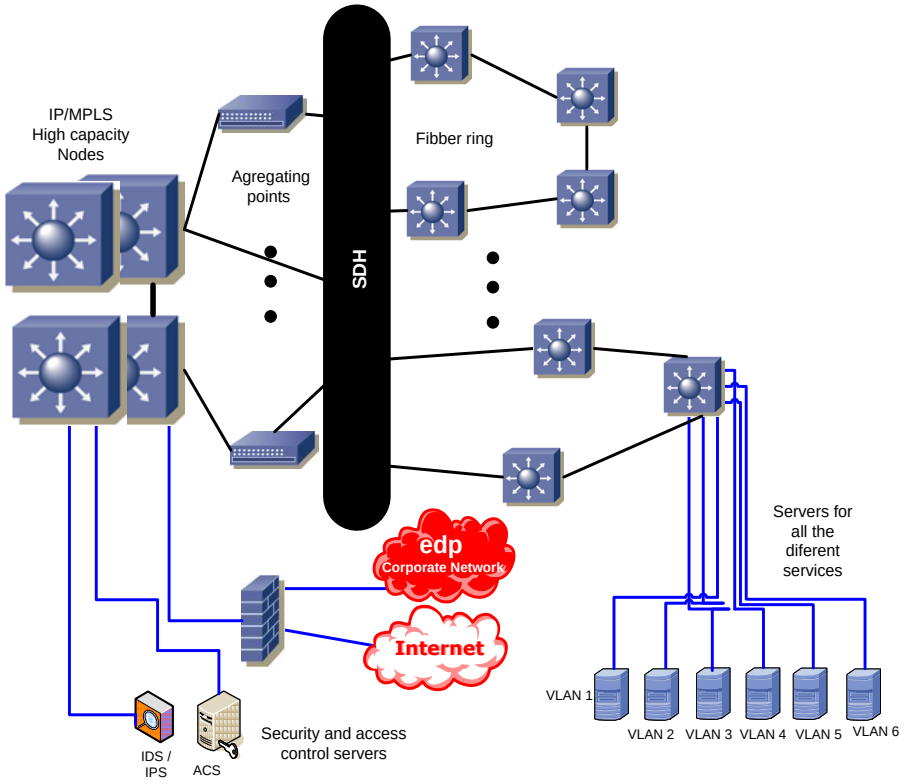


Figure 38: Communication architecture

In Project phase 1 only terminal equipment interconnected by fibber or SDH Circuits was implemented, as we can see in the next design:

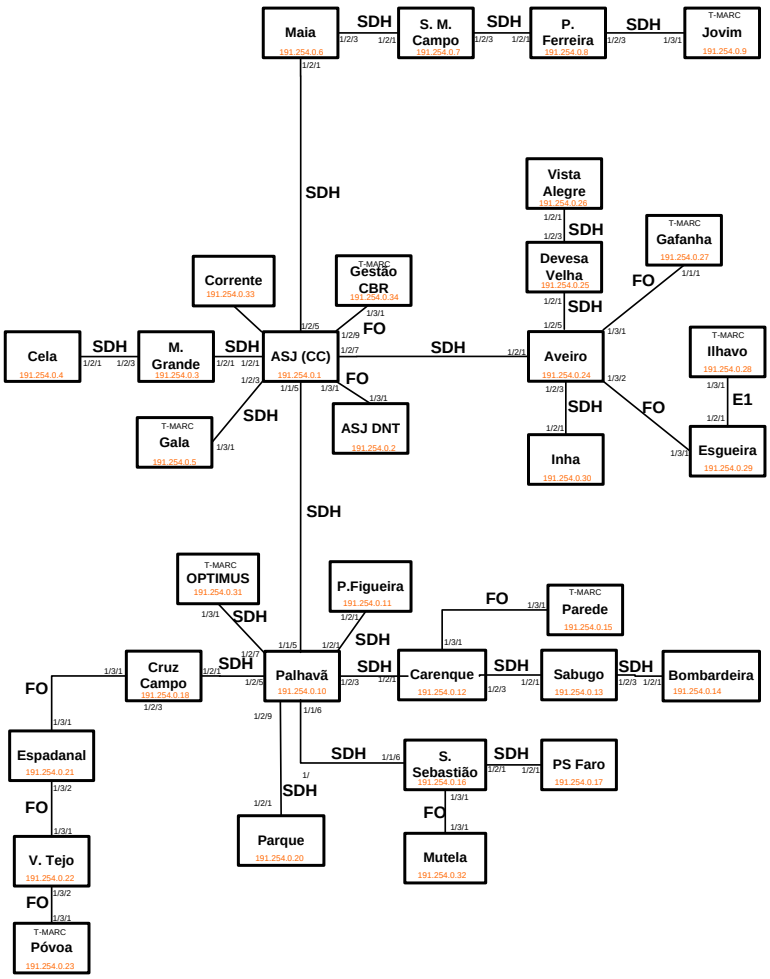


Figure 39: Physical Link Structure

A geographical representation of the network is given here:

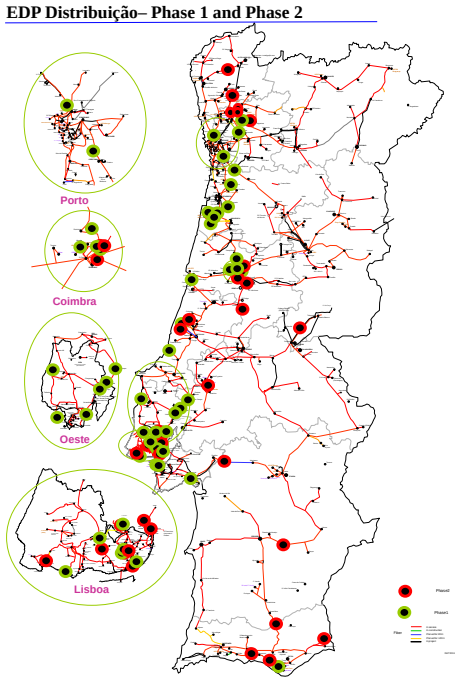


Figure 40: Geographical Network Overview

6.4.2 Characteristics and requirements of the communication system

In the end of second phase the network will interconnect several layer 2 areas over a MPLS backbone interconnect with internet and corporate network.

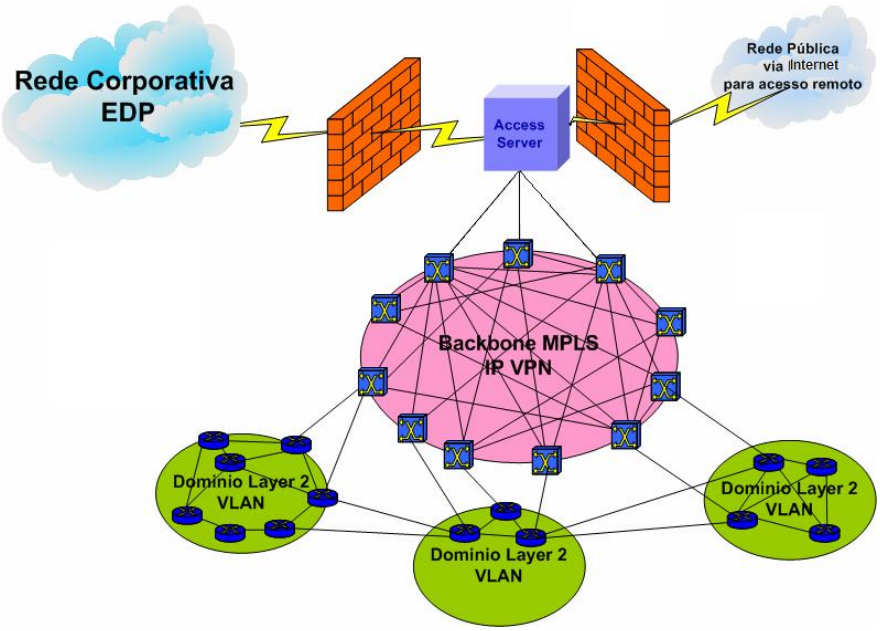


Figure 41: Communication structure

Each layer 2 area will have about 10 substations, and each terminal equipment will have one physical port for each VLAN (IEEE 802.1q).

The network must have 99.99% availability for SCADA application, with the higher priority.

Packet loss < 1%

The reconfiguration of layer 2 area must be <50ms

For security it will be implemented a NAC, IPS and firewall solution.

6.4.3 Work plan to realize the needed system characteristics and requirements

First phase of the project was implemented in 2007.

During 2009 was decided the government model of the Second Phase.

In First quarter of 2011 was launched a RFP(Request for Proposal) for the second Phase.

The implementation of second Phase will be in the last quarter of 2011.

During 2012 EDP Will evaluate this government model, and will decide the roolout of the Third Phase 440 nodes.

6.4.4 Research and investigations used to define the communication system used

For the implementation of the network, were made several meetings with manufactures, and with internal clients, for decide regarding the reference topology, and for understand the needs of each application.

Were made several market studies, concluding that the evolution of the existing and traditional networks (as was made in Phase1) cost almost the same as implementing a new network, and that implementing a network based only in services from an operator it´s always more expensive.

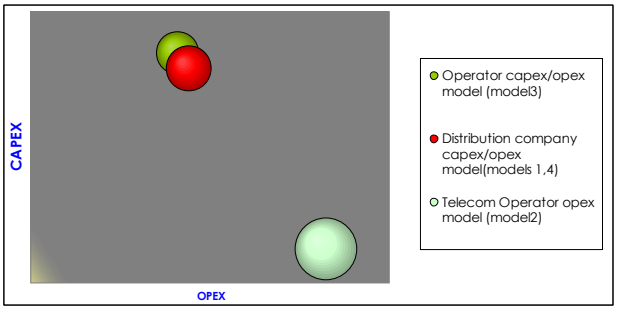


Figure 42: CAPEX/OPEX models

Graphic shows a five years' cost (represented by the ball diameter) versus the CAPEX and OPEX components.

Green ball is the model chosen for phase2, that consider a OPEX/CAPEX implementation, in which, the equipments in the substations are owned by the distribution company and the backbone is from the operator.

The red circle represents the models that consider an OPEX/CAPEX implementation, in which, the entire network is owned by the distribution company, in the scenario of implementing a new network or in the scenario of evolution.

6.4.5 Applications used and their characteristics

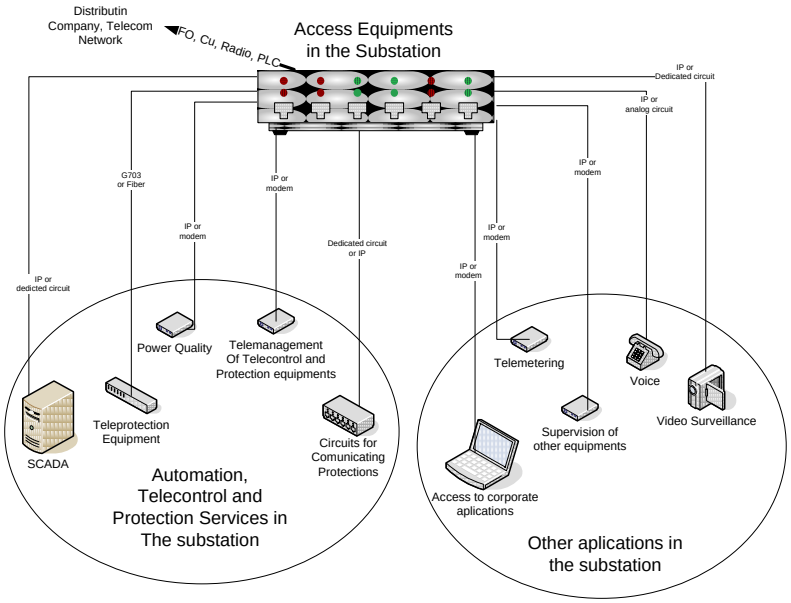


Figure 43: Application structure

Application	Expected Bandwidth
SCADA	100 kbit/s
Telemetering	9.6 kbit/s
Telemanagement of Telecontrol and Protection equipments	1 Mbit/s
Supervision of power DC systems	64 kbit/s
Supervision of telecommunications systems	64 kbit/s
Power Quality	512 kbit/s
Video surveillance	1 Mbit/s
Voice	64 kbit/s
Access to corporate applications	2 Mbit/s

Table 9: Expected bandwidth per application

Each application uses a different physical port in the terminal equipment, and each application uses a different VLAN.

6.4.6 Operational and responsibility experiences (use of in/out source)

At the moment the network has been in operation for 3 years.

The monitoring of the network was integrated by SNMP in an already existing system for the PDH network.

During Phase 1 the SCADA application is used only to interconnect Frontends and mobile operators, there is no RTU using this network.

In Phase 2 there will be SCADA servers and RTU´s using the IEC 60870-5-104 Protocol. In this second phase the operation of the network will be outsourced.

6.4.7 Conclusions and recommendations

With 33 nodes it´s possible to guaranty all the operational applications without having a high level core, and without having access control and security systems, using fixed addresses and layer 2 zones for each application.

For the second phase of the project it´s needed to consider security/access servers.

In the future the decision to take is, if use a backbone from an Telecom operator, build the entire network, or upgrade the existing one.

The reasons that can influence this decision is the type of human resources pretended, the kind of control of all critical processes pretended, and the risks of maintaining the technologic actualization in the backbone.

6.5 Case Study Statnett

Statnett is the national power grid company in Norway and is responsible for all high voltage electricity transmission. Such transmission is mainly from the country's hydroelectric power production plants countrywide.

Statnett has one national and three regional control centers and about 150 substations countrywide. Statnett has, and is continually expanding its own transmission network between its substations and control centres in accordance with requirements set by the regulator.

6.5.1 Description of the communication system

This transmission network mostly consists of radio links and fiber using PDH (Plesiochronous Digital Hierarchy) and Next Generation SDH (Synchronous Digital Hierarchy) technology. With increasing demands on capacity, WDM (Wavelength Division Multiplex) technology will also be implemented on some fiber links.

There is an ongoing change from proprietary and/or dedicated network solutions for tele control traffic towards an open IP network infrastructure. Tele control communication with substations has been carried on point-to-point links using the IEC-60870-5-101 protocol and several proprietary protocols.

In addition, there are increasing demands/needs for information exchange between SCADA networks and enterprise networks, between control centers, between control centers and substations and to/from external partners/vendors. Another challenge is the mutual interdependencies between companies regarding the security level and solutions. This is imposing a set of complex security issues that needs to be addressed and solved by establishing different security domains, and the interface between them.

In Statnett IP communication between control centers and substations will incorporate the following main services:

- Administrative data traffic with accelerating needs for new services and bandwidth.
- Tele control traffic, like IEC-60870-5-104 and IEC 61850
- Inter control-centre communication (ICC) (Elcom-90/TASE.2)
- Access to different maintenance interfaces in the control system (internal and external access)
- Administrative VoIP (Voice over IP) traffic and video
- A second separate VoIP system for power system operation (requirement set by the regulator)
- Video surveillance
- Management of network components (out of band)

Typically a substation will not have the need for all of these services

6.5.2 Characteristics and requirements of the communication system

All of the services mentioned above have different needs for security, flexibility, redundancy, bandwidth, QoS (Quality of Service) and availability that set demands on how to build the data network.

Tele control services demand a high level of availability, and Statnett is therefore building redundancy into the network, fulfilling requirements specified by the regulator. With increasing requirements and new services emerging onto the network, Statnett needs to redesign network infrastructure to cope with security, redundancy, QoS and traffic separation.

One way to address these issues is to keep using any existing IP based data network in the company, and implement some form of network based Virtual Private Network solution to carry the IEC-104 data in a logical separate network for security reasons.

Another approach is to consider building a separate data network for tele control traffic, with separate routers and WAN connections, to minimize the possibility of network outage, thus increasing the security and availability of the network.

Statnett started a project in 2009 with the goal to build a new IP based network infrastructure to all our substations that has the possibility to incorporate all the services mentioned above. This project shall be finalized by the end of 2011. One of the main reasons to start this project is an ongoing SCADA project in Statnett where it is decided that all the communication between the SCADA servers and the RTU's shall use the IEC 60870-5-104 protocol.

6.5.3 Work plan to realize the needed system characteristics and requirements

Within Statnett various aspects of the future overall network design have been considered. One of the main issues has been the possibility to integrate all or some of the different networks mentioned above, into one single integrated physical network. This might be achieved by using some form of network based VPN technology (IPSec, MPLS/VPN) to separate the different services security wise, and by using different QoS mechanisms to achieve acceptable delay, jitter and loss values for the various services. This issue has been the main subject in many working groups prior to the project started in 2009.

Another important work has been to evaluate all existing and upcoming applications/services and evaluate these regarding their specific needs for security, flexibility, redundancy, bandwidth, QoS and availability.

One of the first questions to address was the possibility to integrate the tele control traffic and the administrative traffic to a substation into one physical network. To achieve acceptable separation between the tele control services and the administrative services, different forms of network based VPN technologies were evaluated. In particular, the stability and risk of outage in one physical network were considered, in contrast to two separate networks. The tele control network demands a very high level of security, stability and redundancy compared to the administrative network. Security risks like viruses and denial of service attacks are more likely in the administrative network with many different user groups and connections to Internet. One of the concerns was if instability in the administrative network could influence the stability in the tele control network when using some form of VPN technology on a shared infrastructure. Different VPNs where considered, but the two most relevant technologies in this case were IPSec and MPLS/VPN.

In 2006 it was decided to build two IP networks with separate dedicated routers at the substations for tele control and administrative traffic to minimize the possibility of outage, reduce the complexity of the solution and increase the security. This decision was made mainly due to security reasons, as the tele control traffic is so important that the possibility of service loss on the tele control networks related to the shared infrastructure (denial of service on the shared routers, routing separation problems, bandwidth consumption from viruses, complexity of the VPN, etc.) should be avoided. The downside to this solution is of course increased costs due to the need for more WAN links and routers.

The work also concluded that there was a need to build a separate out of band management network for access to all substations. The purpose of this network is to increase accessibility to various telecom and network equipment in case of emergencies, troubleshooting etc. Increased volumes of IP traffic, services and complexity are placing high demands on the ICT-department, and a separate management network can be an important tool to meet these demands.

The next phase of the work was to decide how to incorporate the other services and networks that Statnett is depending on. One alternative for this was to use VPN in the tele control or administrative network to possibly incorporate other services in these networks. One problem was access to the different maintenance interfaces in the control system. The various user groups that shall have access to these maintenance interfaces are typically situated in the administrative data network, or could be vendors that would like to have access through an Internet connection. The maintenance interfaces are typically placed in a local

process LAN at the substation, and the RTU (Remote Terminal Unit) typically has two other LAN connections (tele control LAN A and tele control LAN B).

Users who need access to different maintenance interfaces should not have access to control LAN A and B for the RTU, and this could be solved by introducing a separate VPN in the tele control network that only gives access to the local process LAN at the substations.

To limit the complexity of VPN protocols in the tele control network, it was decided to use general access lists at the substation and have centralized servers at the main office that all maintenance communication must pass through. Security solutions at the main office will grant the required access rights for the different centralized servers and the general access lists at the substation will prevent cross communication (zone based firewalls on the routers). It is important that the access lists at the substations are as general as possible to prevent errors and keep a simple and similar configuration on the tele control access routers.

A study has also been made considering how to build the new operational IP telephone network. One option was to build a completely new network with separate routers and WAN links as an alternative to incorporating this function into an existing network. Since this IP network needs access to many different power utilities it is not a good idea to incorporate this service into the tele control network or the administrative network. As mentioned earlier, the operational IP telephone network demands very high levels of availability, in fact higher than the tele control network. For this reason, it is not acceptable to incorporate this service into the tele control network, even as a VPN. The study concluded that this service could be incorporated into the ICC network. This network will for this reason be expanded to include all the necessary substations that the IP telephone network needs to access, thus avoiding building a separate IP telephone network. The ICC network needs to be configured with QoS tools to manage bandwidth, delay, jitter and packet loss for the IP telephony packets, but there is so far no security reason for implementing VPN functionality into this network. At a later stage a separation of the ICC and the telephony traffic in this network will also be considered with the use of VPN to simplify routing issues, security etc.

6.5.4 Research and investigations used to define the communication system used

After the paramount decisions above had been made by different internal working groups, a new project was established that should design, plan and implement the different networks on all of Statnett's substations. This project covers installation of racks, structured cabling, network equipment, interface to existing sub station control systems, and at a number of stations, new RTU's. After the project is finished all the RTU's/sub station control systems should be running the IEC 60870-5-104 protocol on IP. The project started medio 2009 and should be finalized by the end of 2011. As mentioned before it is not necessary to implement all the networks on all substations. Some substations just need control and management network, some just need the administrative network and so on. The following are the main points regarding fulfillment of the network implementation in this project.

- ✓ Framework agreement on network equipment

During this project a lot of new networking equipment should be purchased so Statnett made an enquiry to many vendors to establish a new framework agreement.

- ✓ Design phase

During this part of the project a detailed plan regarding routing, QoS, capacity, security, IP plan etc was established. Some adjustments to this plan have been made as the project progress. Some main design decisions is mentioned below.

Routing protocol: OSPF v2 was selected because this is a vendor independent protocol that is well known by technicians, it scales well in big networks and have a relative fast reconvergance time.

QoS: The use of DiffServ was selected and implemented on each router in the network. The different networks have a slightly different configuration regarding the configuration of the traffic classes.

Security: Use of zone based firewall functionality in the routers

The figure below shows a substation that has implemented all the networks.

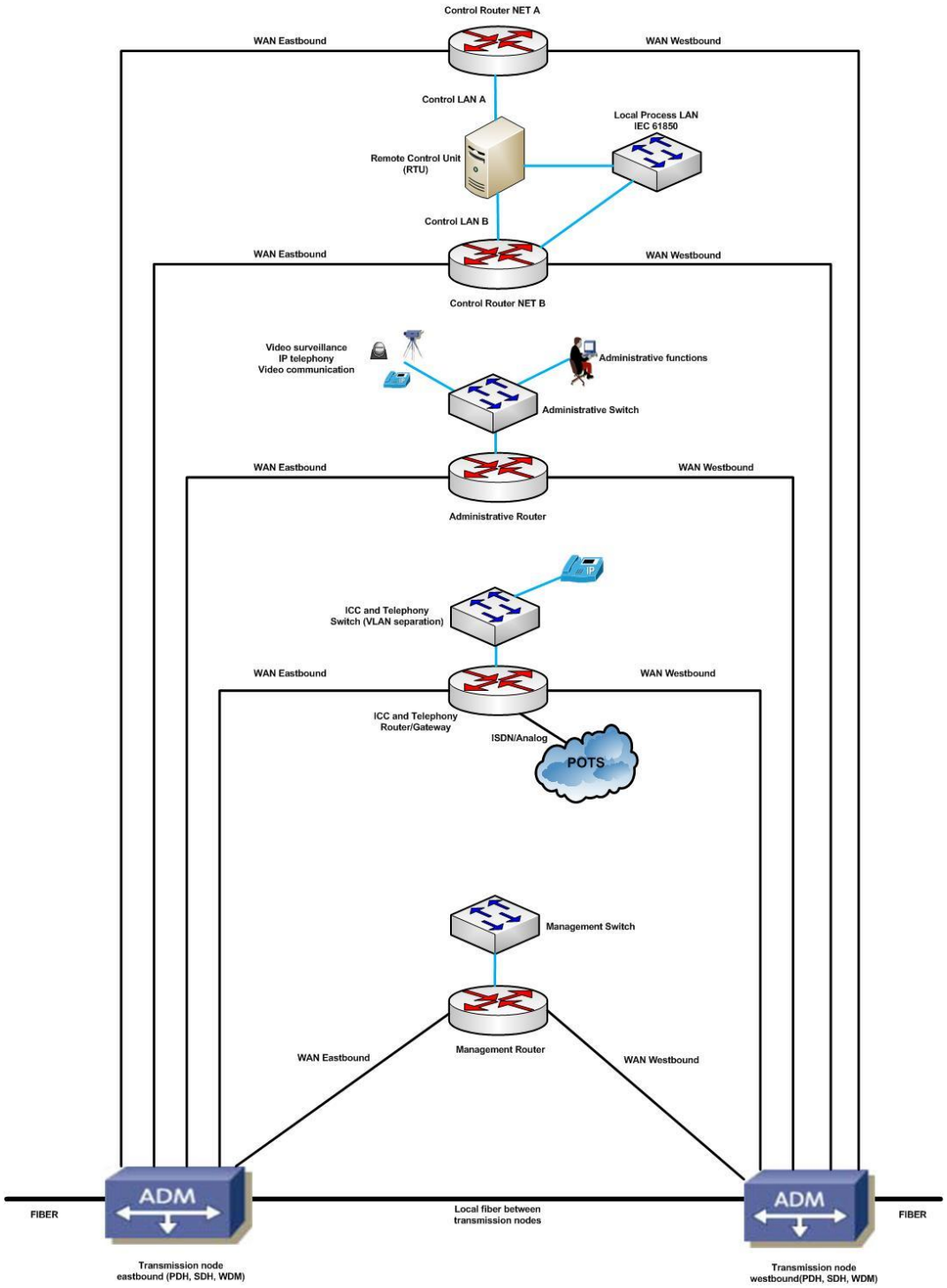


Figure 44: Substation with all networks implemented

In this phase we also designed how the network should look like regarding bandwidth, logical rings or mask to interconnect the substations. The substations in control network A and B are interconnected in logical rings with maximum 5-6 stations in each ring, and this is also the case for the administrative network. The management network and ICC network are designed as a partially meshed network. The figure below indicates how the logical rings are designed in the Control Network A but the same applies to Control Network B and the Administrative network.

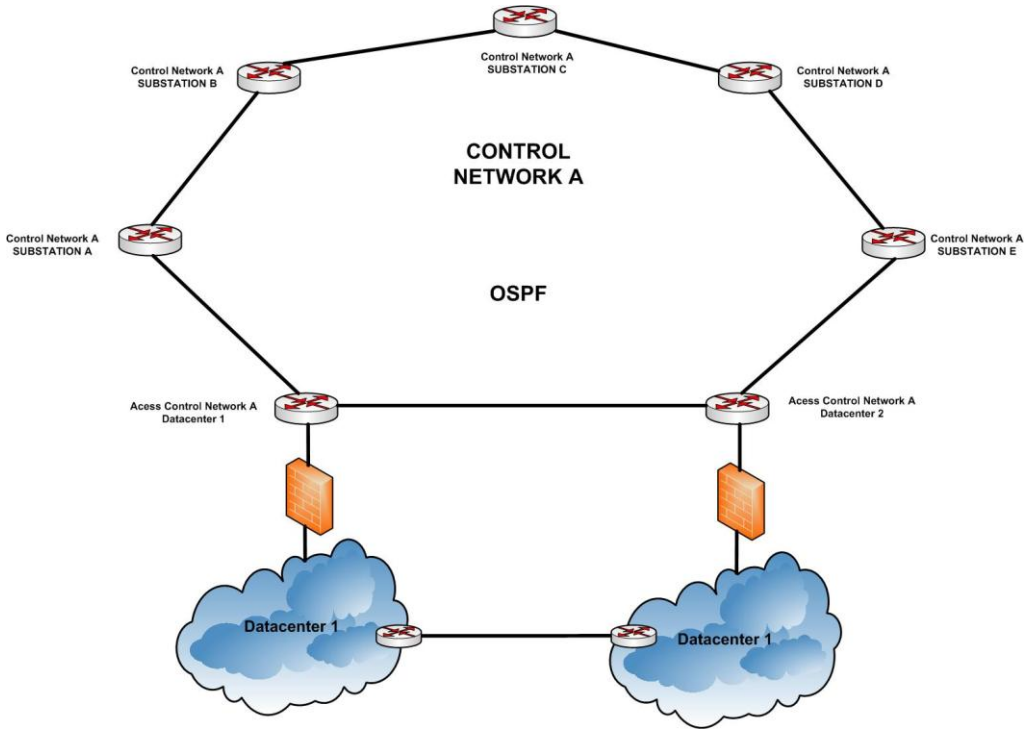


Figure 45: Logical rings in control network

✓ **LAB tests**

To test different design proposals like for instance different routing scenarios a LAB network was established at the main office. This was very helpful to reveal that some configuration proposals did not function as intended. Statnett also have access to test tools like IxChariot to test how the QoS configurations functions.

✓ **Pilot test**

In this part of the project we selected 3 substations where we implemented the different networks. We also had to implement the network solutions at the main sites that should terminate the communication from the different substations and direct the traffic towards the firewall solutions. Some modifications of the routing design where done during the pilot testing to increase the availability of the solution.

✓ **Implementation phase**

Different teams are installing, testing and commissioning the network equipment at the substations. These teams work in parallel so in principal many stations could be installed and commissioned at the same week.

6.5.5 Applications used and their characteristics

As mentioned in the description of the communication system the following applications were identified at the substations:

- Administrative data traffic with accelerating needs for new services and bandwidth.
- Tele control traffic, like IEC-60870-5-104 and IEC 61850
- Inter control-centre communication (ICC) (Elcom-90/TASE.2)
- Access to different maintenance interfaces in the control system (internal and external access)
- Administrative VoIP (Voice over IP) traffic and video
- A second separate VoIP system for power system operation (requirement set by the regulator)
- Video surveillance
- Management of network components (out of band)

The following table gives an overview of the QoS and bandwidth used in the design.

NETWORK	QOS	BANDWIDTH	APPLICATIONS
CONTROL NET A	4 classes, PCU Traffic, Critical Data, Network Control, Best Effort	2Mb/s in each ring	Tele control traffic
CONTROL NET B	4 classes, PCU Traffic, Critical Data, Network Control, Best Effort	10Mb/s in each ring	Tele control traffic, Access to different maintenance interfaces in the control system (internal and external access)
ADMINISTRATIVE	5 classes, Real Time, Call Signaling, Critical Data, Network Control, Best Effort	10Mb/s in each ring	Administrative VoIP and video, Administrative data traffic
ICC AND TELEPHONY	5 classes, Real Time, Call Signaling, Critical Data, Network Control, Best Effort	2Mb/s connections	Inter control-centre communication, separate VoIP system for power system operation
MANAGEMENT	3 classes, Critical Data, Network Control, Best Effort	2Mb/s connections	Management of network components.

Table 10: QoS and Bandwidth Used

6.5.6 Operational and responsibility experiences (use of in/out source)

So far about 60 substations have been commissioned with this new IP based network infrastructure. The networks are monitored by a central management system (ICMP and SNMP) and so far we have not had any major outage.

6.5.7 Conclusions and recommendations

Any high level decisions for example regarding the use of VPN or not must be thoroughly discussed with both the network technicians, security technicians, external experts and the management in the company. Decisions like this are not just about technical issues but also about human factors and what kind of strategy the management in the company would like to take in these issues. In Statnett there have been several working groups that have dealt with these issues, and the conclusions to these working groups are treated by the management and a decision is taken. After all of these high level decisions were taken a new project was started that should plan, test and commission the new infrastructure in detail based on the high level decision taken earlier. It is therefore recommended to spend time on these high level decisions before the

actual implementation project, as well as spending some time on the planning of how to implement the new infrastructure into the old infrastructure without disturbing the running network.

6.6 Case study Outsourcing

The increasing dependency of utilities on network technologies combined with the rapid development of these technologies forces utilities to acquire, apply and maintain practical knowledge of Ethernet and IP network design, implementation and management. Since Ethernet and IP network design, implementation and management are in general not part of the core business of utilities, it might seem logical to outsource these activities to a network technology provider. While this eliminates the need to focus on non-core business activities, it introduces a third party that has a direct influence on Reliability, Availability and Maintainability (RAM) of the electricity supply.

This case study describes the practical experiences with outsourcing the management and provisioning of business LAN and operational Telecommunications networks of a European TSO. At the end of this section, an overview is given of the advantages and disadvantages of outsourcing.

6.6.1 Description of outsourced services

The TSO outsources the management and provision of the business LAN and operational telecommunications network. However, the TSO owns the operational network whereas the business LAN is provided (in a significant part) on MPLS procured from an external company. The operational network is split into two sections – A managed fibre contract and a managed services contract. The managed fibre contract is responsible for all fibre optic media connecting substations and the managed service for the hardware. While the TSO owns the fibres on the overhead lines, all fibres are leased in perpetuity to a technology provider. The TSO rents two fibers from the bundle back from the technology provider. The TSO does not have access to any dark fibers on the network.

6.6.2 Description of the communication system

The operational telecoms network currently only hosts legacy services, Ethernet is not implemented. The business LAN is implemented using Ethernet and IP. The backbone is primarily SDH. This is to facilitate deterministic services for inter substation protection systems. However, the network can carry Ethernet traffic although it is currently mainly focussed on legacy type communication for the majority of applications – SCADA, telephony, etc. The only instance where Ethernet traffic is transported on the operational network is when it's not cost effective to provide another way. Remote access traffic is currently allocated to the business LAN

The TSO recognises that this must change at some time. Wide area monitoring, protection and control will necessitate IP services on the Operational Telecoms network. However, remote access is currently being provided across the business LAN because there is no IP network on the operational telecoms network. The key to providing on the operational network for remote access is establishing cost effectiveness i.e how much money will remote access save and then offset this against providing an IP network on the operational network. Critical functions such as control and protection will demand IP services that have to be provided.

The design of a LAN to carry traffic from a single workforce is considerably less complicate than one where parties from different organisations want to access assets at sites in a complex matrix. The TSO outsources a significant part of substation SCS and protection support with a mix of supplier's equipment at each substation. In today's security challenged world, it must be ensured that only the authorised person can reach the devices they are responsible for. This requires functionality to ensure that a representative from supplier A can only connect to supplier A devices etc. except where a more complex arrangement may be required as shown in the table below:

		Supplier A	Supplier B	Supplier C	Data collector	TSO
Devices Under the Responsibility of	Supplier A	Access				Access
	Supplier B		Access		Access	Access
	Supplier C			Access	Access	Access
	Supplier D			Access		Access

TABLE 11: REMOTE ACCESS POLICY

		Supplier A	Supplier B	Supplier C	Data collector	TSO
Devices Under the Responsibility of	Supplier A	Access				Access
	Supplier B		Access		Access	Access
	Supplier C			Access	Access	Access
	Supplier D			Access		Access

Table 11 shows the policy of granting remote access to different devices in a scenario where multiple third-party companies are responsible for the utility operational network In either case, controlling access to this complexity can cost significant amounts of money if implemented across a specific LAN infrastructure

6.6.3 Expected future steps

In order to limit the dependency on network technology providers, the TSO plans to implement the following approach:

- A core specialist or specialists from the TSO looking at specifications and design / implementation consultancy
- Suppliers responsible for substation LAN network design and implementation working in conjunction with the core TSO team
- An outsourced operational LAN provider supplying pre-agreed and pre-defined network designs that can be ordered in a standardised form

There will be a need to get all parties around the table to identify the requirements of inter substation / operational network communication. Once these have been identified, these would be ordered and supported using a standard call off arrangement and service level agreement much like ordering a service from a telecommunications provider. Another party above acts like a telecommunication provider even though this may be a single source contract set up and provided for the TSO. It may be that this party above will be used as a consultancy resource but it is unlikely that they will ever have any responsibility for anything within a substation environment.

6.6.4 Conclusions and recommendations

The table below gives an overview of the pro's and con's of outsourcing:

Pro's	Con's
Network design by specialists with practical experience: - Implementation can be faster - Network performance can be better - Un-foreseen failures are less likely to occur	Communication concerning the outsourced activities is less direct, because is the communication is cross-company,
Own personnel can focus on core business	The utility is dependent on a third party for the correct functioning of business critical applications
Because a company is responsible for the network instead of a (small) group a people, sickness, holidays and personnel changing jobs have much less impact on continuity	Change requests take longer because the commercial process has to be completed
Because each change has to be planned: - Each change has to be thought trough before it's made - Each change will be registered	Each change has to be planned, so it will take more time to make a change
Because the outsourced activities are performed by specialists they can be performed more efficiently, thus more cost effective.	Because the outsourced activities are performed by a commercial company that needs to make a profit, the performed activities will be less cost effective
Because the outsourced activities are performed by specialists they will apply knowledge about the latest technologies and their application	The network technology provider may not have the necessary domain knowledge required to provide the service level required
	The rotation of staff with commercial third party service providers can be high leading to loss of utility specific knowledge
	Financial stability of contractors may be limited
	Contract life cycles may be such that the optimal use of the services required is not guaranteed
	Unless the responsibilities for all involved parties are defined in detail, it might be difficult to identify the responsible party when something goes wrong

Table 12: Pro's and Con's of outsourcing network services and management

7 Conclusions and proposal for future work

Several interesting observations can be made from the survey results - for instance:

- 50% of the respondents plan to migrate to IP within the next years, and 50% of the respondents expect that their applications will stay in the "old world".
- The current networks are fairly "IP ready" (60%), but only 21% of the applications can run on IP at the moment. Consequently, there is a great need (and probably a large market) for the integration of legacy applications.
- Many respondents do not believe that protection and other applications requiring deterministic network behavior will ever be able to run on IP. Therefore, they build their architecture as a 2-string approach.
- The respondents believe that physical network security and cyber security must be a top one priority from the beginning of network design in order to achieve a successful implementation.
- It can be emphasized, that training and awareness of IP technologies are crucial disciplines to demystify IP. Also, learning from companies who are already using an IP network with fully enabled applications is a good option.

From the technical brochure can be concluded that IP as a one-platform solution provides the possibility to connect any device to a single network. Migrating to IP thus relieves the user from maintaining more than one network.

The scalability and the flexibility of a well-designed IP network is very good. However, following the transition methods used by the majority of utilities, a cost reduction should not be expected from day one because more than one network needs to be maintained during the whole migration period. The survey shows that this migration period is often more than 5 years. On the other hand if the migration to IP is postpone for too long there is a risk of ending up with obsolete technologies.

There are lots of different technologies available for data communication, which are suitable for implementing an IP architecture - and user's needs are very different. Therefore the optimum solution varies accordingly. The directions given in Chapter 4 of this brochure are meant to simplify some of these choices.

Prioritization has been a very important task during the development phase for this brochure. This has resulted in a more narrow approach than originally anticipated, and obviously more work should be carried out within this field. The following future works are suggested to be performed:

- Communication needs for very large grids and communication support for the network of the future. Subtopics: IPv6 as support for networks with a very large number of nodes, the EPU's communication network's readiness for being backbone for the network of the future.
- Traffic engineering, especially latency control and symmetry considerations for real-time data transfer.
- Life cycle considerations for network equipment and network technology.
- Implications of using the IEC reports IEC 61850-90-4, IEC 61850-90-2 and IEC 61850-90-1
- Management systems for improved overview of network status and security rules.
- Guidelines for cost estimation in migration projects.

In addition, we believe that it would be very valuable to make minor modifications to the survey questions and then reissue the survey in 2013 to detect the trends regarding the use and migration of IP in the utility environment. A summary of these results would be very suitable for an article in Electra.

8 References, Bibliography, On-going works

[Reference 1] CIGRE-D2, part 4 Operational Service Implementation

[Reference 2] RuggedCom Application Note: www.ruggedcom.com/pdfs/application_notes/latency_on_a_switched_ethernet_network.pdf

[Reference 3] TR IEC 61850-90-4

[Reference 4] Cigre WG D2.23 The use of Ethernet Technology in the Power Utility Environment

[Reference 5] IEC 61850-7-2

[Reference 6] Sauming Pang "Successful Service Design for Telecommunications", 2009 John Wiley & Sossons Ltd

8.1 Published Papers and Reports

PacWorld Magazine article, March 2010 Issue: "Implementation of Telecontrol Applications over GPRS Networks; http://www.pacw.org/fileadmin/doc/MarchIssue2010/ZIV_march_2010.pdf]:

IEC 61850-90-2 Substation to Control Center communication

IEC 61850-80-1 Guideline to exchanging information from a CDC based data model using IEC 60870-5-101 or IEC 60870-5-104

Cigre WG D2.23 The use of Ethernet Technology in the Power Utility Environment

Cigre WG D2.24 EMS Architectures for the 21st Century (Chaper 10)

Cigre WG D2.22 Treatment of Information Security for Electric power Utilities

R. Seifert, The Switch Book

9 Abbreviations

AS	Autonomous System
ATM	Asynchronous Transfer Mode
CAPEX	Capital Expenditures
CC	Control Center
CCTV	Closed Circuit Television
CDC	Common Data Class (as defined in IEC61850-7-3)
DSO	Distribution System Operator
E-Line	Ethernet Line (Metro Ethernet Forum definition)
E-LAN	Ethernet LAN (Metro Ethernet Forum definition)
E-Tree	Ethernet Tree (Metro Ethernet Forum definition)
EGP	External Gateway Protocol
EM	Electro Magnetic
EMC	Electromagnetic Compatibility
EMS	Energy Management System
EPU	Electric Power Utility
ERP	Ethernet Ring Protection
FAT	Factory Acceptance Test
FO	Fiber Optic
IANA	Internet Assigned Numbers Authority
ICCP	Inter Control Centre Protocol (TASE.2)
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
KPI	Key Performance Indicator
LAN	Local Area Network
LDP	Label Distribution Protocol
NAT	Network Address Translation
NTP	Network Time Protocol
MPLS	Multiprotocol Label Switching
OAM	Operation, Administration and Maintenance

OPEX	Operational Expenditures
OSPF	Open Shortest Path First
PBB	Provider Backbone Bridging
PBR	Provider Backbone Ring
PDH	Plesiochronous Digital Hierarchy
PMU	Phasor Measurement Unit
QoS	Quality of Service
RTU	Remote Terminal Unit
SAT	Site Acceptance test
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SPF	Shortest Path First
SS	Substation
STP	Spanning Tree Protocol
TC	Traffic Control
TDM	Time Division Multiplexing
TSO	Transmission System Operator
VoIP	Voice over IP
VPLS	Virutal Private LAN Service
VPN	Virtual Private Network
VRF (Lite)	Virtual Routing and Forwarding. VRF Lite is the simplest form of a VRF implementation
WAN	Wide Area Network

10 Definitions

In this Brochure, the terms SCADA and Telecontrol are used side by side.

Telecontrol: Means either a range of functions i.e. a subset of the SCADA functionality or refers to an organizational unit which is responsible for e.g. SCADA.

ANNEX 1 Survey IP-based Substation Applications

WGD2.28 – Survey

IP Based Substation Applications

Survey Objective:

Get an overview of the present use of IP-based applications within the substation environment, between Substations and for Substation - to - Control Centre communications.

This survey is conducted among CIGRÉ Working Group D2.28 members and CIGRÉ members. Please check and detail your options.

Questionnaire:

1- Are you a:

- ☐ Transmission System Operator/Distribution System Operator
- ☐ Vendor
- ☐ Other (please detail):

2- Within your own company, which substation applications are using IP and IP networks? (For vendors: Which applications do you see at customer´s sites?)

- ☐ Substation RTU to SCADA platform
- ☐ Inter-Control Centre Interconnections
- ☐ Condition monitoring for HV devices
- ☐ Metering
- ☐ Disturbance recorder data
- ☐ Telephony system
- ☐ CCTV/Video Surveillance
- ☐ Premises access control
- ☐ Building control (temperature, humidity, lights, etc.)
- ☐ Network Management System & Data Communication Network
- ☐ Remote IP Access to substation assets
- ☐ Tele-protection
- ☐ Time synchronization
- ☐ Access to office applications

- ☐ Wireless LAN Access
- ☐ Other (please detail):

3- What are the main operational challenges using IP into the substation environment?

- ☐ Security
- ☐ Converting legacy interfaces into IP
- ☐ Interoperability
- ☐ Ruggedness (environment)
- ☐ Quality of Service
- ☐ Knowledge and Training
- ☐ Scope of Responsibility
- ☐ Other (please detail):
- ☐ Additional comment:

4- What are the main psychological barriers with using IP protocols in Substation applications?

- ☐ Security
- ☐ Reliability
- ☐ Quality of Service
- ☐ Familiarity with Ethernet/IP concepts
- ☐ Rate of innovation and obsolescence
- ☐ Lack of documentation
- ☐ Other (please detail):

5- Are all of your applications compatible with IP at the moment?

- ☐ Yes
- ☐ No (please detail):

6- Prediction to migration of all operational communications into IP?

- ☐ Already done
- ☐ Short term
- ☐ 6 months
- ☐ 1-2 yrs
- ☐ 5 yrs
- ☐ More than 10 yrs

☐ Never - Why?

7- How to deal with legacy protocols and equipment?

☐ Protocol encapsulation

☐ Vendor

☐ Gateway (protocol conversion)

☐ Emulation

☐ Separate network

☐ Other (please detail):

8- Is the existing communications network ready for IP traffic?

☐ Yes

☐ No (please detail):

9- Requisites and concerns for the telecommunication network?

☐ Existence of physical infrastructure (fibre, copper, wireless, etc)

☐ Suitable transport technology (PDH, SDH, Ethernet, etc.)

☐ Suitable IP addressing space and scheme (IPv4 / IPv6)

☐ Identification of Applications

☐ Other (please detail):

10- Which underlying IP technology is the most promising to provide secure reliable IP communications?

☐ MPLS (IP over fibre)

☐ Ethernet/IP over SDH

☐ Ethernet/IP over DWDM

☐ Other (please detail):

11- Should the IP network be reserved for operational service or also be used for corporate services? Two physically/virtual separate networks or one network?

☐ One only network, no separation

☐ Separate network (physical)

☐ Separate network (virtual/logical)

12- Which technology is more promising to separate and provision different types of IP services?

- ☐ Virtual LAN
- ☐ Virtual Private Networks (Layer 3)
- ☐ Virtual Private LAN Service - VPLS (Layer 2)
- ☐ Multicast filtering
- ☐ Other (please detail):

ANNEX 2 Extensive list of applications and migration possibilities

Following, is a raw and non descriptive list of applications that can be found in substations environment, which can be relevant for IP communications networking and design.

There are several types of applications that must be considered:

- Applications which are plugged onto the new technology / equipment
- Applications which are converted
- Applications which stay in their original environment

Applications			Connectivity via Ethernet or IP [Y/N]	Immediate, Short, Medium, Long term [I/S/M/L]	Converter necessary	Comment
Control	System Operation		Y	M		
	Control Location		Y	M		
	Controllable Objects		Y	M		
	Commands	Select	Y	M		
		Operate	Y	M		
		Multi select	Y	M		
Interlocking			Y	L	N	
Blocking			Y	L	N	
Sequential Switching			Y	L	N	
Synchronizing			Y	S	N	
Synchro-check			Y	S	N	
Alarms and Events			Y	S	Y	
Measurements			Y	S	Y	
Human Machine Interface			Y+N			depends on protocol used
Automation			Y+N			
Protection	Disturbances in the High Voltage network		Y	L	N	
	Failures in the Substation Automation or Related Systems		Y	L	N	
	Tripping		Y	L	N	
	Distance Protection		Y	L	N	
	Line Differential Protection		Y	L	N	
	Overcurrent Protection		Y	L	N	
	Directional Overcurrent Protection		Y	L	N	
	Earth Fault Protection		Y	L	N	
	Thermal Protection		Y	L	N	
	Arc Protection		Y	L	N	

Applications		Connectivity via Ethernet or IP [Y/N]	Immediate, Short, Medium, Long term [I/S/M/L]	Converter necessary	Comment
	Transformer Differential Protection	Y	L	N	
	Buchholz Protection	Y	L	N	
	Protection functions based on other physical quantities (Gas Analysis, Partial Discharge, etc)	Y	L	N	
	Unbalance Protection	Y	L	N	
	Under and Over Voltage Protection	Y	L	N	
	Gas Protection	Y	L	N	
	Under and Over Frequency Protection	Y	L	N	
	Busbar Differential Protection	Y	L	N	
	Breaker Failure Protection	Y	L	N	
	Protection based on other physical quantities in enclosed switchgear (Light, Pressure, etc)	Y	L	N	
Power Quality		Y	S	N	
Revenue metering		Y	S	N	
Device Monitoring		Y	S	N	
IED Monitoring		Y	S	N	
Function Monitoring		Y	S	N	
Communication Monitoring		Y	S	N	
Command Circuit Supervision		?			
Monitoring of legacy devices and functions		N	NA	N	depends onprotocol used: if based on SNMP/IP YES if based on other protocol like IS-IS,,, NO

Applications			Connectivity via Ethernet or IP [Y/N]	Immediate, Short, Medium, Long term [I/S/M/L]	Converter necessary	Comment
High Voltage Equipment Monitoring	Circuit Breaker Monitoring	Drive system	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Extinguishing chamber	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Accumulator	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Gas Pressure	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Gas Density	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
	Transformer Monitoring	Partial discharge	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Gas in oil (for oil filled transformers)	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Winding and Oil Temperatures (for oil filled transformers)	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)

Applications			Connectivity via Ethernet or IP [Y/N]	Immediate, Short, Medium, Long term [I/S/M/L]	Converter necessary	Comment
		Gas Pressure Supervision (for gas filled transformers)	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Gas Density Supervision (for gas filled transformers)	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Transformer ageing	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
	Capacitor Monitoring	Partial discharge	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Gas in oil	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Temperatures	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Capacitor ageing	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
	Reactor Monitoring	Partial discharge	Y	S	Y/N	RTU 104 (direct IP) or RTU 101

Applications			Connectivity via Ethernet or IP [Y/N]	Immediate, Short, Medium, Long term [I/S/M/L]	Converter necessary	Comment
						(converter)
		Gas in oil	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Winding and Oil Temperatures	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
		Reactor ageing	Y	S	Y/N	RTU 104 (direct IP) or RTU 101 (converter)
	VT and CT circuit supervision		Y	S	Y/N	
Disturbance Recording			Y	S	NA	
Automatic Load Transfer			?			
Transformer Changeover			?			
Fault Restoration			?			
Network optimization			Y	M	N	
Air forced cooling of high voltage assets			Y	S	N	
Voltage selection			?			
Autoreclose			?			
Adaptive Protection			?			
Time synchronization			Y	S	N	
Voice over IP			Y	I	N	
Fire detection			Y	I	N	
Building control	Premises access control and monitoring		Y	I	N	
	Video over IP		Y	I	N	
	Temperature and air quality control		Y	I	N	
Access to office applications			Y	I	N	

Applications	Connectivity via Ethernet or IP [Y/N]	Immediate, Short, Medium, Long term [I/S/M/L]	Converter necessary	Comment
Diagnosis channels	?			