249

INTEGRATED SERVICE NETWORKS FOR UTILITIES

Working Group
D2.07

August 2004

cigré

Integrated Service Networks for Utilities

Working Group
D2.07

Prepared by :

Convener: Carlos SAMITIER

Secretary: William CAFFREY

TABLE OF CONTENTS

1 INTRODUCTION 5

1.1 HISTORY OF TELECOMMUNICATIONS NETWORK DEVELOPMENTS 5
1.2 SUMMARY OF CIGRE RELATED WORK AND REPORTS 7
1.3 ENVIRONMENT OF A POWER/ENERGY SUPPLIER 8
1.3.1 The Operational environment 8
1.3.2 The Corporate environment 9
1.3.3 The Operational and Corporate Networks 11

2 INTEGRATED SERVICES NETWORK BUSINESS BENEFITS 13

2.1 INTRODUCTION 13
2.2 KEY INVESTMENT DRIVERS FOR NETWORK IMPLEMENTATION 13
2.3 BENEFITS OF AN INTEGRATED SERVICES NETWORK 15
2.3.1 Financial Benefits 16
2.3.2 Technological Benefits 16
2.3.3 Benefit of Scalability over Legacy Networks 17
2.3.4 Service Provision Improvements 17
2.3.5 Organisational Consequences 17
2.4 COMPARISON OF ALTERNATIVES 18
2.4.1 Service Provision from 'Internally Provided' Networks 19
2.4.2 Service Provision from 'External Provided' Networks 20
2.4.3 Network Implementation. 20

3 USER REQUIREMENTS 22

3.1 INTRODUCTION 22
3.2 SERVICE DEFINITION 22
3.3 SECURITY REQUIREMENTS 23
3.4 SCALABILITY REQUIREMENTS 23
3.5 MANAGEMENT REQUIREMENTS 25
3.6 CONTINGENCY REQUIREMENTS 26
3.7 SERVICE LEVEL AGREEMENT 27

4 NETWORK DESIGN 28

4.1 INTRODUCTION 28
4.2 DESCRIPTION OF THE OVERALL NETWORK DESIGN PROCESS 28
4.3 EVALUATION OF RISK 33
4.4 CONTINGENCY PLANNING 33
4.5 TRAFFIC PROFILES DEFINITION 34
4.6 DESIGN POLICY 34
4.7 TOPOLOGY DESIGN 36
4.7.1 Topology constraints 36
4.7.2 Cost/performance optimisation at the topology level 39
4.7.3 Reliability considerations 40
4.8 SERVICE INTEGRATION POLICY 44
4.9 ARCHITECTURAL DESIGN 44
4.10 NETWORKING TECHNOLOGY SELECTION 45
4.10.1 Networking technologies 45
4.10.2 New networking technologies 47
4.11 INTERNETWORKING ARCHITECTURE 48
4.11.1 Multiprotocol Label Switching 48
4.12 MANAGEMENT ARCHITECTURE 49
4.12.1 Network Management Centres 50
4.12.2 Management System 50
4.12.3 Management Data Network 52
4.13 SECURITY ARCHITECTURE 52
4.13.1 Security Policy 52
4.14 SERVICE MAPPING 57
4.14.1 Service Classes and Applications 57

4.14.2 Service integration *57*
4.15 NAMING AND ADDRESSING SCHEMES AND PLANS 59
4.15.1 Addressing strategy *59*
4.15.2 Registered versus unregistered addresses *60*
4.15.3 Dynamic addressing *60*
4.15.4 Naming schemes *61*
4.15.5 Mobility *61*
4.16 ROUTING ARCHITECTURE 62
4.17 TRAFFIC ENGINEERING 65
4.17.1 Introduction to Traffic Engineering Concepts *65*
4.17.2 Traffic Engineering Process *68*
4.17.3 Traffic Engineering Systems Classification *69*
4.17.4 Requirements for IP Network Traffic Engineering *69*
4.17.5 Network Engineering *70*
4.18 SIMULATION 71

5 NETWORK IMPLEMENTATION 75

5.1 INTRODUCTION 75
5.2 IMPLEMENTATION OPTIONS 75
5.2.1 New sites *75*
5.2.2 Migration *76*
5.3 INSTALLATION AND COMMISSIONING CONSIDERATIONS 79
5.3.1 Commissioning *80*
5.3.2 Tools and equipment *80*
5.4 IMPLEMENTATION RISKS 81

6 NETWORK MANAGEMENT AND OPERATION 82

6.1 INTRODUCTION 82
6.2 OPERATIONAL RISKS 82
6.3 NETWORK MANAGEMENT TOOLS 83
6.4 SERVICE LEVEL MANAGEMENT 84
6.4.1 Service Level Management Tools *84*
6.4.2 Reporting Systems *85*
6.4.3 Configuration and Change Management *85*
6.5 MAINTENANCE PLAN 85
6.6 STAFF REQUIREMENT 86
6.7 STAFF TRAINING 86

A. TRAFFIC MODELS 88

B. TOPOLOGY PLANNING AND DIMENSIONING 92

C. GUIDELINE FOR THE DEFINITION OF A TRAFFIC MODEL 98

D. REFERENCES 101

Foreword

Cigré Study Committee 35 created Working Group 07 in 1994 to investigate the manner in which power utility telecommunications could be provided in the emerging high speed telecommunications environment.

Working Group 07 has been following technological advances in the field of networking technologies exploring its potential application in the power utility environment.

This work, together with two previously published technical brochures and a number of papers, completes a comprehensive set of publications that offer a complete view of the broadband technologies and their use in the power utility environment.

The membership of the Working Group comprised:

Members		**Corresponding members**	
Mr João Almeida	Portugal	Mr Peter Cristaudo	Australia
Mr William Caffrey (Secretary)	Ireland	Mr Bernhard Gutmann	Germany
Mr Günter Endlich	Germany	Mr Gary Michael	United States
Mr Adam Erdheim	Sweden	Ms. Milena Matic	Yugoslavia
Mr Harald Lotsch	Germany	Mr. Claudio Trigo	Brasil
Mr. Daniel Gonzalez	Spain	Mr Kubon Nakajima	Japan
Mr. Enrique Garcia	Spain	Mr Tony Parkin	Great Britain
Dr. Surat Tanterdtit	Thailand	Dr Fernando Gonzalo	Spain
Mr Johannes Hvidevold	Norway	Mr. Maurizio Monti	France
Mr Hermann Spiess	Switzerland	Mr. Joan Viaplana	Spain
Mr Carlos Samitier (Convener)	Spain	Mr. Gao Kunlun	China
		Mr. Rodolfo Pellizzoni	Argentina
		Mr Jan Piotrowski	Poland

This Technical Brochure is dedicated to the memory of Klaus Morf, who died in June 2000.

Klaus represented ABB as a member of CIGRE for more than 20 years as a Study Committee member on SC35, as well as the National Committee for Switzerland, and as part of this Working Group.

1 Introduction

The previous work in this area by this Working Group was focussed on exploring the various technologies suitable for utility wide area telecommunications. This Technical Brochure is intended to follow up on this earlier work by providing a guide for the design and implementation of a new broadband telecommunications network for the provision of an Integrated Service Network (ISN), with particular emphasis on the needs of utility companies.

At a general level, it is intended to assist customers and service providers understand the basic principles and issues involved and to act as a guide for the specification and negotiation of services. It attempts to present the design of an ISN in terms of:

- The internal network architecture design
- The principles of service integration and guidelines, and
- Practical recommendations and supporting principles.

It is structured to facilitate the information requirements of different users within the Electrical Power Industry, from senior management to network operators.

The first chapter describes the environment of a power/energy supplier, analysing the corporate and operational network environment.

Chapter 2 is addressed to top management and presents the business needs for service networks and the policies for business provision.

Chapter 3 is addressed to network users. It analyses the different aspects of service specification and requirements.

Chapter 4 is addressed to network designers and is the core of the brochure. It depicts with detail the different phases of the network design process.

Chapter 5 is addressed to network implementers. It describes the processes and options for migration, installation and commissioning of networks and services.

Chapter 6 is addressed to network managers and covers the aspects of management and operation, including contingency planning.

It is intended that the each chapter can be referred to separately.

For those wishing to know the technical details, appendices with specific information and corresponding references have been included.

1.1 History of Telecommunications Network Developments

The concept of telecommunication network in the field of power utilities was formerly introduced when the first generation of analogue transit telephone exchanges were deployed.

Although the timing was different in every country, it can be stated that back in early 80's power utilities used analogue networks based on transit exchanges to offer automatic telephony service. This service was a very important complement to the emerging automation system and was very important to communicate substation staff with control centres since automation and control systems provided a very limited functionality.

Since earlier times, telecommunication networks have experienced several technological revolutions, the most important being the introduction of digital technologies in late 80's. This involved not only the replacement of most equipment but also the introduction of completely new concepts. WG35.02 published in June 1989 the technical brochure "*Guide for Planning*

of Power Utility Digital Telecommunication networks". This brochure offers a good description of the new concepts introduced by digital technology and the key aspects that have to be considered in the design of digital networks.

The first generation of digital networks, now know as PDH, introduced the concept of service integration by using time division multiplexing. Voice and data services were delivered using independent networks at that time, with the aid of PDH both shared part of the transmission infrastructure.

Although using digital channels, voice networks remained analogue until Integrated Service Digital Network (ISDN), now know as Narrow Band ISDN (NB-ISDN), was introduced.

Data networks were not used in power utilities when the former telecontrol systems were deployed. Automation systems requiring communications used point-to-point analogue channels that progressively were replaced by digital channels provided by PDH networks. Connection-oriented packet networks based on X.25 were only used to connect computers or regional to national control centres.

The massive deployment of fibre optics links and the advanced in broadband switching paved the way to the introduction of broadband networks. The great challenge of this new technology was to integrate packet and voice services over a common infrastructure providing both constant bit-rate and variable bit-rate service integrated over a common transport infrastructure based on SDH thus achieving the convergence between data and voice networks. ATM was the technology that provided the integration of different classes of services with QoS guarantees. It was planned to use ATM from the desktop to the backbone network but, at that time, the IP protocol was gaining ground and won the battle for the control of the desktop and access networks becoming the universal service provision technology. This forced the implementation of internetworking architectures that allow IP to be mapped over ATM.

With the advent of Gigabit routers, IP is also becoming the dominant technology in the core of the network which helps to simplify internetworking models.

Technological evolution today is focussed on all-optical networks that provide Ethernet transport. In this new approach, IP could become less important in the core of the network.

Figure 1.1 shows a mind-map of the different aspects of telecommunication evolution. Starting from the transmission, how services are integrated, how the network layer is implemented, what is the network architecture, and finally how the services are provided; every branch shows the evolution of the related concept. The oldest concepts are closer to the centre whereas future trends are out of the branches.

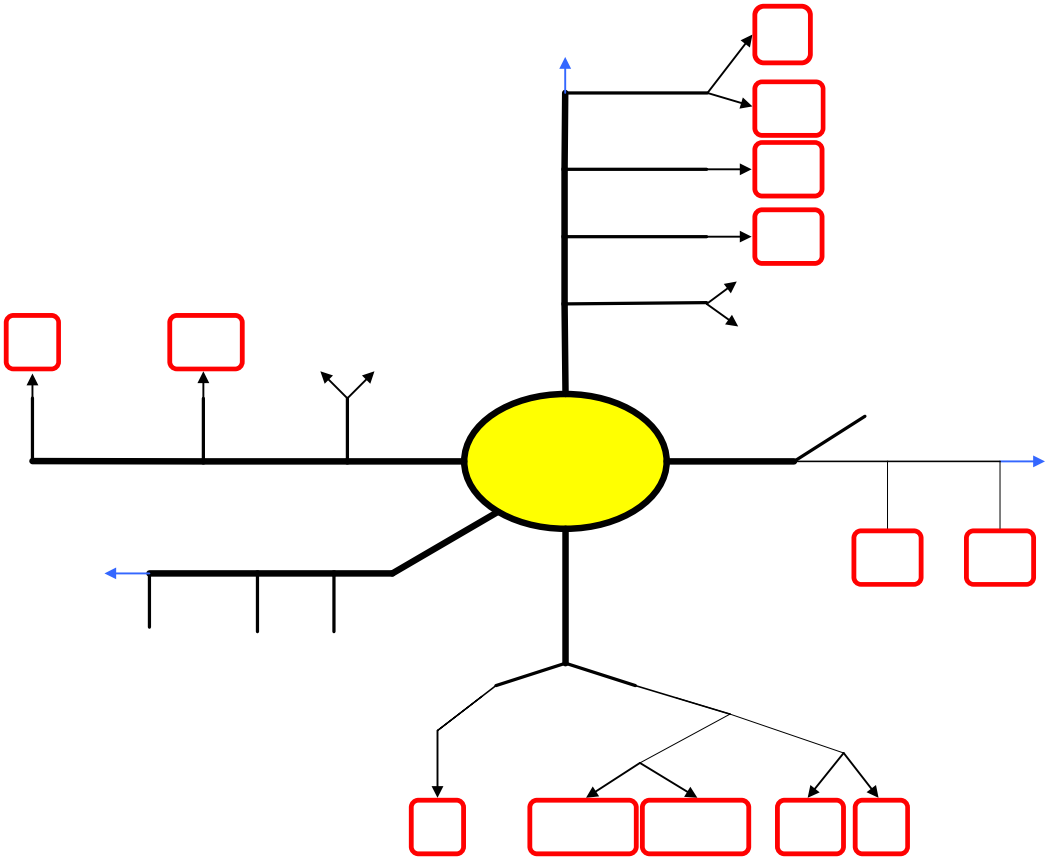


Figure 1.1 Telecommunication Evolution

1.2 Summary of CIGRE related work and reports

The former Study Committee 35 (now Study Committee D2) has been working in the field of networking since early 80's. WG35.07 has been following the developments of Broadband technology and has produced a number of publications the most relevant being:

TB-107. "*Power System Communications in the High Speed Environment*". December 1996.

Electra magazine. "*IP-Technology, an introduction*". June 1997.

Electra magazine. "*Transmission of real-time data with guaranteed quality of service using IP-technology*". August 1997.

CIGRE Colloquium. "Telecontrol over ATM". September 1997.

Electra magazine. "Service Integration". October 1997.

Electra magazine. "Implementation of an IP-network for the transmission of utility real-time data". February 1998.

CIGRE Paris Session. "*Potential Internet Protocol Technologies*". September 1998.

CIGRE Colloquium. "*Implementation of Operational Services like Telecontrol Using QoS IP Networks*". October 1999.

TB-153. "*The Use of IP Technology in the Power Utility Environment*". April 2000.

IP ISDN

CONNECTION LESS CONNECTI ORIENTE

ETHERNET TRANSPORT

CIGRE Paris Session. "*Potential of New Telecommunication Technologies for Power System Protection*". September 2000.

CIGRE Paris Session. "*Architectures for Internetworking*". September 2000.

CIGRE Colloquium. "*External Vs Internal IP Network Provision*". June 2001.

CIGRE Paris Session. "Substation Migration into an IP Network". September 2002.

CIGRE Paris Session. "*Potential Applications of Resilient Packet Ring Technology for Power Utilities*". September 2002.

1.3 Environment of a power/energy supplier

1.3.1 The Operational environment

Operational aspects regarding power stations, power transmission and power distribution define the needs for data transmission. This includes for example the following activities:

- Electric power generation (fossil-fuel power stations, hydro-electric power stations, nuclear power stations, wind/solar power plants) and distribution
- Generation of Process heat
- Operation of District heating systems

Supervision and control is a very important task within this complex environment. Different working condition must be controlled and monitored remotely. The status of the different elements (power plants, power transmission lines and power/heating distribution systems) has to be monitored and controlled permanently. Furthermore the status of the whole environment has to be controlled to guarantee the efficient use of all facilities. These data are relevant for:

- Internal operational aspects (security, profitability)
- Internal administrative aspects (e.g. statistics for marketing)
- External operational aspects (interconnection with other power suppliers)

Regarding the transmission of the data within the operation environment (supervision, control, monitoring, etc.) security and privacy are the most important issues. The requirements for security and privacy is also valid for the remote working operational/maintenance personnel connected to the Voice or Data-Network.

Furthermore the latest multimedia technologies (audio and video) offers new possibilities for different purposes like:

- support/supervision of installation/maintenance personal
- visual remote control of facilities
- video conferences

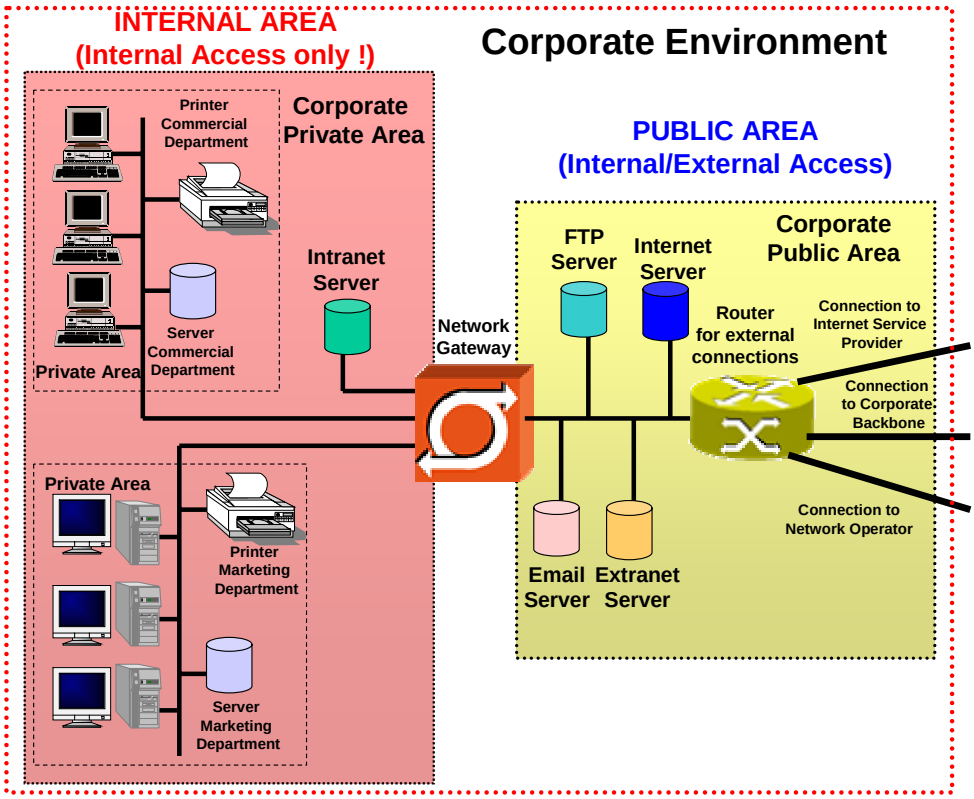


Figure 1.2 Network Environments

1.3.2 The Corporate environment

Different aspects has to be covered including:

- Operational logistics (fuel supply for fossil-fuel power stations, spare part provisioning etc.)
- Customer related logistics (customer relationship management, billing, helpdesk etc.)
- Relationship to other energy (power/heating) suppliers
- Internal/External logistics
- Marketing (which is relevant for deregulated Countries)
- Furthermore consultancy services for other power suppliers might be offered (e.g. planning, construction and operation of power plants, management of power plant by-products).

This corporate environment can be compared with office environments of other industrial branches. This means that the working environment is mainly based on "standard equipment" (Personal Computers with standard applications, Local Area Networks using the Internet Protocol).

Depending on the organisational structure the network can be organised as different "private areas" with several common entities (e.g. Intranet Server).

Another important region of the network is the "public area". Since the external representation of a corporate gets more and more important (e.g. the appearance in the Internet), a "controlled access" from the outside must be possible. The customer/supplier association via the "Extranet" is another important example.

There are remotely working peoples for operative purposes as well as for administrative purposes within the environment of a power/energy supplier. These remote workers might have fixed or mobile places to work. Normally the "telephone network" (analog, digital or mobile) is used to connect remote workers to their corporate environment. In Principle there are two possibilities to access the corporate network:

- Remote LAN Access via corporate owned Dial-Up access points (see figure below)
- Remote Access via the Public Internet

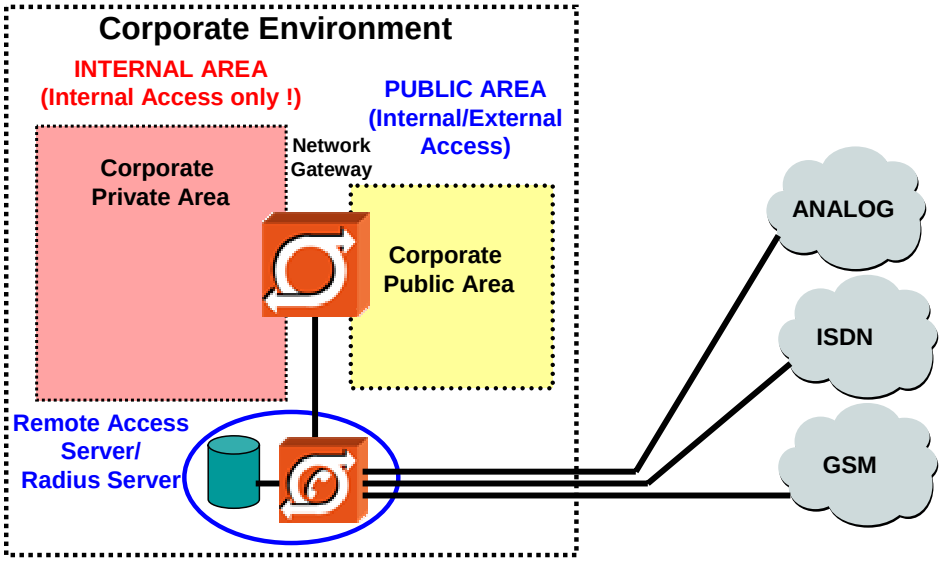


Figure 1.3 Corporate Environment

The workflow within the administrative environment will also be influenced by multimedia technologies (audio and video):

- Computer based Training
- Supervision by the Network/Application administrator
- Video conferences

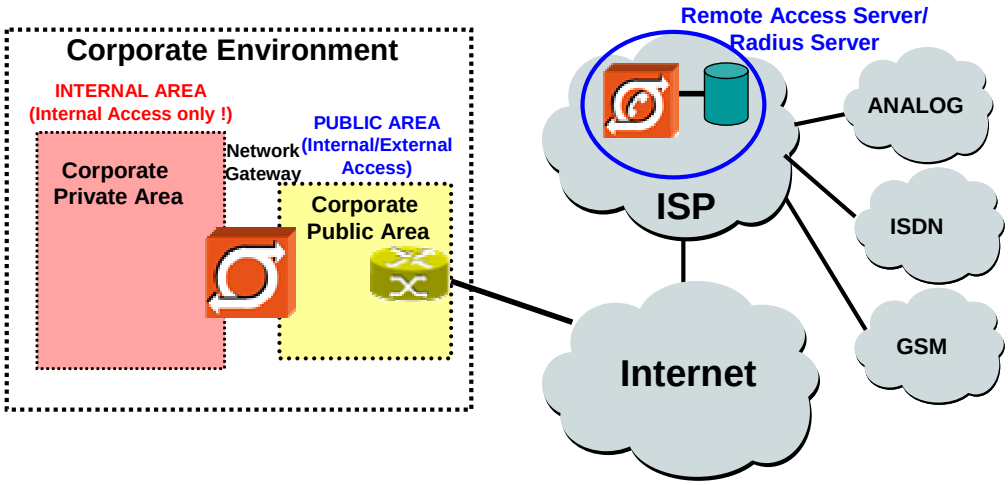


Figure 1.4 Remote Access

1.3.3 The Operational and Corporate Networks

The operational network

In former times almost every lines needed for the operational network were owned by the power/ energy supplier, and therefore under his complete control. This is still valid in some cases, but there were two opposite trends over the last years, changing the situation.

- The first trend was based on the deregulation of the voice/data market. The euphoria resulting out of the new business opportunities induced a considerable amount of investment. Many of the national/international acting power companies extend their long and medium distance power transmission utilities in order to participate in the new alternative Data Carrier business.

- The second trend (following the first one in chronological order) results from the deregulation in the electricity market and the competitive situation in the voice/data market. The power companies that have entered the data carrier market are facing the following challenges:

  - On the one hand the data carrier business did not reach the expectations (the costs for operation and maintenance of the data transmission network were relatively high compared to the possible tariffs for data transmission).

  - On the other hand other power suppliers attacked the core business.

The results of these trends are:

- That just the most essential lines (e.g. for protection switching) was kept private. All connection of the power supplier with "second priority" was treated as a part of the common available transmission bandwidth. Main target was to use as much as possible of the transmission bandwidth for "Carrier Purposes".

- The second trend forces the affected power companies to verify their strategy. The attempt to refocus on the core business sometimes causes reactions that was out of all proportions. Some power suppliers tried to get rid of the whole Data Transmission Area. Outsourcing or even selling out seems to be the appropriate solution to solve the problems. This rigorous proceeding on the other hand causes, that many of the connections/lines used by power suppliers are no longer under their control.

The corporate network

The locations of the Central offices or branch offices very often depend on the necessary customer relationships. This means the preferred choice is not in any case the most cost efficient location (e.g. the company owned campus versus a densely populated city area). Besides the cost factor there are of course several security aspects belonging to the choice of the office area e.g. "Physical Access" to the Network and the belonging components:

- *Access to the Network-Computers, Servers and Printers:* The possibilities to control admittance are in most cases better for a Companies Campus then for rented floor space in a Business Building.

- *Access to the Cabling (including passive components like Ethernet Hubs etc.):* There is basically no difference in the security of a single office (company campus versus rented floor space), because the cable normally does not leave the floor space of the office. The situation regarding security becomes worse, if there is an existing cabling infrastructure within the rented Business Building. There is also a lack regarding security if different offices at different floors have to be connected. Within a rented

Business Building the cables normally runs through false bottom, raised floors or manholes with common access.

- *Access to the Transport Equipment (IP-Router, ATM-Switches etc.):* Within a rented building the rooms for the transport equipment might be commonly used, because they are specific requirements for air condition. In same cases even a shared communication infrastructure is offered as part of the building services.

The interconnection between the different branch offices and the headquarters respectively between the Operational Network and the Corporate Network is mostly done by means of "Leased Lines". Depending on the security requirements this connections may*:*

- share the bandwidth of an existing connection
- be a dedicated connection with a specified bandwidth
- be a dark copper/fiber connection

2 Integrated Services Network Business Benefits

2.1 Introduction

This chapter is focussed on the key business benefits associated with the introduction of an Integrated Services Network (ISN) for power system operational applications that are of primary interest to those responsible for the development of business strategies and the approving of major investments. The chapter outlines the issues and questions that may need to be satisfied in order to support and justify the required investment decisions. It also endeavours to outline the options and alternatives that are available to companies as part of the implementation process.

As stated in earlier chapters this Technical Brochure is essentially a guide for the design and implementation of a new broadband telecommunications network for the provision of an ISN, with particular emphasis on the needs of utility companies.

It is not intended as part of this Technical Brochure to detail the financial information or financial analysis involved in the evaluation of these types of projects but it is intended to highlight the business impact of certain choices in relation to the key technologies involved.

At a basic level, all businesses need to carry out some form of cost-benefit analysis in order to determine whether installing such an integrated service network offers good value for money. The necessity for a company to invest in such a venture is obviously dependent upon a myriad of factors that are expected to be quite subjective to the individual company concerned. The decision processes within companies will also differ greatly between different organisations. In general, however, there are essential key questions that are common to most companies but to which the answers are extremely individual to a company's environment and business strategy at any particular point in time.

These key issues are discussed below.

2.2 Key Investment Drivers for Network Implementation

Future networks need to provide:

- High levels of bandwidth easily
- Absolute security
- Complete Mobility
- "Plug-and-Play"
- Simplicity for service provision and management
- Completely 'open' standardisation
- Highly sophisticated management capabilities
- Maximum flexibility
- Lower Total Cost of Ownership (TCO)

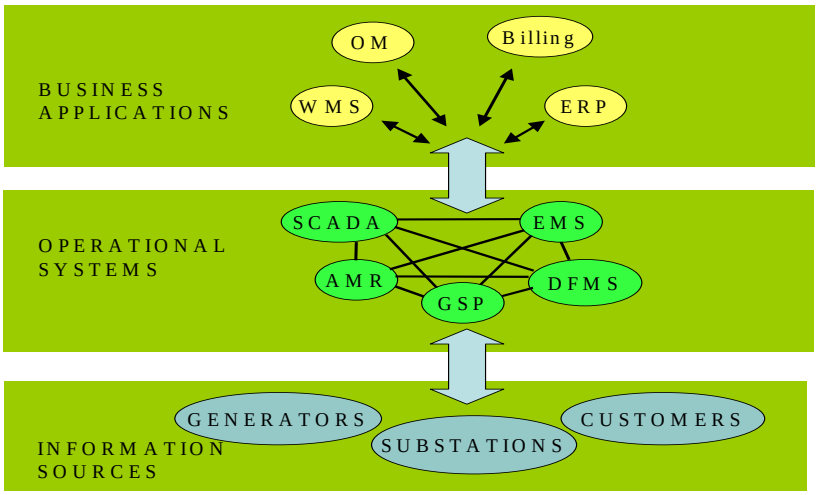


Figure 2.1 Utility Environment

The factors that may influence the investment decision for an ISN include:

- The existing network is approaching end-of-life, either operationally or financially,
- The existing operating costs may be increasing,
- There is decreasing reliability of existing services,
- There are increasing difficulties in the management of growth in existing services,
- There may be pressure to change the service delivery processes,
- The demand for new services as well as the rate of change in technology and demand for higher levels of functionality,
- There may be increasing difficulties in the provision of new services,
- The impact of new regulatory environments (deregulation of the utility and telecommunications industries, changes in competition law, etc),
- The developments in the corporate company (expansions, mergers, acquisitions)
- The push from the technology itself,
- The demand for mobility and remote access,
- The risks associated with not implementing a new network

The right time for the investment is likely to be driven by a combination of the above factors that are critical to the business as well as the overall strategy of the business.

The issues that may influence the timing and scale of investment include:

- The interfacing with legacy systems.
- The need to maximise the return from existing legacy systems.
- The risks with implementing it now or at some later stage.
- The fit with the company's strategy and/or expansion plans.
- The impact on existing services.
- The developments with external suppliers and the real availability of alternatives, not only in terms of products but also in terms of new service delivery models.
- The consequences of remaining with the existing systems.
- The constraints placed on some utilities by governments.
- The impact of integrating power system operational applications with corporate business systems on reliability and availability requirements.
- The comparisons with competing investments.

2.3 Benefits of an Integrated Services Network

The key benefits of implementing an Integrated Services Network (ISN) are discussed below in terms of :

- Financial
- Technologicol
- Scalability
- Serviceability
- Organisational

An important dilemma for most companies is the desire to reduce costs by integrating services and optimising the use of resources and unifying the management of the network and services. However, against this is the need to keep services apart that are mission-critical and that cannot be jeopardised by any means or affected by anything that might happen on the network.

This Technical Brochure is predicated on the use of the Internet Protocol (IP) as the core building block for the ISN. IP can be seen as a service integration approach. Service isolation can be achieved through the use of Virtual Private Network (VPN) and other methods described in later chapters.

The world-wide acceptance and increasing implementation of the IP protocol as the standard network protocol paves the way to new forms of capacity interchange. Utilitising the advantages introduced by the IP protocol, such as flexibility, connectivity, etc, it is now possible to share or interchange capacity at the *network* layer. This integrates different networks at a common network layer based on the IP protocol. *The key advantage of this new approach is that all network infrastructure, including capacity, is now shared by the different users.* It is essential, however, to realise that this will only become true if the proper network architecture is deployed such that the necessary level of *service isolation* and Quality of Service (*QoS) performances* could be guaranteed.

Some of the advantages of IP networks are:

- Service improvements by increased resilience and better performance control
- Improved flexibility through simplified network configuration and re-configuration
- Reduced investment through resource optimisation and TCO reductions
- Access to many different services
- Faster implementation of services
- Ease of sharing information between applications
- Standardised interfaces
- Less management overhead and demand on resources

These are possible provided that the network is designed and engineered properly. Some of the potential disadvantages compared to legacy networks include:

- More complex design and error identification
- Security threats through open standards
- Non-deterministic behaviour (delay)

IP technology, however, is considered the best approach for operational services. There are many papers published and the trend is supported through the development of IEC 61850 standard and the UCA (Utilities Communications Architechture) initiative. There are a number of user experiences in countries such as USA, Japan, Sweden, Switzerland, Portugal, Spain, etc.

The use of IP supports and enables the current trends in substation communication:

- Integration of Protection and Control functions.

- A single protocol providing all functions.
- A single type of communications used for the whole substation i.e. Control and Field bus using the same communication technology, Ethernet and IP.
- The extention of the real time LAN from the Control Centre to the substations.
- Rationalising the IT applications that use substation data.
- The use of intelligent networks to improve the reliability of power system oprations.

2.3.1 Financial Benefits

Financial savings from an integrated service network will arise from the way that the IP technology is deployed. As discussed in previous CIGRE papers and Technical Brochures, the use of IP technology introduces a number of inherent advantages that drive reductions in the overall network cost as well as providing increased performance and service improvements through better availability. The cost benefits are primarily related to asset optimisation and are derived from the fact that IP technology in particular offers the following benefits:

- Standardisation
- Greater resource utilisation through
  - Minimisation of the number of links
  - Significantly better utilisation and life extension of existing links.
  - Integration of existing services
  - Optimisation of link dimensioning as a function of the Capacity and Quality of Service required
- Absolute scalability

Standardisation is a key contributor to the cost of network and refers to vendor compatibility through physical interfaces, data formats and protocols. With standardisation, off-the-shelf equipment can be used that result in reduced prices, standard performance and easier and less costly maintenance over the life of the network.

Performance is improved by the increase in service reliability through the introduction of resilient technologies such as SDH (Synchronous Digital Hierarchy) loops at the transport layers and IP adaptive routing at the network layer. New networking functions provide intrinsic connectivity, distributed data access and integration at the service layer.

In practical terms, where specific cost-benefits are required to justify investment decisions it is preferable if a pilot of a number of applications, ideally spread across a company's operations, in order to quantify the less tangible benefits and critical design assumptions.

2.3.2 Technological Benefits

Technological advantages such as bandwidth efficiency, service integration, architecture flexibility, etc. drive a generic flexibility advantage that paves the way to asset optimisation and future network growth. When the networking technology and the network architecture have been properly chosen, the following benefits can be achieved:

- Network scalability to cope with sustained growth
- Total interconnectivity, which allows any service to be accessed from any network access point
- A high degree of freedom to evolve network performance strategically according to the needs of the company
- Integration of new services

The degree of resource optimisation achieved may be different for every network. It will depend on a number of different factors such as: number of users, classes of services to be integrated, network architecture including internetworking architecture, network growth, etc. This is discussed in more detail in chapter 4.

2.3.3 Benefit of Scalability over Legacy Networks

Rapid technological evolution drives an increasingly shorter life cycle for equipment and services. Demand for new services drives the need to more and more bandwidth through incremental capacity provision. The ability of a network to scale up to these demands is a key requirement.

The 'scalability' of a network can provide real reductions in the TCO by introducing a longer lifetime and thus a higher Return on Investment (ROI) opportunity. Internetworking is the highest expression of applying standardisation at every network layer. It optimises the complete network owing to the standardised interconnection mechanisms and is applicable to all layers.

The key benefit of scalablity of an IP-based integrated services network compared to traditional networks is an important element in the overall business case. This is essenitally future proofing the planned investment by ensuring that the network as implemented can provide not the existing known requirements but also that it will be capable of providing additional and new services by growing incrementally with corresponding marginal investment over the life of the network.

IP technology facilitates increased levels of internetworking between different networks and internetworking offers the advantage of scalability. The technology concerned is suitable for all network sizes from small private networks to vary large public networks. It also allows the network to grow in line with the number of users and the amount of traffic, while at the same time providing new services and capabilities. This is particularly attractive to utilities considering providing services to third parties.

With fast emerging technologies the capacity to scale the network beyond present capabilities is essential and needs to be considered in a number of dimensions, including bandwidth, routing, addressing, QoS, user service provisioning, and security.

2.3.4 Service Provision Improvements

The use of a single communication platform to provide the range of services required for the operation and control of Power Systems is the major benefit of an integrated service network. The intrinsic connectivity and flexibility of IP technology provides the capability of increasing information flow between applications. This provides end-to-end transparency that facilitates service provision and management.

2.3.5 Organisational Consequences

The implementation of an Integrated Service Network (ISN) will present opportunities to examine the delivery of services and also the supporting organisations both internal and external to the company. Traditionally companies may separate responsibilities for the provision of voice and data or the provision of corporate voice and data from power systems operational voice and data services. The trend from fixed to mobile applications is another area that may have been treated separately. Some companies may also have a mix of internally and externally provided network services.

A key issue for utility companies is their approach to the growing trend in the convergence of not only the different types of data services but also the convergence of voice and data services. A major benefit for companies examining the business cases for implementation of ISNs are the opportunities that an integrated network approach will present in the delivery of existing and new services through more efficient use of all the resources involved.

A concern for some companies may be managing the change in the skills and expertise required with more and more emphasis on IT skills are required compared to traditional telecommunications. On the other hand, there may be cultural issues required by IT personnel in terms of dealing with mission-critical power system telecommunications systems compared to corporate office applications.

2.4 Comparison of Alternatives

The alternatives available to a company will depend to a great extend on how the existing services are presently delivered, the strategy towards future delivery of these services and other non-operational services, the necessity for provision of new services, and the availability of external network providers.

At a high level, the options open to a company outlined below are based on the following assumptions:

- The existing operational services are internally provided by a network or combination of networks that are primarily dedicated to the provision of Power System Control services such as telecontrol and operational voice

- The operational services are separate from the provision of corporate services

The generic options can be described as follows:

1. Develop a 'greenfield' network, i.e. a completely new network without any legacy systems.
2. Develop a separate dedicated IP network for operational services and migrate existing services over time.
3. Migrate the existing and new operational services over the existing corporate IP network. The existing corporate IP network may be internally or externally provided.
4. Provide the operational services through an external commercially available network.

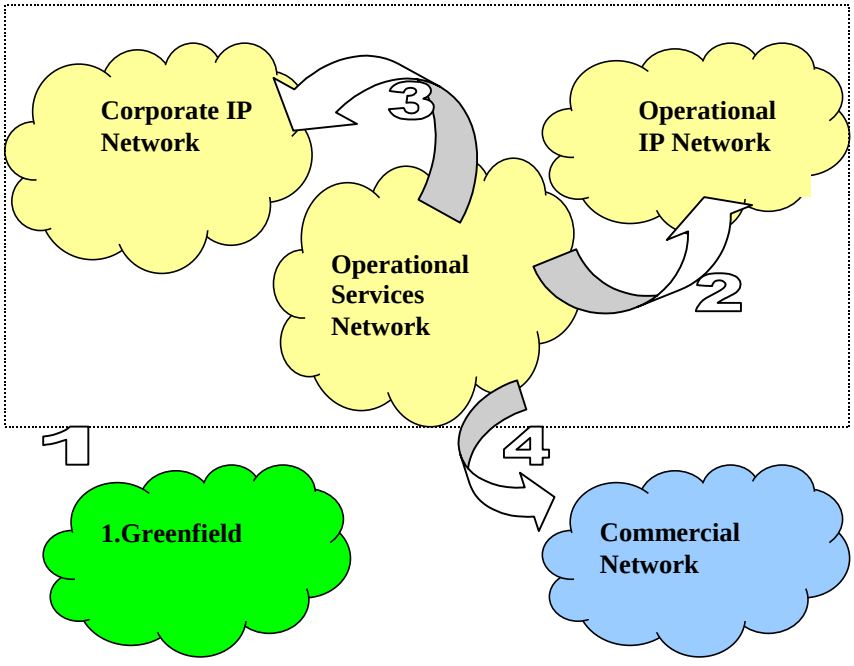


Figure 2.2 Network Implementation Options

The final implementation may be some combination of the above. The implementation on a site by site basis is discussed in more detail in chapter 5.

Although based on the same technology, design and operation principles, externally and internally provided IP networks present significant differences relevant to the provision of critical operational services.

Public networks tend to be designed using statistical dimensioning while private networks have to be designed using deterministic non-blocking methods.

Utilities must always be sensitive to the fact that mission critical applications are a great concern to their business but are just another customer for a service provider. It will depend very heavily on the effectiveness of the SLA (Service Level Agreement). The details of the elements of a typical SLA are discussed in more detail in chapter 3.

2.4.1 Service Provision from 'Internally Provided' Networks

The term 'internally provided' network is used when the physical network and its management are under the control of the Utility and formerly designed to provide Power Control operational services.

The internally provided network allows for full control of design and performance. QoS can be customised for every user/service and if the network is properly designed, fixed service guarantees can be achieved.

In spite of their limitations, externally provided networks may complement an internal Power Control network if the proper Service Level Agreement is defined and the intrinsic characteristics of the service are understood.

Figure 2.3 shows the different possibilities that can be found in the scenario of internal and external IP service provision.

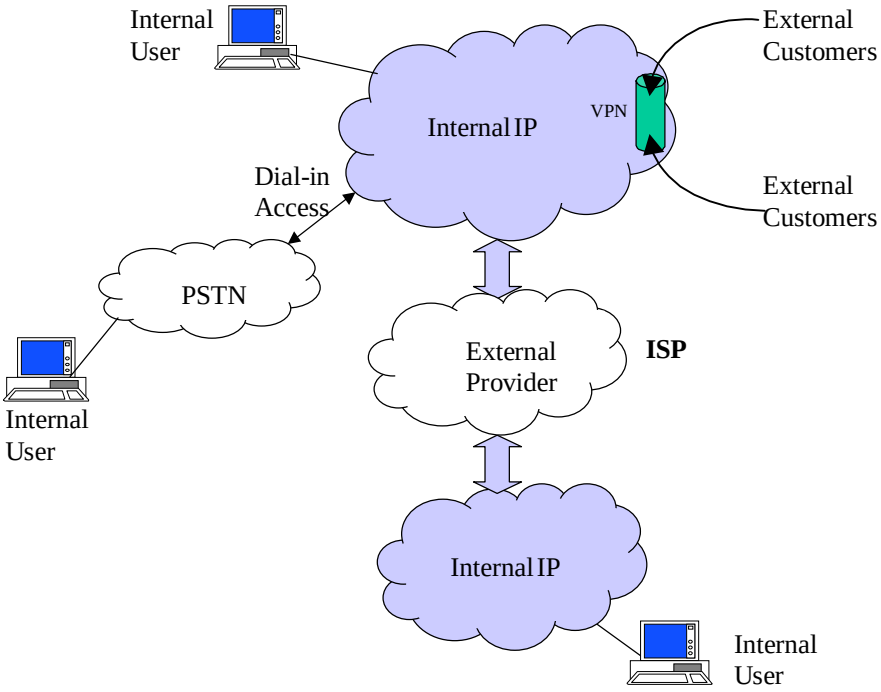


Figure 2.3 Internal and External Network Provision

The major advantage with an internally provided network is that it is under company control and provided it is given sufficient resources and funding will give the level of service required. Public Internet services can be subject to peak time loading delays over which there is no control.

One major problem with internal networks is the management of the capital investment. The technology for hubs, bridges, routers, etc that make up an IP network comes mainly from the

IT world. Networking products have a market life span of typically 5 years. Utilities are used to manage long life assets with life cycles of up to 40 years.

Installation programmes for IP network projects of even three years may mean the equipment specified at the outset is not available, or has been superseded, at the end of the project. Maintenance and replacement need to be managed entirely differently for IT networking products than for utility traditional assets. New techniques and policies have to be developed to deal with these differences.

Another disadvantage with the internal network is the speed of technological development. Once the investment has been made, it has to be constantly updated to keep pace with the services that users will demand; this is especially relevant for corporate services.

Public telecommunications operators are constantly developing new products reducing the cost to the end user whilst offering service enhancements. By and large technology developments are transparent to the user. Convergence of data and voice on routed IP networks is further reducing costs by sharing bandwidth between data and voice.

2.4.2 Service Provision from 'External Provided' Networks

While considering features of the externally provided networks it is worth noting that:

- Externally provided networks are normally designed to provide a service level and availability fulfilling the ITU-T recommendation, which is at least one order of magnitude lower than required by some critical operational services like Teleprotection.

- They offer few differentiated classes of services- up to four- and cannot be customised to be adapted to specific service requirements. An open QoS architecture with hard guarantees accepting the Reservation Protocol (RSVP) is not commonly supported.

- Traffic engineering is carried out using standard traffic models instead of the actual traffic profiles. This could introduce significant errors that could impair the service performance.

- Design, dimensioning and expected performance of the network is carried out by means of probabilistic estimation based on the laws of large numbers, which provides loose guarantees - statistical- instead of hard guarantees.

- Power Utility services are not the core business of external service operators. No specific service development may be possible.

- In the event of an outage, there is reliance on the external service provider, who may not realise the importance of the network for the utility's business.

When considering an external network provider it is important that there is a geographical match between their network presence and the locations where services are required, both now and into the future.

The service provider's network architecture needs to be examined in detail in order to ensure that there is adequate capability and flexibility to provide the service levels and quality of services required.

2.4.3 Network Implementation

Existing private networks can be generally categorised into two types - dedicated WANs (Wide Area Networks) that permanently connect together multiple sites, and dial networks, that allow on-demand connections through the Public Switched Telephone Network (PSTN) to one or more sites in the private network. WANs are typically implemented using leased lines or dedicated circuits - for instance, Frame Relay or ATM connections - between the multiple sites. Customer Premises Equipment (CPE) routers or switches at the various sites connect these dedicated facilities together and allow for connectivity across the network. Given the cost and complexity of such dedicated facilities and the complexity of CPE device

configuration, such networks are generally not fully meshed, but instead have some form of hierarchical topology. Private dial networks are used to allow remote users to connect into an enterprise network using PSTN or Integrated Services Digital Network (ISDN) links. Typically, this is done through the deployment of Network Access Servers (NASs) at one or more central sites.

An increasingly common solution for a company's networking needs is a virtual private networking (VPN) solution. A VPN is defined as a network of virtual circuits that allows users to conduct private communications through public or shared infrastructure. An IP-VPN is a virtual private network that uses the Internet Protocol (IP) for routing.

There is growing interest in the use of IP-VPNs as a more cost-effective means of building and deploying private communication networks for multi-site communication than with existing approaches. VPN simplifies the outsourcing of telecommunications services by providing a virtual point-to-point link that does not require the user to be involved in maintenance functions or to have knowledge of the network that supports their services.

3 User Requirements

3.1 Introduction

This chapter introduces how services are defined. The content, mainly addressed to network users, introduces the different aspects that need to be considered to define a network service.

The success of an ISN deployment depends to a great extent on the mutual understanding between clients and service providers. This chapter introduces the key aspects that allow service agreements to be properly defined.

3.2 Service definition

The definition of a service requires in-depth knowledge of applications characteristics and its requirements. As shown in figure 3.1, a balance has to be obtained between the working characteristics of the applications and the service level offered by the network in order to fulfil the application requirements.

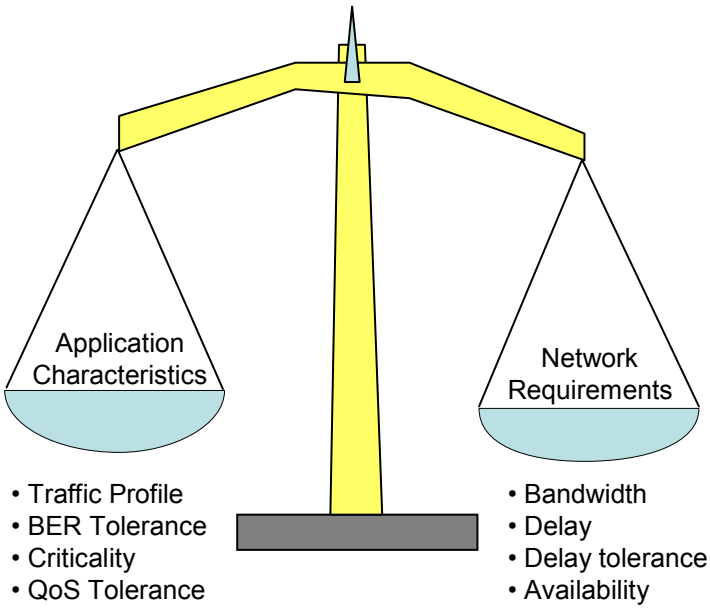


Figure 3.1 Application Requirements

Traffic profiles and traffic estimates will need to be determined in order to properly dimension network capacity. Estimates can be difficult to gauge with appropriate levels of accuracy, so that actual traffic measurements on a trial site may be needed. When contemplating the overall network design there are a number of simulation packages available that can predict the network performance for given traffic conditions.

There may be a number of services required to a site. For example a network for corporate applications purposes may be a fully managed service provided by the Public Telecommunications Operators (PTO) whereas a network for operational data services may be provided with the utilities' own networking equipment to obtain the level of service required. (PTOs usually have a service handbook available that will describe the type of service available the level of service that can be expected, presentation, prices etc. The

service handbook may be a source of useful information and give any limitations on the service being considered).

The following outlines the key characteristics of typical utility operational services:

Operational Service	Telecontrol SCADA	Operational Telephony	Corporate Data	Tele-protection	Video Surveillance
QoS Requirement	Non-critical real-time QoS	Real-time QoS	Best-Effort	Very critical real-time QoS	Real-time QoS
End-to-End Delay	Less than 1 sec.	Less than 150msec.	Less than 1min	Less than 10msec.	Less than 2sec.
Service Availability	> 99.98%	> 99.5%	> 99.5%	> 99.99%	>99.5%
Bandwidth	Low	Low	Medium - High	Low	Low-High
Bit-error Tolerance	High	High	High	Very Low	High
Variable Delay Tolerance	High	Low	High	Very Low	Low
Flow Control Required	Yes	No	Yes	No	Yes

Table 3.1 Service Key Characteristics

3.3 Security Requirements

It is possible to divide the security into three different aspects:

- Security of the data, in terms of integrity and availability.
- Security of the equipment, in terms of redundancy and access.
- Security of the network in terms of internal and external interference. This refers to deciding those parts of the network and services that must use firewalls, encryption, or VPNs and those parts of the network that do not require special protection (this part is used to be called DMZ (De-militarised zone)).

The first step is to define a security policy. This needs to define what is permitted for different users. The best way is to consider that if it is not allowed, it is forbidden. The grade of confidentiality of the different information and services must be decided, and who can get access any piece of information. It is important to consider that internal staff carries out 75% of the attacks.

For assessing security performance there are a number of software applications that can simulate attacks. These applications can be initiated periodically. Some examples of Software are SATAN, ISS (Internet Security Scanner), Strobe, NSS, etc.

3.4 Scalability Requirements

Scalability in a network means that it has been designed to remain stable while undergoing rapid growth in the number of network channels, the number of attached computers, and the amount of network bandwidth. The goal of scalability has an effect on a wide range of engineering decisions, including, which network protocols are supported and what kinds of equipment are used in the network.

Scalability is essential to any business that wishes to achieve a sustainable growth scenario. The network needs to be able to grow in capacity without technological limitations in order to

realise the capital and operational investments. In a properly designed network with built-in scalability, the total cost of ownership should be reduced as the network grows.

There are a number of approaches to providing scaling in networks:

- Increasing capacity by additional network devices, i.e. horizontal scaling. The complexity of the management of the network may limit how much this can be applied.

- Improving the network architecture needs to be designed at an early stage of the project and should enable the network to be built and operated at a lower cost. For example, moving service functions out towards the edge devices can reduce the need for end-to-end computing, while some applications may merge the router and application access functions.

- Increasing capacity by upgrading hardware specifications, while maintaining the same physical equipment size, i.e. vertical scaling. This applies mostly to the core level and will simplify network management but generally at a higher cost than horizontal scaling or improving architecture.

There are a number of key aspects that need to be considered in relation to scalability.

- The technological limitation refers to the choices of the physical medium such as fibre or radio, (in some cases capacity may not be the determining factor in the growth of a network but speed and ease of provision). It may also include choosing between of PDH versus SDH, taking account of the switching limit of IP, ATM, etc, as well as the nature of the internetworking model employed.

- Architectural flexibility is important in terms of the ability to integrate and adapt new services.

- The rate of change in technology in terms of both hardware and software at the core, edge and access network levels will not generally be synchronised and the evolution of this architecture must occur with impact on services. The network management system may also need to grow in line with the growth of the network. This can refer to the actual licensing arrangements for the number of users as well as the functionality of the management, e.g. the ability to automate some functions as the number of network devices and users grow.

It may also be important to have some degree of flexibility in the way maintenance is carried out on the network and if there are ongoing changes in the organisation or customer base it may be desirable that the network topology can adapt to geographical changes.

Internetworking offers the advantage of scalability, the technology being suitable for all network sizes from small private networks to vary large public networks. It also allows the network to grow in line with the number of users and the amount of traffic, while at the same time provide new services and capabilities. This is particularly attractive to utilities considering providing services to third parties.

With fast emerging technologies the capacity to scale the network beyond present capabilities is essential and needs to be considered in a number of dimensions, including bandwidth, routing, addressing, QoS, user service provisioning, and security. For example, MPLS has largely evolved from the need to use the high speeds of existing technologies, such as ATM, with existing router networks, by seamlessly integrating the connectionless nature of IP to the connection capability of switches.

Security architecture may impair scalability. Amongst several other aspects, it has to be mentioned the limitation introduced by the Internet Key Exchange protocol (IKE Protocol) in which every node must be linked to every other node by a unique key. A new version of IKE is planned to overcome this problem by generating new keys using a certificate authority.

Another problem is that IPsec (Ref. RFC 2401) requires every user to have a defined public IP address. Many private networks are using Network Address Translation (NAT) to share addresses and thus will end up sharing security privileges.

3.5 Management Requirements

Network Management is one of the most important aspects in the telecommunication networks and often, it is one of the most forgotten.

At an organisational level, it is necessary to decide whether this function will be provided internally or by outsourcing.

One of the disadvantages of the second option is that the control of the network is hhanded over to people outside the company, who may not have the necessary knowledge and experience of the applications particular to the utility's businesses. On the other hand, the outsourcing option has other benefits. There is no need to employ the highly specialised technical personnel and to invest in the skills that require continuously upgrading. The outsourcing company is generally following the development of new technologies.

However, it is essential that the outsourcing contract be carefully managed. It is critical to write a Service Level Agreement (SLA´s) with the outsource company to ensure that a proper service is delivered.

Generally, a mix of these options is used by many companies. For example, the e-mail service can be outsourced, but the management of the enrolments, drops and modifications of the e-mail counts can continue in-house. Or the telecommunication part of the network can be outsourced, but not the application part.

According to OSI, the functions in the structure of TMN (Telecommunication Management Network) are the following:

Fault: How to manage the alarms of the different network elements.

Configuration: It involves configuration services, elements, circuits, etc.

Accounting: How to measure the use of the services, network, etc, by the customers. Many times it is oriented to billing. If the telecommunication unit of the enterprise is not consider as an external or internal service provider it is not necessary this item.

Performance: The way of measuring the performance. It can imply the recollection of statistics and the creation of informs.

Security aspects: It implies the auditing and protection of the access, changes or modifications of the network elements, the services or the information that they carry.

All these areas must be taken into account in the elaboration of the requirements.

The management architecture is considered to be composed of different layers, each one gives services to its upper layer:

Management element layer: It manages the network elements

Management network layer: It manages the communication network.

Management service layer: It manages the services of the network.
Business Management layer: It manages your own business.

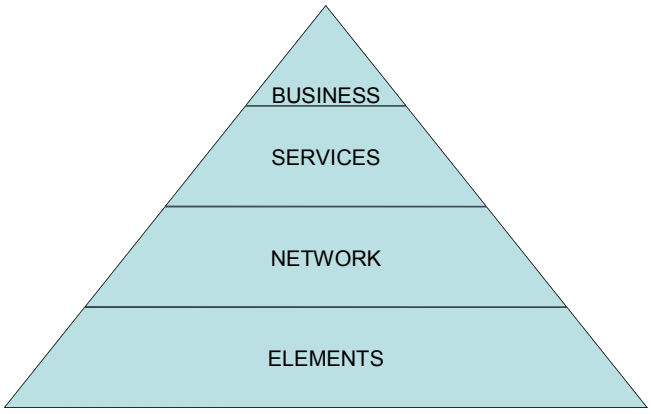


Figure 3.2 Network Management Layers

Nowadays this is structure applies until service level (in some cases only until the network layer), and this is generally only with the products of the same manufacturer. It is very difficult and costly to have a fully integrated management system in a multivendor-platform.

In developing the management requirements, it is necessary to decide the level of integration that is required in the functional groups of TMN described above.

Another aspect to consider is the organisation structure of the management of the network and services. It is necessary to decide the number and location of the Network Management Centres. There may be a requirement for a hierarchy of Network Management Centres and to decide on the various key skills required.

The level of security required has to be decided, in terms of the company corporate security policy through to the security requirements for each department or application.

3.6 Contingency Requirements

Network contingency, and in particular, emergency recovery, plans are a necessity in today's utility environments and adequate planning is essential in order to mitigate a potential disaster or to prevent it from happening in the first place. Some contingencies cannot be entirely avoided, but having a solid continuity plan in place is required in order to ensure that the critical services are not immobilised.

While a major drive and benefit of IP networks is the integration of services, the design process must take into account the impact of potential common mode failures on the individuals services.

With the drive to decrease costs, networks are designed such that more and more equipment is consolidated, which decreases operations and maintenance costs but increases the impact of common mode failures. Networks need to be designed that possess fast recovery from any changes or scheduled downtime, data security and interoperability problems, while realising a lower cost of ownership.

3.7 Service Level Agreement

An essential mechanism to ensure the successful provision and operation of network services from an external provider is a comprehensive Service Level Agreement. The primary parameters that go to make up such an SLA include:

- **Service Availability:** The frequency, duration, and timing of service failures need to be determined for each service.
- **Bandwidth:** This is the bandwidth available to the different services and may include some flexibility in how this is applied.
- **Delay and delay variation:** It will be necessary to specify this for each application.
- **Data security:** Again, this will be specific to different applications.
- **Power faults correlation:** For services that are critical during power system disturbances, it may be important that specific additional precautions are specified.
- **Penalties:** While penalties may not compensate for loss of critical services, they do focus a service provider's attention on the need to accurately monitor the SLA guarantees.
- **Mean Time to Repair (MTTR):** It is important that there is adequate confidence in the service provider's ability to respond to service failures and carry out the necessary repairs in an acceptable time.
- **Service isolation guarantees:** This refers both to isolation between internal and external traffic, as well as between different internal services.
- **Physical redundancy check (reliability):** This may specify the level of redundancy required for example at a network level, an equipment level, or at specific locations.
- **Power backup:** This is critical for those services required during power system disturbances. It is important to ensure that rural switching locations have sufficient standby arrangements.
- **Performance reports specification:** It is important that meaningful and comprehensible information is provided in a timely fashion. There is very little use in providing vast amounts of data but very little information.
- **Qualified workforce availability:** Obtaining and holding on to qualified personnel is an increasing difficulty for service providers. It is important to ensure that a potential service provider has sufficient depth in their workforce. It is also worth examining that they have the right number of personnel in the right locations in order to ensure that response time guarantees are realistic.

4 Network Design

4.1 Introduction

Network design could be a complex task depending on the network size and the number and type of services supported. This chapter is intended for network implementers that want to understand some of the specific and detailed network design techniques involved. The chapter is focused towards the design of Integrated Service Networks (ISN) for power utilities. Although the use of IP technology is assumed, other technologies are also considered as being used in ISNs in combination with IP.

Complex mathematics is involved in network design and generally cannot be achieved without the use of appropriate algorithms. Common sense and experience is as well a necessary component to achieve a good network design. The body of the chapter introduces the details of the design process whilst the mathematical formulation has been moved to appendixes A, B and C. A list of comprehensive references has also been included in the reference list.

With this structure, the body of the chapter is self-contained and useful for those designers wishing to know the details of modern broadband networks. For those wishing to know the mathematical principles behind the algorithms and techniques mentioned throughout the chapter, please refer to the appendixes and the related references.

4.2 Description of the overall network design process

Network design is a trade-off between the four main characteristics:

- Requirements
- Cost
- Performance
- Reliability.

The best design is the one that at the lowest cost can achieve the performance and reliability goals set by the design requirements. It is recommended to use the top-down design approach, i.e. begin with the application layer and its requirement. These requirements not only affect the design of the application, but will also have influence on the lower layers.

Network design implies the definition of every aspect of the network from its topology to the capacity of links and nodes as well as the choice of the algorithms that support the services. Based on the business policy, the company financial strength and its competence in communications, an organisation will have to decide whether to operate the services or network itself or whether total or partial outsourcing is a more desirable option.

An organisation will also have to define its external service plan in order to define the interconnection with other networks or service providers. The plan will regulate the relation between the company and the external communication customers and/or external service providers. The external plan will also define to which degree its services will provide full interoperability across service borders and across network borders.

Figure 4.1 shows the straightforward process of the network design life cycle. Although not shown in the diagram, after the completion of every step an evaluation process is carried out to analyse the feasibility of the results. When these results do not fulfil the specification, one or more previous steps have to be repeated or the general project baseline modified. Network design is an activity that has to be considered as a part of the necessary network maintenance and update and thus will continue during the whole network lifetime.

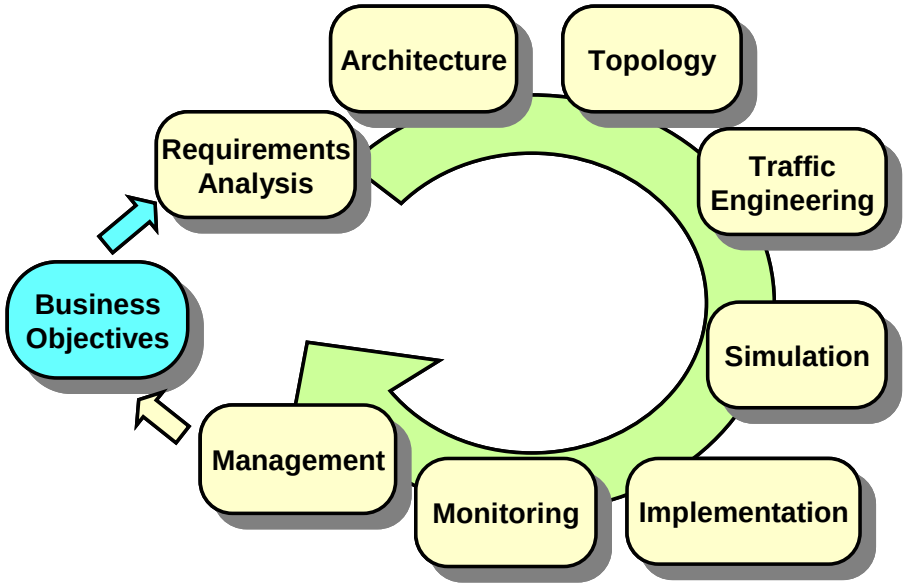


Figure 4.1 Network design life-cycle

Based on the business objectives that define the overall communication performance required by the company, the design of any network has to start with an investigation of the existing and potential users to produce a listing of the required services. These services have to be quantified and broken down to produce a Quality of Service (QoS) specification (see Table 3.1 in chapter 3). This specification should be expressed by means of the corresponding QoS parameters such as availability, capacity-profile, accepted error tolerance and delay parameters. A requirement specification based on these parameters will make up the basic specification for the network design.

This specification will include amongst others the following information:

- Number of services to be integrated in the network
- Class of service specification
- QoS objectives for every service including availability level
- Traffic profiles of every service user obtained from the application profiling process
- Budget
- Any existing constraint such as:
  - Topological constraints
  - Reuse of existing equipment
  - Technological limitations, etc.

The choice of the service network technology depends on the type of service to be offered by the network and on the service integration architecture chosen. Real-time services such as SCADA, Telecontrol and Teleprotection are fundamental to Power Utility operations. The integration of such services in an IP network is highly attractive. However, the integration of Teleprotection in the service layer is not possible at present. IP networks offer bandwidth optimisation, survivability, reliability, low cost, proven technology and vendor independence, but the basic protocol suite is a best effort technology. To meet those requirements imposed by real-time services like bounded delay and delay variation, guaranteed bandwidth and a high degree of priority, new components have to be added in order to achieve the desired QoS performance. In few words, the present trend in network design is to use the new IP architecture capable of giving Quality of Service (QoS) to those services under request.

The Quality of Service (QoS) is an essential feature of any modern network design. It allows the user and/or operator to differentiate between services and determines the degree of reliability of a certain service. Examples are services that require low delay or bounded delay variation.

The quality of service, in terms of delay and packet loss, depends not only on the network actions but also on the current load. Traditional Internet protocol suites cannot assure the QoS. Thus, present IP-technology cannot be applied to critical services such as Telecontrol and Teleprotection unless some specific mechanisms are added in order to guarantee bandwidth and/or delay. However, in recent years there has been a great amount of research activity devoted to the development of new network architectures and service models oriented to obtain guaranteed QoS levels. New versions of IP look set to deliver time-critical QoS-specified services.

Traditional networks are often dimensioned according to the data-traffic or telephone- traffic and some rough empirical guidelines. Both these methods work fine for networks based on non-critical services. For Mission-Critical services, the design of the network should guarantee availability and serviceability. This cannot be achieved with a design based on statistical approximation but with one based on firm guarantees. This design principle requires accurate simulation and monitoring phases specially when IP or IP over ATM technologies have been chosen whether in the service layer or in the access interfaces.

The implementation of a network supporting different services requires carrying out a complete project baseline. Some generic data as well as some service specific data have to be gathered in to complete the project requirements.

The following information will be required for the implementation of a network supporting pure data services:

- Make an overview of all data applications needing communications.
- Define what applications/users require communications. Make an overview of what resources are in use and how much.
- Find the load during the busiest hour of the day.
- Build a table to show how the traffic flows between the various nodes.
- Estimate the capacity needed for routing-information and other administrative traffic.
- Dimension links and nodes capacity so that the average load over any one period never exceeds 50% of the total capacity.
- For critical applications or large networks add resources to give sufficient resilience.
- Identify maximum end-to-end delays.
- Assess additional capacity required for expected future growth

Various methods have been used to model the traffic in telephony networks. These include models such as Erlang, Poisson and binomial distributions. Most commonly used is the method known as Erlang B. This method gives the relationship between the traffic level, the number of trunks and the expected blocking rate of the network.

To dimension networks with mixed services the following information will be required:

- The number of traffic sources.
- Individual capacity requirements - both average and peak.
- The delay requirements of each service.
- Availability requirements of each service.
- Capacity of routers and switches.
- Capacity of transport links.
- Error performance of these links.
- Availability requirement of each network component.

Once the design process starts, it could be possible that the design requirements together with the constraints applied to the selected network technology do not result in a possible implementation so a re-negotiation of the requirements would have to be carried out.

After the monitoring process that will verify the correctness of the actual network implementation, the Network Management information will give an indication to evaluate if the network is covering the business expectations. The analysis of this information together with any change introduced at the business level would be used to decide if the whole process has to be started again.

It is widely accepted that the best choice for the design of a network that integrates several services is an internetworking solution. This approach makes the design process even harder to accomplish since the best solution is the one that combines different networking and transport technologies to obtain the cheapest solution that fulfils the design goals.

Although there are design tools that could help in this process, there are no accepted rules for the design as it is a multidimensional problem without a mathematical solution. That is to say, it cannot be proved that a network is an optimum design, but can only be stated that is better than another one. Due to this, the objective of the network design process is to achieve the objectives set in the network design specification.

The main points in summary are:

- *Scalability:* A well designed network should be scalable with the potential to grow with increasing requirement.
- *Open standards:* The entire design and the components that build the network should be based on open standards.
- *Availability:* The applications requirements assuredly demand a level of availability and reliability of the network, including QoS.
- *Modularity:* An important concept to adopt is the modular design approach in building a network.
- *Security:* Considering security risks and taking care of them in the design stage of the IP network is essential for complete certitude in the network.
- *Network Management:* Implementing Network Management should be integrated into the design of the network from the beginning.
- *Performance:* There are two key forms of performance measures, throughput requirement and response time, that should be considered for the network.

Figure 4.2 shows the detailed network design process. The rest of the chapter explains the details of the technologies or techniques used to carried out every of the tasks that will allow a completed design to be obtained.

Figure 4.2 shows the details of the basic concepts introduced by figure 4.1.

The most important steps of the design process are:

- The preparation of the design specification documents which gathers information form the service demand, the company policies as well as the site location and asset availability.
- The topology design that will drive to the definition of the internetworking architecture which implies the selection of the technology of every one of the layers that form the model.
- Service integration and mapping.
- The definition of the management architecture including that of the management centres.
- Security architecture.
- Routing design and set-up as a function of the naming and addressing and the service mapping.

- Traffic engineering techniques and tools to assure the service level specified as a function of the topology network architecture and routing design.
- Finally, once the final network design is obtained, a simulation of some services or a part of the network could be advisable as a function of the technology and architecture selected.
- Once the design has been fully validated, the network can be implemented.
- Using the network management tools a report about service performance could be obtained to check the need for a network redesign.

Other aspect like risk assessment, contingency planning or reliability considerations are not shown in the diagram but developed throughout the chapter.

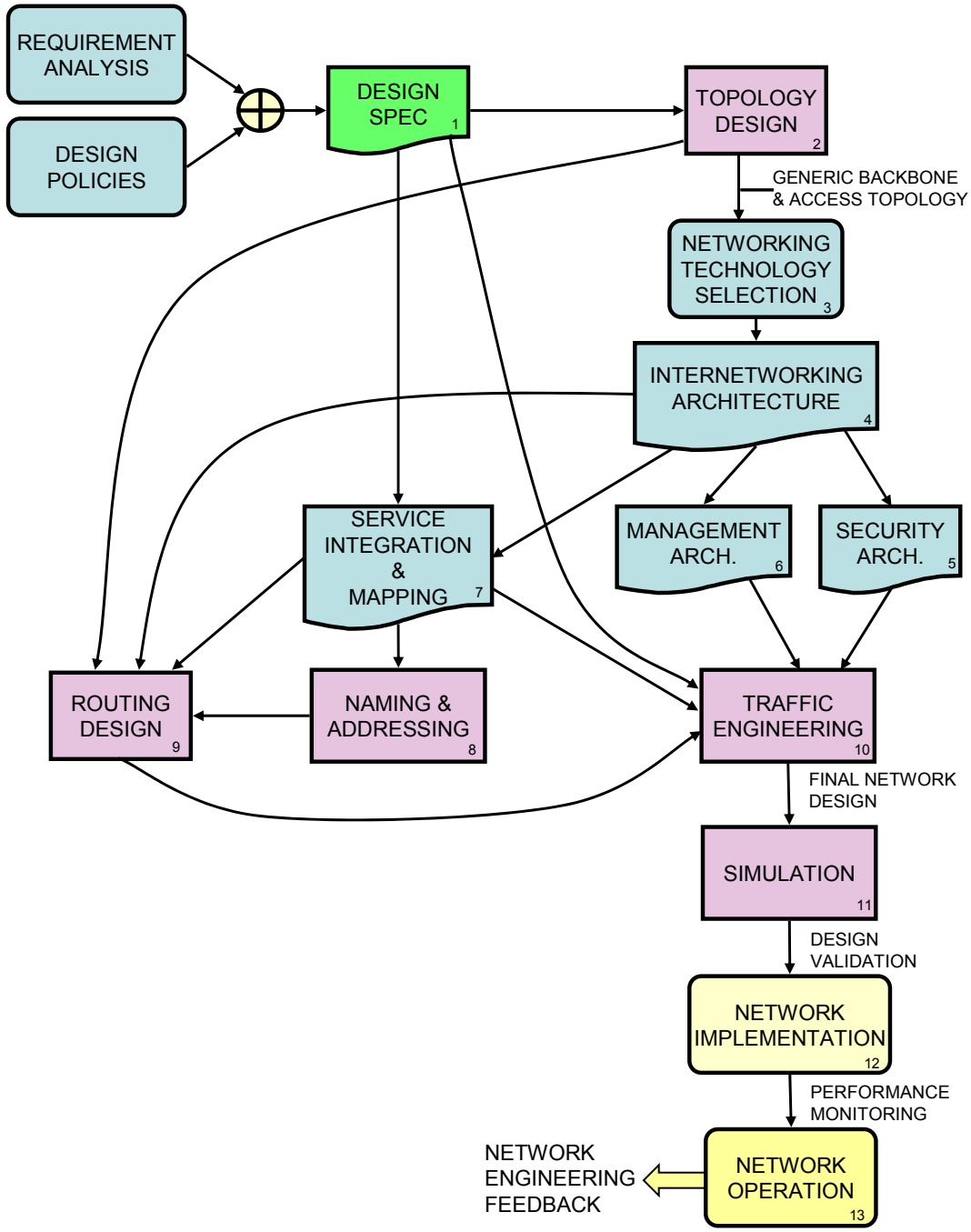


Figure 4.2 Network design and operation process details

4.3 Evaluation of risk

In general, the advantages of using IP technology can be mathematically evaluated before the actual deployment of the network so that we can forecast the saving and the Return of Investment of our communication infrastructure.

However, risk evaluation is not so easy to determine since no major intrinsic technological risk can be identified in IP technology. Possible risks are closely related with network design procedure and most of the above-related advantages and improvements depend on how the network has been designed.

IP networks require a quite different design approach. Some network performances and some advantages can only be guaranteed by means of the proper design of the network. The main aspects to be considered are:

- The right topology to achieve service availability
- The optimum capacity for links and nodes. This issue is more relevant at the network edge than at the core.
- The QoS required by the user.

On the other hand, network design should avoid possible network instabilities caused by:

- Routing topology interactions or improper routing schemes.
- Addressing scheme mismatches or limiting addressing schemes.
- Congestion problems due to poor traffic engineering.

Other generic threats have to be avoided:

- Common mode failure due to Service Integration. A contingency plan that considers this circumstance has to be prepared.
- Lack of specific trained people. Specific training will have to be arranged. Intrinsic connectivity will significantly reduce the number of top level specialist.

4.4 Contingency planning

Network contingency, and in particular, emergency recovery, plans are a necessity in today's utility environments and adequate planning is essential in order to mitigate a potential disaster or to prevent it from happening in the first place. Some contingencies cannot be entirely avoided, but having a solid continuity plan in place is required in order to ensure that the critical services are not immobilised.

While a major drive and benefit of IP networks is the integration of services, the design process must take into account the impact of potential common mode failures on the individuals services.

With the drive to decrease costs, networks are designed such that more and more equipment is consolidated, which decreases operations and maintenance costs but increases the impact of common mode failures. Networks need to be designed that possess fast recovery from any changes or scheduled downtime, data security and interoperability problems, while realising a lower cost of ownership.

The inputs to the design process are the set of network and service contingencies that can reasonable be forecasted and need to be taken into account. The output is the incorporation of recovery plans that are either fully integrated into the network design or set out as separate discrete actions that are initiated either automatically or manually.

Contingency plans should be developed for scenarios that involve failures internal and external to the network, as well as for scenarios that impact the sources used for delivery of services.

It is important to recognise that wherever redundant parts of a network share certain characteristics, they may both be simultaneously vulnerable to the same common threat (e.g. multiple systems sharing a power feed may all fail if the supply fails).

Network planning teams can simplify network design and contingency planning with the use of integrated planning tools that model capacity and enable architectural planning of the network. Implementation of contingency plans can benefit from auto-discovery functionality in equipment to assist with network re-configuration.

Sensitivity analysis is very useful to contingency planning in outlining the effects of sudden increases or decreases in traffic. A decrease in traffic is normally viewed as reserve capacity, but events that may cause saturated bandwidth of the network, or parts thereof, may require fast reallocation of resources.

Contingency planning includes:

- identifying & documenting the critical services
- identifying network resource requirements
- Identifying critical services and users
- identifying & documenting recovery procedures
- develop specific network recovery procedures

4.5 Traffic Profiles Definition

Network design and performance analysis are two of the main tasks to be performed in order to assure that a specific network meets the service demands that originated its need. To test a specific network design against a specific Service Level Agreement (SLA) – that is to say, to do a performance analysis – some characterisation of these services is needed, as the network is going to behave according to the service behaviour. The services are specified through modelling the traffic sources of its users as individual sources, as well as the aggregation of multiples of these sources, thus obtaining results for the individual or aggregated streams.

Once there is a network design, a set of SLAs agreed with the different users, and the required traffic profiles, the necessary analysis may be done by one of the following approaches: Mathematical analysis or simulation.

It is clear that the models used for each component, i.e. the network, the SLAs and the traffic flows, are closely related to the chosen analysis method as well as the models chosen for each of the other components. This leads to the existence of different model "families" which correspond to different network-wide assumptions and analysis methods.

4.6 Design Policy

The process of planning an ISN includes several tasks, both technical and non-technical. Depending on the starting point, there are several aspects that could be of main interest:

- Operational costs
- Reliability
- Transmission Capacity
- Manageability

At the end there needs to be a network solution that satisfies all points of view and considers all requirements. Considering this complexity, it is understandable, that the execution of the whole process takes several steps.

Each of the different steps are accompanied by decisions. Some steps has to be executed several times, to optimize the result. The step for a rough subdivision of the Network planning process deal with the following aspects:

- Principle need
- Range of action for the network
- Expectations for the IP-Traffic
- Basic architecture of the network
- Topology and Dimensioning
- Depiction of the IP-Network to the Transport-platform

At the very beginning of the process there is the decision to build a new IP-Network respectively to extend an existing Network. In some cases it is relatively difficult to ascertain the demand justifying a new or bigger network. Sometimes non-technical reasons like business administration aspects, company strategy or outsourcing strategy plays an important role.

Based on the previous considerations the special kind of the net as well as the catchment areas can be derived.

As a matter of priority the following points has to clarified:

- Users
- Purpose of the network
- Applications

Answers to the previous points are also depending on the principle type of the net. A transit network e.g. acting as a backbone network for other service providers is different from a regional or national limited access network.

Afterwards a careful look to the demands of the end users is necessary. Considering the dimension of the network all possible data traffic relations has to be investigated, and the resulting amount of data traffic has to be assessed quantitative. Realtime applications will become important in the near future and will have a strong influence to the traffic assessments.

A further step in planning an IP-Network is the selection of a general Network Architecture. At this stage, it is not planned the detailed topology, but it is selected what technologies shall be used for Layer 1 and Layer 2, and what network structures are meaningful.

Today the IP-Traffic is meanly transported by ATM- or SDH-Networks. Furthermore, it is conceivable to put IP direct on optical networks with WDM or DWDM technology. Hybrid Architectures should also be considered.

If the overall network shall be structured hierarchical, the single hierarchical levels can be realized with different technologies. Besides all technological considerations, the overall network solution must be manageable. Therefore, a homogeneous approach might be the better solution.

The next step of the planning process is dealing with the optimization of the network topology and dimensioning of the network elements. Since the optimization and dimensioning is just done on IP-Level, a mapping of the IP-Network structure to the used Transport platform is required.

It might happen, that the topology of the Transport Network is different from the topology of the logical IP-Network, because an IP-Connection between two IP-Routers is not done in any case via a physical link (it is possible to establish virtual links on the lower Layers).

4.7 Topology design

The generic problem of designing the topology of a network implies the definition of how the users and applications are going to be interconnected whilst optimising the number and length of links required. To achieve this, a number of switching nodes have to be provided so that the solution will also include their optimal number and location.

Graph theory is used to mathematically represent the problem but only heuristic algorithms have been defined to solve this type of problems due to their mathematical complexity. Appendix B includes a detailed description of the mathematical principles involved in topology design.

Such a complex problem occurs only when a greenfield design is carried out. In most cases, the complexity is drastically simplified due to the fact that the new design is normally an evolution of the existing network and moreover, power utilities build their communication networks based upon the locations of their substations and buildings. Furthermore, the users are not distributed in a region but located in buildings and substations which could further simplify the network design since the topology will in most cases use the template of the power system grid as a reference.

The final topology of the network would have to take into account the requirements and constraints explained in the following chapters.

4.7.1 Topology constraints

The topology within the operational environment is mainly influenced by the strict requirements regarding timing and security existing for some applications (e.g. protection switching). While the total amount of data to be transported is relatively low, it is crucial to recognize events and to react in a timeframe of milliseconds. Within an IP-Network (Public or Private) a certain amount of Network Elements (e.g. IP-Routers) has to be passed. Even IP-Networks with state-of-the-art IP-Routers using available methods to deliver Quality of Service (e.g. MPLS) are not able to satisfy these critical needs. Nevertheless, for a first step it is possible to use IP-Technology combined with point to point connections (owned by the power supplier or leased lines) to fulfill all requirements. This will allow a smooth transition as soon as the appropriate requirements are available within IP-Networks.

On the other hand there are several less critical applications in the power suppliers operational environment. For this type of applications it would be possible to use a connection via an IP-Network to transport the data.

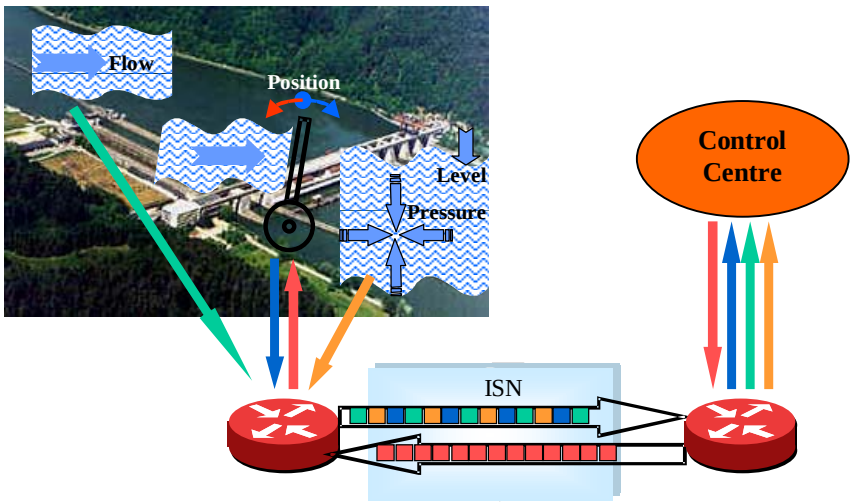


Figure 4.3 Example of data integration

IP technology is able to guarantee security regarding privacy and security of the data transmission (but not yet regarding the timing).

For these types of applications it would even be possible to collect several data and transport them via one logical connection over the IP-Network.

Nowadays the overall network topology of the Operational Network of a Power/Energy Supplier could consist of one (or more) Network Management/Control Center(s) connected to power stations, power transmission and power distribution utilities (via dedicated lines or via an ISN).

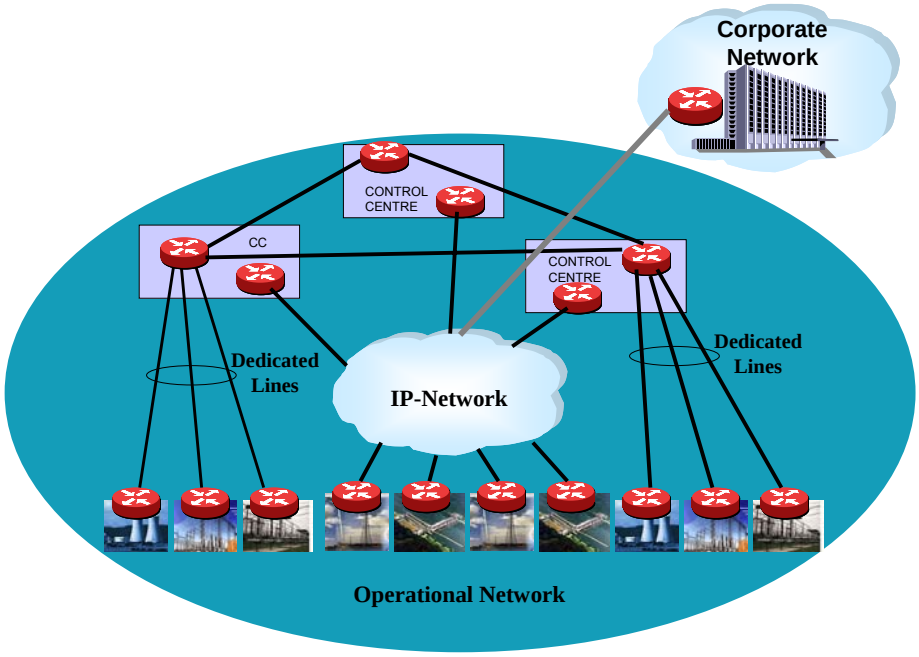


Figure 4.4 Example of Existing Topology

Additionally the operational network will also be connected to the corporate network to forward statistical- and billing-data to be processed.

With the future evolution of the IP-Network technology the operational network of an Energy/Power Supplier could as in the following figure:

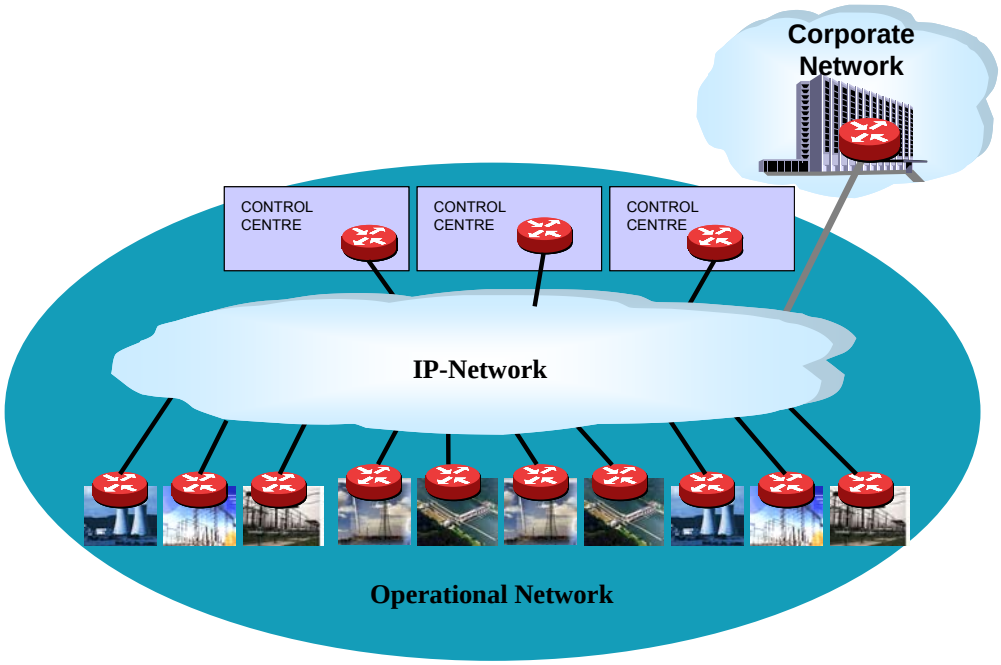


Figure 4.5 Future Operational Network

The topology within the corporate environment is by the size and the number of the locations. The network is normally arranged in a hierarchy based on the existing buildings (see figure below).

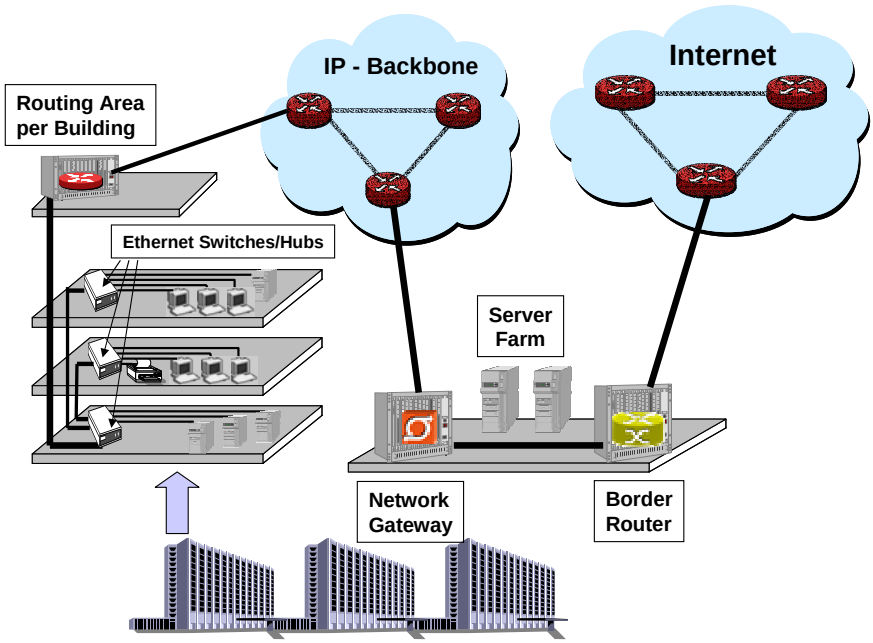


Figure 4.6 Typical Network Hierarchy

The lowest level is the data traffic of one floor within a building. Ethernet Hubs or Switches consolidate this traffic. Several floors are then further consolidated in so called "Routing

Areas". These Routing Areas can be connected via a "IP-Backbone". The "Public Area" of the Network (including all Servers that can be accessed from outside) is also part of this network.

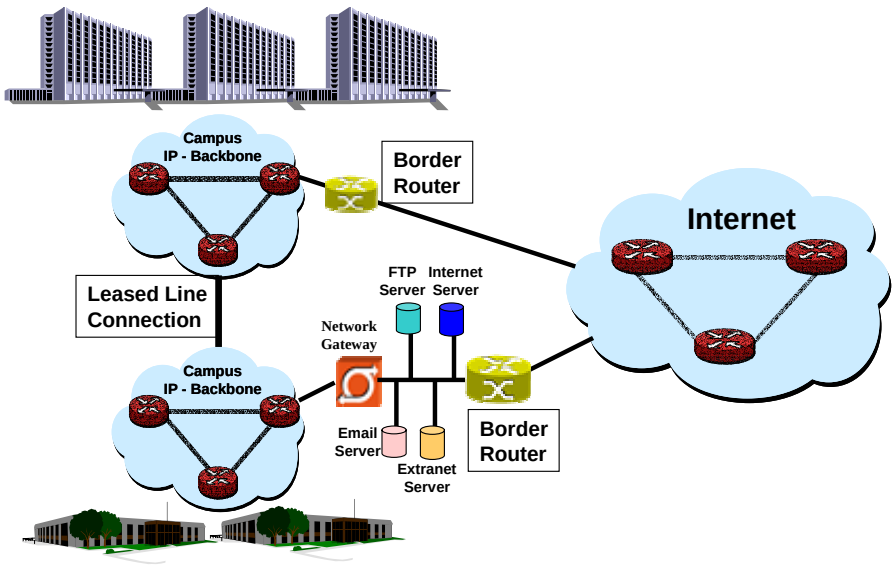


Figure 4.7 Distributed Corporate Network

In case of a geographically distributed corporate network the different backbones might be interconnected via leased lines (or Energy/Power Supplier owned Lines). Normally the "Public Area" of the corporate network is part of a single location (see previous figure).

4.7.2 Cost/performance optimisation at the topology level

Looking at internal cost factors, a corporate network over a medium or long term the major factor is the operational cost. The investment for new equipment is just a single event, while the costs to maintain and to manage the network are visible over a longer period of time.

In general the networks of companies are already overcomplicated. Looking to the pure physics copper wires of different types are coexisting with fiber-optic cable. Different transport techniques (e.g. WDM and DWDM for fiber optics) and different transport protocols (e.g. FR, ATM, DTM) can also be use in the environment of a corporate network.

With the upcoming new access options (DSL, cable modems, fixed wireless and third-generation wireless, etc) the level of complexity will increase further. While the number of mobile workers and tele-commuters continue to increase, these users also expect to access the network from an increasing array of nontraditional devices (e.g. Web phones). The only optimum way to manage this increasing complexity is to avail of the benefits that IP offers.

In this context the term convergence is very important. With IP it is possible to provide convergence on different levels:

- **Physical level:** The payload passes the same physical network equipment regardless of their service requirements. Different types of traffic (e.g. Control traffic, Internet traffic) can use the facilities of one network, regardless the requirement for bandwidth, delay, and jitter. The IP-Packages are classified by mechanisms within the network. There are a number of mechanisms for Quality of Service (QoS) and Class of Service (CoS) still available (e.g. policing or priority queuing) available within the network to differentiate the service requirements of the different types of traffic from each another to deliver the necessary service.

- **Protocol level:** The movement to a single protocol (IP) network will simplify maintenance and management. The common approach for legacy networks is to handle several protocols, but just one type of data (so called "best effort"). Converged networks support one protocol (IP), but provide the services necessary for multiple types of data (such as real time services).

- **Device level:** The use of relatively equal devices (e.g. routers) will bring significant cost saving regarding overall management of the network, and also regarding the service for the network devices. It will also simplify the handling of spares.

- **Application level:** Formerly separated application (e.g. carrying multimedia content such as audio, video, high-resolution graphics, virtual reality graphics, and interactive voice) can now be handled by a single network platform.

- **Payload level:** The different data types are carried in the same communications format, regardless the type of data traffic (stream, bursty). However, that payload convergence does not prohibit the network from handling packets differently, according to their service requirements.

- **Technology level:** A common technology level signifies the move toward common networking technologies that satisfy both LAN and WAN requirements.

- **Organization level:** The centralization of networking, telecommunications, and computing services, providing the necessary framework for integrating voice, video, and data on a single network platform.

In terms of external cost factors, IP is rapidly becoming the standard platform on which most networks, applications, and services are delivered. Therefore, most of the communication between companies, but also between companies and their suppliers and customers will be based on IP-based applications:

- **The Internet**: The idea of the Internet is to be a unique medium for exchange of information. Therefore, the representation of a company on the Internet is like traditional geographical medium, a "place" to do business. Advertising on the Internet mean reaching a global market. The Internet is connecting advertisers and marketers to customers from all continents with text, interactive graphics, video and audio.

- **E-mail:** While the Internet allows a worldwide representation of companies, the email service is able to personalize an organization. Companies can target at customers based on their previous purchases by email.

- **File-Transfer:** Is a simple tool that provides many functions, such as downloading of software, uploading web pages, or transferring of information. Because of its easy use and its functionality it is an ideal completion of the Internet and email application.

The above IP-based applications are also an essential part of the internal communication within a company. In many companies the Intranet is nowadays a necessary medium to widespread the available knowledge. The same is valid for email and file-transfer.

4.7.3 Reliability considerations

Definition of Reliability
Reliable delivery has been succinctly defined as "Data is accepted at one end of a link in the same order as was transmitted at the other end, without loss and without duplicates." This implies four constraints:

- No loss (at least one copy of each frame is sent)
- No duplication (no more than one copy is sent)
- FIFO delivery (the frames are forwarded in the original order)

- A frame must be delivered within a reasonable period

For a communications protocol to support reliability, requires that the protocol identifies each individual PDUs that is transmitted. The protocol implements an error recovery procedure e.g. polling (checkpointing in HDLC), or Go-Back (REJ in HDLC), and provides error-free procedures for link management.

The requirement for the network strongly depends on the applications that should be supported. Therefore in some cases a network with reliable links might be sufficient (Note: this may lead to loss of packets).

Within the environment of a power supplier environment the necessity of reliability is given.
The total reliability is mainly influenced by the under-lying network infrastructure. SONET/SDH-Networks or Ethernet LANs for example are highly reliable (this aspect is covered later on in the document).

Reliability within layered protocol environment
Looking to the OSI reference model (see figure 4.8) it is quite obvious that the reliability of a layered protocol environment is determined not just by a single layer. Reliability may be provided at various levels of the OSI reference model.

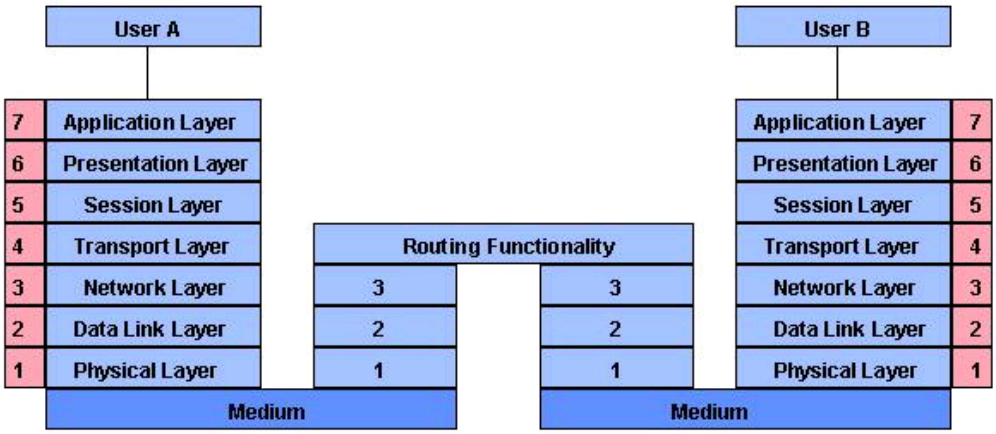


Figure 4.8 OSI reference model

Layered protocols usually also employ timers at each level, to fulfill the fourth constrain (reasonable period). The service provided by a protocol layer may be unreliable for various reasons including:

- Corruption of bits within the physical medium or the interface to the physical media
- Faulty bit-timing resulting in erroneous decoding of the value of a received bit
- Software error within the software used to implement the communications protocol
- Insufficient buffer space within the communications equipment

Examples of reliable communications protocols are:

- Data Link Layer - HDLC (ABM)
- Transport Layer – TCP

The Internet Protocol (IP) itself provides a network layer service for connecting “computers”. Each computer is identified by one or more IP-Address. The network layer PDUs are known as either "Packets" or "Datagrams”.

The IP network service transmits Datagrams between intermediate nodes using IP-Routers.
The reliability of these IP-Routers is also a main factor influencing the total reliability of an IP-Network (Reliability of IP-Routers is covered later on in the document).

The most complex part of an IP-Router is concerned with determining the optimum link to use to reach each destination in a network. This process is known as "Routing". Although this process is computationally intensive, it is only performed at periodic intervals. An IP-Network normally uses a dynamic routing protocol to find alternate Routes whenever a link becomes unavailable. This provides considerable robustness from the failure of either links or IP-Routers, but does not guarantee reliable delivery. For some applications this basic service is sufficient. They are using a simple transport protocol known as the Universal Datagram Protocol (UDP) to access this Service.

Most Users (Applications) need additional functions such as end-to-end error and sequence control to give a reliable service. This reliability is provided by the Transmission Control Protocol (TCP) which is used end-to-end across the IP-Network.

Examining Reliability of IP-Networks

The primary original design objective of the Internet was "survivability in the face of failure." The precursor to the Internet –ARPANET - was conceived by the Department of Defense as a distributed Data Communications Network designed to withstand any kind of attack.

As a result, the IP-Networks of the past provide very high packet delivery rates – even in the case of multiple router or link outages. The consequence of the focus on survivability is significant variance in the latency of packets delivered. This design proved ideal for the Internet's initial applications – e-mail, data and web browsing, but inappropriate for delivering latency-critical services such as voice or video.

Today, applications such as voice, video and secure VPNs are placing new higher demands on IP-networks. In order to support these services, IP-network equipment must not only support high packet delivery, but deliver packets within stringent latency parameters (generally <50ms). This additional requirement reduces the tolerance for IP-Router failures and can result in re-routing and excessive latency. The consequence of this evolution is to maintain IP-Networks to the higher quality standards required by real-time services.

Under-Lying Network Infrastructure (e.g. SONET/SDH)

For today's Backbone Networks Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) Transmission Technologies is widely used. The SONET/SDH specification outlines the frame format, multiplexing method, and Synchronization Method between the equipment, as well as the specifying optical interface. SONET/SDH will continue to play a key role in the next generation of networks. The core of IP-networks is often built on under-lying SONET/SDH Networks.

Reliability of SONET/SDH-Networks

SONET/SDH networks have a ring structure, which adds high reliability to the overall transmission network. Even if the optical fiber is cut, the transmission path is backed-up and restored within 50 ms.

Reliability of IP-Routers

The reliability of IP-Routers is considerably influenced by the availability of the system. Although some IP-Router-Vendors making considerable progress regarding the availability issue, the five 9s goal (99,999 % availability) is not yet reached. A new class of fault tolerant IP-Routers is needed to provide protection at the service layer and support redundancy of routing states and tables. This capability is essential to building equipment capable of restoring services to SONET APS-like speed in less than 50 ms.

The realization that Upper-Layer Protocol behavior dominates restoration time in IP- Routers has lead to a new generation of Carrier-Class IP-Routers that provide full redundancy. The task of Routing (computing of Routing Tables) is completely separated from the task of Packet forwarding. This type of IP-routers feature hot standby routing processors, mirrored routing session and information states, redundant interface-cards (including forwarding tables).

If the active routing processor or one of the active interface cards is interrupted, the standby system steps in and immediately resumes normal operation without any noticeable impact to routing traffic. All the active routing sessions are maintained.

Without any noticeable downtime, adjacent IP-routers do not need to be notified as the hitless IP-router recovers instantly. This is important because when a router becomes unavailable or its TCP status becomes unsynchronized, in which case it can lose its BGP routing sessions. The disappearance or loss of synchronization of the failed IP-Router will likely have a negative impact on stability and performance, as adjacent routers become aware of the problem.

Reliability improvement by Traffic Engineering (e.g. MPLS)

Multi-Protocol Label Switching (MPLS) brings strong traffic-engineering capabilities to IP-Networks by providing explicit routing capabilities. Internal Gateway Routing Protocol (IGP) protocols do not take account of available bandwidth and link-state information when calculating routes. This could result in congestion on some paths in the network and in under-utilisation of other paths. In "Wide Area" IP-Networks, MPLS is used to conserve bandwidth by directing traffic in an optimal manner. For "Local Area" IP-Networks traffic engineering, however, is a powerful tool to enable a responsive network to meet service-level agreements. To minimise congestion in IP-networks, MPLS supports traffic-engineering extensions to the IGP protocols OSPF-TE and IS-IS-TE. These extensions provide additional link-state information such as reserved bandwidth, available bandwidth and affinity, along with route updates.

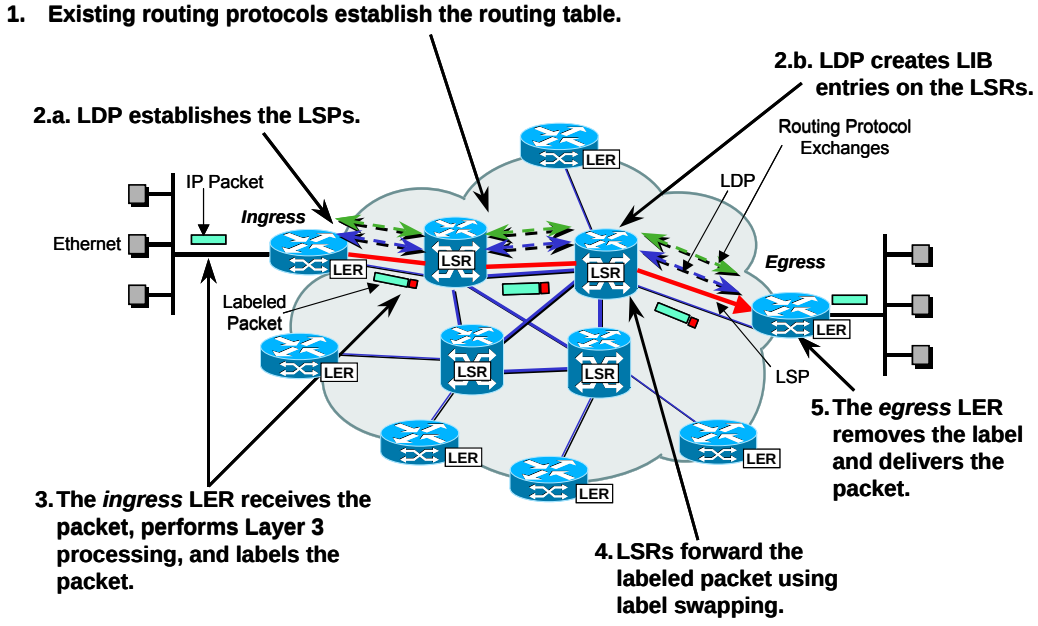


Figure 4.9 MPLS working principles

With an MPLS solutions, backup Label Switch Path's (LSPs) can be configured for fast fail-over, thus improving overall service reliability for the customer (see figure 4.9). Backup LSPs can be defined as hot-standby LSPs that have been pre-established, or can be dynamically created upon failure of the primary LSP. Another alternative is to enable the fast-reroute option when an LSP is established. This leads to the creation of 'detour LSPs' around each point of failure in the path. If a node or link fails, a local detour around the failure will be used and the ingress IP-Router (Label Edge Router, LER) will be notified. The ingress router can then decide to set up a new LSP.

When the primary LSP is restored, a user-defined option allows traffic to be switched back to the primary.

4.8 Service integration policy

The service integration policy has a considerable influence in the architecture of the network and thus on the performance and the cost of the final design.

Service integration policy is influenced by many factors related with the design policy and the service delivery policy. Reason for service integration as well as risk and problems arising from this integration could be identified. It is the task of the network designer to evaluate them in function of the policy of the company and make the decision of the service integration architecture that better suits the network design goals.

The key reasons for service integration are:

- Capability of the service layer technology to offer different services.
- Saving due to the use of spare resources at the service layer.
- Simplification of the internetworking model due to the reduction of the number of service layers.

The main risks/problems of service integration are:

- Service interaction.
- Security risks.
- Resources stealing between services due to a lack of service isolation.
- Higher service layer management complexity.

The impact of the advantages and disadvantages of service integration depends at a great extend on the integration model adopted. At the same time, every model reflects a different service integration policy.

The main service integration models that can be identified are:

- Loose service integration model. Different services are integrated over the transport layer. Characteristics:
  - High degree of service isolation.
  - Security guarantees.
  - Network resource allocation guarantees.

- Weak service integration model. Different service layers are integrated over the transport layer. Characteristics:
  - Higher degree of complexity than previous model.
  - More flexibility in the service layer design.

- Tight service integration model. Different services are integrated at the service layer. Characteristics:
  - Economy.
  - Less architectural complexity.
  - Service isolation mechanisms required.
  - Resource optimisation which could drive to lower costs

Details of the working principles of every model are developed in chapter 4.14.2.

4.9 Architectural design

The architecture of a network has not a regular structure. In order to achieve cost saving implementation the network is divided into to main parts: the access and the core or backbone.

The function of the access network is to provide connectivity to the users gather the traffic and deliver it to the backbone which function is to provide broadband transport and connectivity of all the access point. More details about the technologies used in access and backbones and the typical structure can be found in TB-153 [1].

In the case of power utilities, the design of the access networks use to be an easy task since users are located in substation or main company buildings. In this case, LAN technology is the approach that better suits the access requirements.

The design of backbones can be afforded using different alternatives and combination of technologies. The different architectures that can be used in the design and implementation of backbones for power utilities are discussed and analysed in TB-153 [1]. The design of the topology and dimensioning of the links are discussed in the corresponding chapters.

4.10 Networking technology selection

The selection of networking technology depends on a number of factors. Only in the rare case that the entire network can be built from scratch one would have full freedom in selecting the technology that would best meets the requirements regarding:

- Cost effectiveness
- Performance
- Scalability and flexibility
- Reliability and resiliency
- Simplicity
- Manageability
- Homogeneity

In practice it is hardly ever possible to design the entire network from scratch for historic and economic reasons. Networks consisting of one homogenous technology from access to the core are therefore normally neither realistic nor practical. Different technologies have normally to co-exist and to collaborate in order to satisfy traffic and connectivity requirements most efficiently.

4.10.1 Networking technologies

Networking technologies may be broadly categorised according to the switching technology that is used for routing the traffic from source to destination:

- Circuit switched
- Packet switched

Networks may also be categorised according to the underlying protocol. The most commonly used are:

- SDH
- ATM
- X.25
- Frame Relay
- IP

Each one of these technologies can be found throughout the network hierarchy, i.e. from access to the core, or from the service to the transport layers.

Circuit switched networks

In circuit switched network the path through the network from source to destination has to be established before any communication can take place. Once the path has been set up, communication can start and network resources (the "circuit") are dedicated exclusively to the

service that requested it, until the connection is released. If the network cannot provide the required resources, the connection is refused. An example for a circuit switched network is the PSTN (Public Switched Telephone Network).

In particular, circuits may be connected on a permanent basis rather than on a temporary basis, depending on the traffic requirements.

Packet switched networks

In packet switched networks, the data to be transmitted are split into packets, each packet carrying a source and destination address. The destination addresses are read by the packet switches or routers in the nodes of the network, and routed through the network to the destination according to the particular routing or switching algorithms used. Individual packets may even follow different paths through the network, before they are re-assembled in the original order at the destination. Hence no fixed path is established prior to traffic flow, and unless special protocols are used, the network forwards the packets according to the "best effort" principle.

Examples for packet switched networks are IP and X.25 networks.

SDH Networks

SDH (Synchronous Digital Hierarchy) networks are mainly used at the transport layer for carrying huge amounts of traffic over geographically widely spread areas (wide-area network, WAN). The transmission medium is normally optical fibres or microwave radio. Data are multiplexed into higher order aggregates by fixed TDM (Time-Division Multiplexing) in SDH multiplexers according to standards defined by the ITU-T. Data is routed through the network by DXC units (Digital Cross-Connects) which drop, insert or through-connect the data on a time-slot basis. The settings of the DXC are controlled by a network management system.

SDH networks are therefore of the circuit-switched type, allocating fixed network resources to the services with QoS (Quality of Service) guarantees.

SDH networks are typically configured as rings. Resiliency is achieved by reversing the traffic in the opposite direction in case of a failure, e.g. due to a fibre breaks.

On optical level, the capacity of SDH networks can be further enhanced by means of DWDM (Dense Wavelength Division Multiplexing), where individual SDH aggregates are multiplexed onto the same optical fibre by using different wavelengths for each aggregate.

ATM Networks

ATM (Asynchronous Transfer Mode) is based on cell switching. Data are split into cells of fixed length (53 bytes) that are routed through the network by the ATM switches in the nodes of the network. Thanks to the fixed cell length, the switching fabric is realised in hardware, which ensures very fast switching and low latency. ATM is a packed-switched technology that can also emulate circuit-switched circuits and LANs. It is a very powerful technology as it can carry all kind of services with true QoS (Quality of Service) guarantees, e.g. in regard of data throughput and latency.

ATM is mainly used in transport networks and at the network edge. Due to cost and complexity compared to IP, "ATM to the desktop" has not materialised.

X.25

X.25 is one of the earlier protocols for packet switching. It has been designed for copper networks that are prone to producing bit errors during transmission. X.25 therefore includes error-handling procedures on a hop-per-hop basis, hence involving quite some overhead at the expense of efficiency. Packets are routed from source to destination by X.25 switches in the nodes of the network.

Frame relay

Simply speaking, the original idea behind Frame Relay (FR) was a simplified X.21 with less overhead and better efficiency, taking advantage of digital networks that normally produce

very little errors during transmission. Hence error handling was relegated to an end-to-end basis rather than on hop-per-hop basis. In recent years, FR developed into a rather universal networking technology, which, depending on the implementation, can also carry voice with a certain QoS (Quality of Service).
The fast deployment of FR, in particular in the US, has in a certain way adversely affected the introduction of ATM.

IP
IP stands for a synonym for networks based on the suite of Internet Protocols. Originally intended for reliable and resilient communication between computers in a network, IP has developed into the dominant networking protocol not only for LANs (Local Area Networks) in conjunction with Ethernet, but also penetrating the WAN domain by gradually overcoming its original weakness of a "best effort" technology.

IP is a packet switching technology. Data are packetized into packets of variable length, and routed through the network by IP routers or IP switches.

Well known IP protocols are TCP/IP, UDP, FTP, SMTP and VoIP for Voice.

In the industry sector, there is a clear trend to standardise on IP and Ethernet for local area networks, e.g. in power stations and substations of electric utilities, are gradually replacing the many different legacy - and in case proprietary - bus systems.

4.10.2 New networking technologies

Two emerging networking technologies shall be mentioned here: DTM and RPR.

DTM – Dynamic Synchronous Transfer Mode
DTM combines some of the advantages of ATM, IP and SDH at a lower equipment and network management complexity.

Time slots can be freely and dynamically allocated to services as follows:

- Constant delay and bandwidth are guaranteed
- Possibility for minimum bandwidth guarantee: A minimum number of time slots are dedicated to the service, but more information can be transmitted if more time slots become available (dynamic allocation of time slots)
- Best effort: The channel is established when data has to be transmitted, depending on available time slots. No minimum bandwidth is guaranteed.

DTM permits a simple and fast distribution of bandwidth. So far it has mainly established itself in video distribution applications, where QoS (bandwidth, latency, data throughput) is a prerequisite. DTM belongs to the category of circuit switched technology.

RPR – Resilient Package Ring
RPR is positioned as a networking technology for MANs (Metropolitan area networks) where today multiple low performance platforms (PDH, Fractional E1, ISDN) frequently dominate.
RPR can be looked at as a distributed Ethernet/IP switch supporting dual ring topologies (similar to SDH), with the following claims:

- Bandwidth multiplication or spatial reuse: Add/drop traffic on the fibre ring only between a sender and receiver while simultaneously allowing the rest of the ring to carry traffic from other sender/receiver pairs.
- Dynamic bandwidth allocation: Control the amount of traffic by each network element and provide fairness in accessing the ring under congestion scenarios.
- Resiliency or ring protection: Ability to recover from ring or node failures within 50ms. Similar to SDH.
- Dual ring operation: Both ring directions carry traffic thereby doubling traffic carrying capacity. Reverse direction is not reserved for backup in case of ring failure

RPR belongs to the category of packet switched networking technologies and is about to be standardised by the IEEE.

4.11 Internetworking architecture

Internetworking is a concept introduced at the late 90's and refers to the use of different technologies in different parts of the network in order to obtain a more efficient network design. The TB-153 introduces the details of this approach as well as the different models and their typical applications.

The latest development in this field is the Multiprotocol Label Switching (MPLS) approach. This architecture follows the integrated model and provides a core set of mechanisms to switch data flows throughout a broadband core. MPLS is the most successful internetworking architecture. The rest of the chapter is focus in this approach. More information related with other internetworking models can be found in the TB-153.

4.11.1 Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) is seen as a new core technology for next-generation networks. MPLS is a new protocol defined by IETF (Internet Engineering Task Force), that simplifies IP addressing. The "MP" means that it supports multitude of other protocols, or in other word is encapsulation protocol. Its techniques are applicable to any network layer protocol. "LS" stands for label swapping at each hop while the packet is forwarded through the network.

A router, which supports MPLS, is known as a "Label Switching Router" or LSR. Label Switching Router must be able to take label-encapsulated packet on any of its interface, and after looking up in the switching table, it has to insert a new label and send the packet out to the appropriate interface.

A label is a short identifier of local significance, and represents a FEC to which packet is assigned. Forwarding equivalence class (FEC) is a group of IP packets, which are forwarded in the same manner, actually over the same path, with the same forwarding treatment. In MPLS, the packet is assigned to a particular FEC just once when the packet enters the MPLS network, which is a set of nodes that operate MPLS routing and forwarding.

Using conventional IP routing protocols and LDP (Label Distribution Protocol), Label Switching Routers build up routing tables supplemented by labels. So the first router in the MPLS network, so called edge LSR assigns the initial label to the packet after performing the longest-match lookup on the IP header. Once the packet is labelled, it is forwarded through the network using only the label. The forwarding mechanism is based on label swapping, and is independent of the encapsulated IP header fields, such as IP destination address. Once a sequence of labels and links called a Label Switched Path (LSP) has been established, LSRs can switch traffic quickly and the labels drive all forwarding.

Decision to assign a particular label to a particular FEC is made by the LSR that is downstream. The downstream LSR then informs the upstream LSR of the label-FEC binding it has made. A set of procedures by which one LSR informs another of the label-FEC bindings is called LDP (Label Distribution Protocol). A number of different label distribution protocols are being standardised, existing protocols have been extended (MPLS-BGP, MPLS-RSVP-TUNNELS), and some new protocols have also been defined (MPLS-LDP, MPLS-CR-LDP).

MPLS technology provides a number of new capabilities and benefits in an IP network such as: support of scalable VPN, traffic engineering and support of IP routing on ATM switches.

Virtual Private Networks

One of the most important applications of MPLS is the support of the VPNs (Virtual Private Networks), so that for VPN customers, provider's network appears to be their own private IP backbone.

VPNs must be scalable and cost-effective. These networks must support customer requirements such as quality of service (QoS). MPLS-based VPNs provide any-to-any connectivity and scalability of the IP backbone, but still providing QoS and the privacy. Greater efficiency is provided because the decisions are made at the network edge.

VPN customers do not have to establish point-to-point circuits between their offices; they only need to provide connection from their office router to a service provider edge router. This edge LSR labels the packets and forwards it through the MPLS network to the other edge LSR closest to the packet's destination. So customer router peers with edge LSR and exchange routing information using RIP or BGP, and then the label is assigned, based on the incoming interface that determines VPN membership and the destination. Customers can choose their own addressing plan which may overlap with those of other customer, because of the fact that on the MPLS provider's backbone label are used for packet forwarding and not IP addresses.

MPLS VPNs are specific because they can be built over multiple network architecture such as: IP, ATM and Frame Relay.

Traffic engineering

One of the biggest problems on the Internet is controlling the traffic so that resources are used efficiently. Standard IP-routing protocols provide little information about available bandwidth.

MPLS can provide traffic engineering functions, which can be used to map traffic flows onto the network in such a way that it gets QoS it needs, but also to reduce congestion in the network and use the most of the available facilities. Traffic engineering is the ability to control routes more flexibly then it is in least cost hop-by-hop routing. This feature will allow a network provider to control and monitor bandwidth and paths, enabling capacity planning, routing control, traffic management and path management. For traffic engineering purposes explicitly specified label-switched paths can be set up through the network.

This means that, for example, if there are two paths from one router to another, all the traffic will be sent over the shortest path. This may cause congestion, while another path can be underloaded. In MPLS network, traffic flow can be managed by defining policies that select packets to follow particular paths.

IP routing on ATM switches

MPLS enables support of IP routing on ATM switches, or let's say they can perform virtually IP routing. This ATM label switch should have control software to establish virtual channel identifiers table entries, for witch it uses IP routing protocols and LDP. ATM label switch supports IP addressing, rather then using address resolution protocol for ATM to map IP addresses to ATM addresses. ATM label switch should also operate as ATM switch, while its resources are partitioned between the ATM and MPLS control plane [8].

MPLS is an emerging technology that will enable IP network to become more reliable and thus ready to support the next generation service. MPLS technology offers scalable VPNs with QoS, enables traffic engineering features on IP networks and is a way of integrating ATM and IP technology. It is seen as a key technology for future internetworking.

4.12 Management architecture

The definition of the management architecture covers three different aspects:

- The implementation of the Network Management Centres
- The implementation of the Management Systems
- The implementation of the Management Network

The following sections develop these aspects.

4.12.1 Network Management Centres

In the case of wide network, a hierarchy structure of networks is usual. This structure can be created following the geographical distribution or/and the kind of technology of the networks. Due to safety reasons, all the functions of one network management centre should be able to be taken by another network management centre or by the main network management centre.

In the case of smaller networks, the use of a unique management centre can be valid. However, in this case if there are different maintenance zones is wise to have minimum equipment in these zones that let do the more critical functions in the case of catastrophe.

As management is used to be critical, a redundancy in the equipment is needed. Sometimes, equipment with redundancy in their component is valid. In the most critical cases, a geographical redundancy is necessary. This solution is very expensive and if the amount of data is very large, a broadband connection is needed. It is very important to have spare pieces or to write a support contract that implies a minimum time for response for the critical elements. The room of the equipment must be clean, tidy and have air conditioning. Temperature is a fact that has a great influence in the life and in the Mean Time Between Failures (MTBF) of the equipment. A network management centre should have due to its importance a protection system against fire and security measures.

The organisation is another important aspect of a network management centre. The number of people, their functions and their timetable depends on the amount of services they give to the customers, the importance of the services, and the money a company can spend in it. Management Centres can be considered to be composed of a network management centre and an application management centre. In most cases, they are divided in two different management centres. In the following example, it is considered as one and it is divided into the following parts:

- *Customer Care:* The focus is on attending to the customers rather than solving technical problems. In most organisations this function is provided through a Call Centre.

- *Network Operators:* Their function is supervising the network and resolving the technical problems and performance issues that may arise. Many times, depending of the training of these people, and the number of technologies they need to understand, they can be grouped in different specialist sections. For example: PABX, transmission, data switching, applications, etc.

- *Network Specialists:* They have to solve the problems that the operators have not been able to solve. They are one or two people for speciality. They are the bosses of the operators, and they have a great knowledge in their speciality.

- *IT Systems Operators:* Because there are a lot of computers, a group or a person specialised in the administration of servers, data bases, security, etc may be required.

- *Control Centre Manager:* This may be one person or a group of people if the centre is very large.

Depending of the structure of the enterprise, people responsible for the network planning may be part of the management centre.

4.12.2 Management System

In a Management Centre, they are a lot of technologies and different types of machines, each one with their operating system. It is necessary to have people specialised in each equipment and technology.

A lot of information is received in the centre, and the operator has to understand it. Many times, one failure in an element can generate a large number of alarms. For example, a break

in a fibre link can generate alarms, for example, in the SDH equipment, in many frame relay virtual circuits, and in a router, and perhaps even in the applications of the office.

The integration of services over an ISN will alleviate these problems and reduce the network management overhead.

The management architecture needs to be analysed in relation to the five functional groups, as defined by the Telecommunications Management Network (TMN) architecture:

Fault:

This function can be divided as follows:

- Detection of alarms
- Correlation of alarms
- Corrective actions

The integration has achieved almost only in the first part, thanks to the use of SNMP. Nowadays, much equipment is able to talk this protocol. For the equipment that does not talk SNMP, proxy equipment that asks this equipment can be used. Other solution for this equipment is the development of software that translates the proprietary protocol of the alarms of these equipment into SNMP.

There are a number of software platforms based in SNMP that manage the different elements of a network.

Correlation of alarms refers to the capacity of a system of distinguish among a flood of alarms, which is the original problem. Up to now, the correlation of alarms has only achieved with the alarms from the same system.

Some software for correlation of different system exists, but the problem is the definition of the rules that define every case, and that when a version of a program is changed, it is necessary to redo the work. In addition, new rules have to be introduced for every type of equipment. The most common action is to use the proprietary management software of the different elements or networks.

It is also possible to develop a single software platform for the different protocols of the different manufacturers, but modification will be required every time new elements or software versions are introduced.

Software products are available that work in the service level and collect all the information of all the proprietary software and manage all the alarms information, creating reports and letting the user to create customised correlation and display rules.

Configuration:

This is one of the more difficult aspects to achieve integration and generally the only way is to use proprietary software.

This is because firstly the need to obtain the structure of data of the different machines that need to be supervised and this is unlikely to be forthcoming from the vendor. And secondly, every new release will require modifications of the configuration software in order to incorporate the new features.

It is worth noting that the object oriented programming language called CORBA is beginning to be used for creating interfaces that let interchange information among different management tools.

Accounting and billing:

If the company is considering billing for services to internal groups and/or to external companies, it has to acquire an accounting and a billing tool.

Many companies that bill internally generally use a flat rate. In this case, it is not necessary to have an accounting system and the billing tool is very easy to develop.

Performance:
There are two ways to measure the network and service performance, either by the use of proprietary software or using a system based on deploying probes throughout the network. These probes take the information from the network and transfer it to a centralised processing unit. One issue is that these tools are normally used only in the data network equipment, and not in the transmission systems, such as SDH. A very common tool to carry out the measurement for machines are RMON tools.

Security:
This aspect will be treated in the part of this document dedicated to Security.

4.12.3 Management Data Network

This can be provided by creating a different data network for the management system or by overlaying on the network being managed. In the second case, the management circuit must have privileges over the data traffic.

The more common approach is a combination of both. All the management data has a higher priority (note: statistical data does not require this) and in the zones of the network that are not adequately meshed, alternative paths to the edge have to be implemented (very often by modem).

If buses are being used, it is advisable to ensure that access to the management buses can be provided at both ends.

4.13 Security architecture

In this Technical Brochure, aspects such as fire safety and physical access restrictions to the network management centre are not going to be addressed.

The first step is to define a security policy based on the requirement analysis (see Chapter 3).

4.13.1 Security Policy

Security policy must be defined using a top-down approach, starting with the corporate security policy through to the security policy of each department and application. The security policy must be written using rules so that it will be easier to implement. For instance, the first rule at a high level may be: "If it's not allowed, it's forbidden".

Subsequent rules need to define subjects such as which information are confidential, the access and use of resources such as the Internet, e-mail, corporate and operational applications.

Other rules imply a good knowledge of the functions of each department of the company and their inter-relationships. The permissions for access to different information and applications must be decided for each users or group of users. The procedures for permission and the people responsible for granting it need to be specified.

The security rules will be changed many times over the life of a system. In fact, many aspects that may not have been considered will arise in the implementation stages, and the policy will have to be modified.

To implement the policy, the following need to be addressed:

- Network security
- Equipment security

- Data security
- Backups

Network Security

Firstly the protection of a network from external attacks has to be implemented by the implementation of a protection device, generally called a 'firewall'. This firewall is the border between outside world and the private network.

However, many times the enterprise possesses information that it is not critical and required to be accessible by external users. A web site with information of the company can be an example. For these cases, some companies create a DMZ (DeMilitarizated Zone). This is a part of the network of the company that it is not protected by a firewall. The only protection of these machines is the virus detection software specific to these devices. All the data on these machines should be read-only data and users should never be able to modify internal information.

There are four types of firewalls:

Router firewall: A router can act as a firewall. This way it is possible that a router looks into each packet and depending on the address of the origin and of the destination and sometimes, of the ports, it can filter the packet. This implies a bigger load for the router. This is not a major problem for routers nowadays because their processing capacities are increasing day by day. The problem is that it is not a flexible way to develop and manage the security policy rules.

Proxy firewall: This kind of firewall filters the packets depending on the application and the user's privileges. Normally, it asks for an authentication of the user. Proxy firewalls have a big cache memory and are very common for example, Internet access.

Application Firewall: This application allows the administrators to define security rules in a flexible way. It can filter depending on the protocols and addresses. It creates logical groups of users and machines. The rules are analysed in a sequential manner and the analysis is completed when one rule permits or forbids access.

Access Firewall: These firewalls ask for a password to external users that connect to the network by modem. An example of a well-known access firewall is RADIUS.

All these types of firewalls can be employed in the same network at various stages. Because the majority of attacks are internal some applications are protected by internal firewalls.

The administrator of the network must translate the security policy in the network implementation. In addition, the security administrator must introduce the rules into the firewalls so that only the authorised group of people can access to their authorised resources.

A typical security topology of a network could be the following:

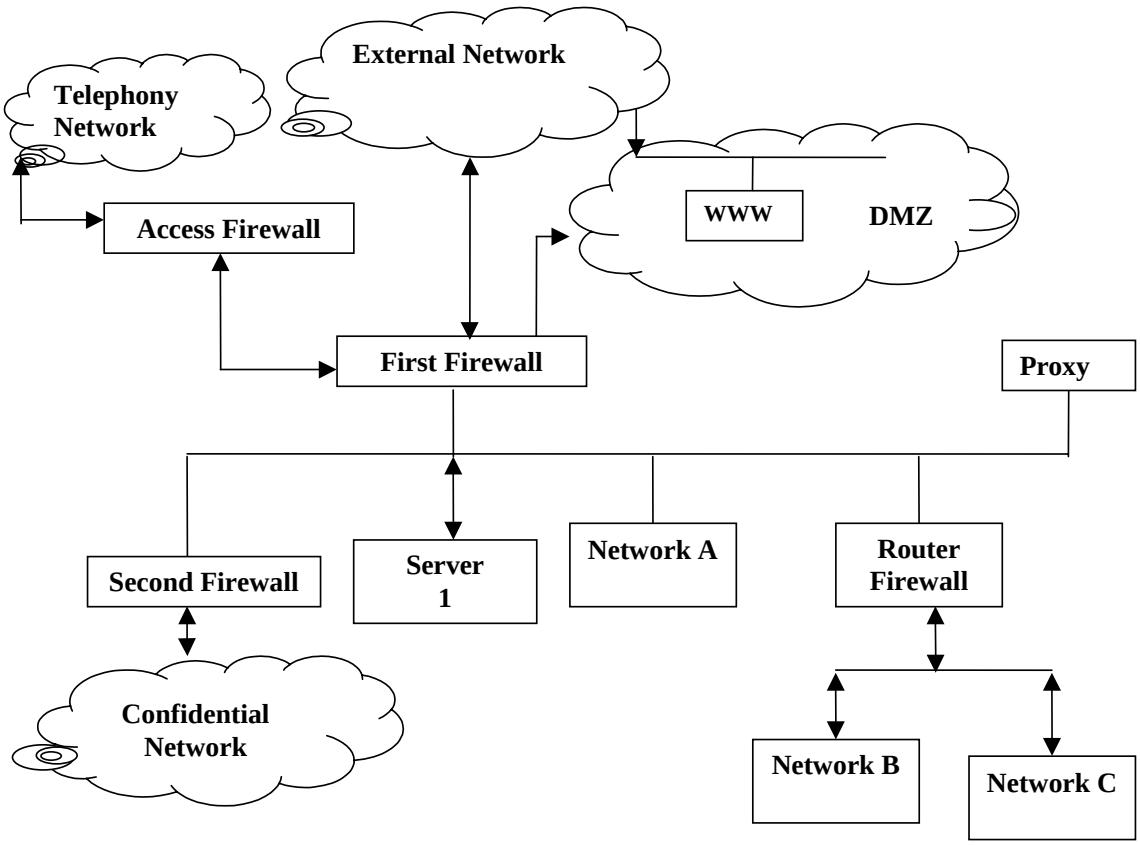


Figure 4.10 Security Topology

The external users access to the DMZ without limitations. If they want to enter in the internal network they have to authenticate themselves in the access firewall if they access by modem. If they are allowed users they are allowed to the first firewall. If they access through an external data network such as Internet they are connected to the first firewall directly. The first firewall can ask for an authentication and check the rules. If all is in order, the external user will be able to access to the requested application.

For Internet, it is very common to use a proxy firewall. That way, the first firewall, will be free of this duty. In this case, its function will be to direct the HTTP, Real Audio, etc, traffic to the proxy and from this one to Internet.

The proxy will check all the rules about Internet directions and their contents. In addition, the proxy is used to provide two other functions. One of them is being used as a Cache. That way, many times there is no need to access through Internet to the same information, some users have accessed a moment before. The other function is the translation of directions between internal address and legal addresses (Internet addresses). So, as well as not having to ask for many legal addresses, it increases the security because external users do not know the real direction of the machine they are talking. This function can be done by the first firewall too.

The second firewall and the router with packet filter activation are put to protect the resources from internal users or as a second protection if a hacker has taken the control of one internal machine. They may not be necessary. It is possible to redirect all the packets among all the internal sub-networks to the first firewall and made the firewall check the rules. However, if the network is not small, it is better use more than one firewall, than let divide the control.

As source addresses have a high importance in the filtering function of the firewall, it is very critical to remove all the packets that come from outside with an internal address. This

prevents identity spoofing. In order to prevent external users suffering the same problems, it be good practice to avoid the use of other addresses that there are not specific to the private network.

For the same reason, in order to avoid internal attacks, the routers should discard the packets received by their LAN connection whose addresses do not belong to their own network.

It is recommended to install the first firewall with a second device for redundancy.

Another method to implement security is using VPN's (Virtual Private Networks). For doing this, it is necessary to implement it in the routers of the network.

Equipment security:
This can be considered to consist of two aspects:

- The first one is the implementation of the security policy for controlling the access and privileges of a user to individual pieces of equipment. This access can be a local access or a remote access that satisfies the firewall rules or a remote access does not require passing through the firewall. For example, a firewall can authorised a telnet connection between two computers, however it is possible that a password has not been asked, or that password is a generic one of one department. However, the user has to demonstrate who they are in order that the computer allows only the actions they are authorised. This security can be based on a password-based system.

- The second aspect is the revision of all security flaws such as bugs in the operating system or applications, which can be used by malicious users to take control of the machine. This task requires daily verification of any new attacks than are notified and the application of the patches to fix them.

It is a mistake to consider the network is totally protected from external attacks because of the implementation of the network security through firewalls alone.

Firstly, a firewall is a machine with its own software; therefore, it is necessary to verify if there are any bugs on this machine.

Secondly, some services that are allowed by a firewall can have errors that let a hacker do illegal actions. For example, a firewall that authorises Internet connections to an internal server, which is something perfectly legal, but it is possible that a bug in the server of WEB pages let a remote user be considered as root user when they write a long field in a questionnaire. Or for example, an authorised user of FTP, due to a bug in this program, can change his user into root.

The third reason is that many times a network security policy has errors that are very difficult to discover because of increasing complexity.

The following are some basic rules for implementation:

- All the resources must be protected with passwords.
- Users without a password must not exist.
- The length of passwords must be at least of 8 characters (it is very easy to discover for example a password of 4 characters with a little program of trial and error).
- The passwords should never be words of a language, nouns of people, dates important for one person, the name of the machine, the name of the manufacturer, etc.
- All the default passwords must be changed.
- SNMP passwords for changing parameters must be different from public or the name of the manufacturer.
- It is recommendable to include some numbers or capital letters.

- The password of the users must be encrypted in the file where they are stored. In the Unix case, it is better that the encrypted password are not be in the /etc/passwd file).

For the passwords, there are other solutions, such as the use of identification cards or the use of system that generate one password for each access (for example in the S-Key system). These systems require additional hardware but they increase the security level.

Respecting the consistence of the system, it is very important to be informed about the new forms of attacks. For this duty, it is interested to be in some security forums of news, or e-mail list (one very good is the CERT´s one). Some direction when are possible to find security information are the following: http://www.cert.org, http://www.ciac.org/ciac/, http://www.first.org/team-info, http:// www.iss.net/.

These attacks can be of three types: Deny of Service (DOS), Access to the root, access to the information. In the first case, the purpose of the hacker is to put out of order a system or one of its services. In the second, to take the control of the machine, and in the third one, to change or read some information.

Besides of being informed of the attacks and their remedies, it is very important removing of the services in the machines that there are not necessary. This reduces the number of possible attacks.

In TCP/IP, besides the address of a machine, a port number is used in order to access a service. It is important to check all the active services in each machine. Those services that not required should be removed or changed for other more secure services.

To facility this duty, they are some programs that check the system and report the weak points they find. Many of them are used by hackers and are available through the Internet.

Data security

A lot has been done respecting the data security if the latter parts of security (network and equipment security) have been implemented. Because of these two actions, a hacker cannot access to any equipment to change or read the data. However, they can still read or change the data, because the data flows in our network (or in the external one).

First of all, this hacker can connect some equipment in our network, or if they are internal, they can put some program in their computer that analyses all the data that is in their network.

In order to restrict physical access, it is advised to use optical wire instead of copper and employ strict control of the addresses that connects to the network.

A solution for this problem is data encryption, VPN´s, IPsec, or the use of secure applications.

A common trend is to change the telnet application for a Secure Socket Layer (SSL) application (this is an encrypted telnet). It is important to know that when someone is connecting to one machine through telnet, the password they write flows in the network without any protection.

There is another problem with the data. It is referred to as identity spoofing, i.e. someone pretends to be another user. The solution for this problem is the use of some kind of digital signature. System based on public/private key can be used. These aspects are usual more important in Internet, than inside an internal network.

All the security systems has to have an auditing system in order to collect the information necessary to identify and to know what actions have been done by intruders. The auditing systems uses log's to store the information and it is wise to save these logs in another machine in order to make it difficult for the intruder to change or remove the logs.

Backups

The security policy must posses information about which data needs a backup, when and how often each data must be backed-up, and how much time this data must be archived (legal aspects must be considered).

It is very worthwhile to consider some automatic system that carries out the backups. The backup system should be tested. Sometimes, depending on the importance of the data and the availability of the services, redundant storage systems are required.

The backup tapes should in different locations to that where the system they are supporting, in order to preserve the information in case of a disaster. If this is not possible, some form of safety cabinet can be useful.

4.14 Service Mapping

The decision of which service can be integrated at which level or network layer has to consider the service class, the specific requirements of the service and the network layer capability. This cross analysis together with the service integration policy of the company will give the decision of which service has to be integrated in which network layer.

The service mapping procedure has to consider the following aspects:

- QoS matching. Check if the delay, delay variation bound and bandwidth guarantees provided by the layer chosen to map the service fulfil the service requirements.
- Service Availability. Check if the resiliency of the layer technology that has to support the service will provide the required availability.
- Security requirements. Check if the security mechanisms provided by the layer chosen fulfil the security requirements of the service.
- Service isolation. Check the isolation mechanisms provided by the network layer that has to support the service.

Furthermore, a risk assessment process would have to be carried out to ascertain if the network layer technology will provided the required degree of reliability in function of the impact that the service could have on the business operation and results.

4.14.1 Service Classes and Applications

The concept of Service Classes introduces a way of broadly defining the performance offered by a service thus allowing the suitability of the service to fulfil application requirements to be determined. Service classes classify services in function of their main characteristics without considering the details of every QoS parameter; likewise applications are also mapped into these classes.

For applications that require QoS, two service classes are suggested: *non-elastic* and *elastic*.

The non-elastic service class is used to support those applications that are not tolerant to uncontrolled delays and/or losses. Elastic applications are those that can control the traffic flow that they are offering to the network and therefore can tolerate some changes in delay and throughput.

More details about of the requirements and working principles of non-elastic and elastic application can be found in the TB-153.

4.14.2 Service integration

Service integration has a significant influence on the network design. The service integration policy must be defined before network design taking place. Addressing, service isolation mechanism, routing and traffic engineering at every layer must be considered regarding service integration, in order to achieve the correct network design and the expected performance.

Service integration can be implemented following three approaches introduced in chapter 4.8:

- Different services integrated over the same "Service Layer". The overall performance of the network depends greatly on the following aspects:
  - **Addressing scheme:** If isolation of every service is needed, it must be defined before the network design.
  - **Service isolation mechanism:** It must be specified, e.g. tunnelling.
  - **Service Layer traffic engineering:** This has to be carried out considering the consolidation of the traffic generated by every service. In some cases it is difficult to correlate different services in order to foresee traffic peaks.
  - **Routing:** Depending on the technology used, different routing policies can be implemented over the same service layer. For instance IP will require layer_4 routing or policy routing whereas ATM allows the definition of different virtual networks which provide independent routing and isolation.
- One service layer for every service. In this case, different services, real or virtual, are integrated over different "Service Layers".
  Addressing and routing implementation will be independently solved for every service in its corresponding service layer.
  The overall performance of the network depends greatly on the following aspects:
  - **Internetworking model:** The use of internetworking architectures presents many advantages when regarding integration of services. Some services can be supported by IP technology and some others by ATM, Frame-relay or any other technology.
  - **Service isolation** will depend on the internetworking model.
  - **The traffic engineering** of every layer is independent but both results will have to be added to dimension the transport layer.
- Different services integrated over different network layer. Some services can be integrated in the service layer, some other in the transport layer.

The integration of some critical services, like Teleprotection, can only be carried out at the transport layer whereas most services can be integrated at any network layer. That is to say, network implementation can be found to range from integration at the physical layer where only transmission equipment is shared to integration at the service layer where every network component is shared by the services integrated on the network.

The decision of the layer at which a service will be integrated depends basically on the service performance required and the technology of every layer. Although it can be stated that the possible interaction between services increases when they are integrated at a higher layer, the interaction experienced by a service depends also on the layer technology and architecture.

When two services are integrated at the physical layer, sharing transmission equipment, the only interaction that can occur is at the Common Mode Failure level, that is to say, the failure of the transmission media/equipment will affect both services.

The integration of the services at the transport layer means that the transport infrastructure is shared, so out of the common mode failure of the transmission and cross-connect equipment both services are sharing the same management platform. Furthermore, if self-healing functionality has been specified, the transport layer should be able to recover a service in an

outage situation regardless of the state of other services that could also be carried by the network.

When services are integrated at the service layer, almost every network component is shared and in order to guarantee service isolation and differentiated QoS for every service, the corresponding network architecture has to be implemented.

The integration of services by means of a Virtual Private Network implementation emulates the integration at the physical layer. Under this architecture, virtual links are generated to interconnect service users. The availability of these virtual links will depend on the global network resilience. Therefore, the interaction between services at this virtual level could be considered as a Common Mode Failure that can only occur due to a lack of network resilience. That is to say, for a poor network design with a low resilience level, an outage will affect all those services that cannot be recovered using the remaining network resources. This failure from the point of view of the user will be perceived as a link (Virtual) failure.

Integration of services at the higher layers increases the amount of network resources shared so that the reduction in investment and maintenance costs achieved is also higher. Nevertheless, integration of services at the service layer limits the choice of service layer technology so that only those technologies able to offer differentiated QoS and service isolation guarantees can be used in this kind of application.

The new generation of IP protocols provide service layer technologies that can offer the above requested characteristics to integrate services being also capable for VPN implementation.

4.15 Naming and Addressing Schemes and Plans

4.15.1 Addressing strategy

An IP naming and addressing scheme is a very important issue and has to be considered very carefully. Such a scheme must both take into consideration possible legacy systems as well as be flexible in fulfilling future needs. Once a network is built on a decided scheme it is extremely difficult and costly to change it afterwards.

A successful IP addressing scheme operates on two levels. It works on a global level, allowing related group of device to share common ranges of addresses. It also works on a local level, ensuring that addresses are available for all local devices, without wasting addresses (which in a sense contradicts another good IP addressing strategy which is a careful overestimating of the requirements, just in case).

The global issue assumes that you can break up the large network into connected regions. Having done so, you should summarise routing information between these regions. To make routing summarisation work in the final network, you need a routing protocol that is able to do this work for you. Thus, a key part of any successful IP addressing scheme is to understand the specific routing protocol or protocols to be used.

Another important global-scale issue is the network's physical geography. An organisation with a branch-office WAN usually needs a large number of small subnets for each of the branch offices. Is also probably has a similar large number of point-to-point circuits for the actual WAN connections.

However, the organisation, which is concentrated on a single campus, perhaps with a small number of satellite sites, needs to break up its address ranges in a completely different way. Many organisations are a hybrid of these extremes. Thus there is not a single scheme that will suit every organisation, but there are some principles that go into building a good strategy:

- Create large, yet easily summarised chunks
- Set standard subnet masks for common use

- Ensure that there is enough capacity in each chunk for everything it needs to do
- Provide enough flexibility to allow integration of new networks and new technologies.

A clear, logical, easily understandable addressing scheme will also improve the maintainability of the network and subsequently it's stability.

4.15.2 Registered versus unregistered addresses

When selecting the addressing range (network number) for an IP-network, several other concerns have to be taken into account such as

- Shortage of addresses
- Security
- Quality of Service

The first issue is a shortage of addresses because of the fact that 32 bits of the IP-address field of IPv4 imposes a strong limitation on the number of the non-conflicting IP-addresses available on globally interconnected network. The introduction of IPv6 with 16 bytes long address alleviates this limitation but is outside of the scope of this chapter. Network numbers are managed by ICANN (Internet Corporation for Assigned Names and Numbers), which delegated parts of address space to various regional authorities. At present most of the organisations have to use the unregistered network address ranges set aside by IETF and documented in RFC 1918:

Class A	10.0.0.0
Class B	172.16.0.0 through 171.31.0.0
Class C	192.168.0.0 through 192.168.255.0

On the outside these networks can communicate over the Internet using NAT (Network Address Translation) implemented in firewalls or routers and using just a few (one or more) registered addresses assigned by the ISP.

NAT technique, which detailed description is outside the scope of this document, is a quick and dirty fix that violates some of the principles of the architectural model of IP such as:

- Worldwide uniqueness of every single machine address
- Connectionless networking (NAT creates mapping for each connection)
- Independent protocol layering (NAT, which is in network layer, uses properties of the transport layer TCP/UDP protocols)

Implementation of NAT reduces also the pressure of implementation of the real solutions, which is introduction of IPv6.

The address space shortage could be one of the reasons for using the private (unregistered) address ranges. The other is security. Power utilities (and not only) are reluctant to connecting their networks straight onto the Internet. Thus using device addresses hidden from the Internet community provides an additional level of security. Even Quality of Service is easier to maintain in a network that is separated from the freely passing of the Internet traffic.

4.15.3 Dynamic addressing

It is obvious that the task of administration of individual IP-addresses in a large network would be quite cumbersome. Static device addressing would also prevent the ease of mobility of the devices within the organisation. Using DHCP (Dynamic Host Configuration Protocol) can resolve these issues.

DHCP is a protocol that makes it possible to automatically configure end devices. The most common things to include in this configuration are the devices IP address, mask and default gateway. It is also possible to configure several other kinds of information such as the addresses of DNS (see next sub-chapter) servers, times servers, application servers etc.

Another advantage of DHCP is the possibility of cloning the images of the individual devices, again making the work of the network administrators easier.

Assuming that not all devices on a network are active at the same time, DHCP allows also for having more physical device connected to a network that it's number of available IP-addresses. A time limited leasing procedure allows for the addresses to be returned to the address pool and for devices to be removed from a network without loosing any addresses from the pool.

To find its IP address, a newly booted device broadcasts a request for it. The DHCP server does not have to be located on the same network, it is enough if there is a DHCP relay agent on the same network that knows where to find the DHCP-server.

4.15.4 Naming schemes

Domain Name System (DNS) is an application that provides mapping between host names and the corresponding IP-address. When looking up an address on a network, computer sends out a query to a pre-configured (e.g. using DHCP) DNS-server IP addresses. This query asks the DNS server to convert (resolve) this name into an address. The greatest advantage of using DNS this way is not that it allows a human to remember the name rather than the address, although this feature is convenient. It is rather important because it allows the administrator to change IP addresses with relative ease. For example replacing one server with another would only require setting DNS to map the same name to a new address rather than changing the addresses in all the hosts needing to access this server.

The essence of DNS is a hierarchical, domain based naming scheme and a distributed database system for implementing this naming scheme.

Advent of IEDs (Intelligent Electronic Devices) in the networks of power utilities requires further standardisation of the naming schemes. It can however not be done globally since various utilities use different naming conventions for their power system components. Only the lowest level of these components, the function name, will be specified in the forthcoming IEC 61850-7 standard. Therefore it is essential that every network define its own rules for naming the components. A good example from the power utility environment is the UCTE-URTICA network concept [11] that gives unique identifiers to the different active network components as for example:

Router	r_
TASE2.Gateway	GW_
Real time Network	URTICA_
Forecast Network	ETSO_
Ethernet interface	_e
Location	Predefined abbreviation for company name

Thus Ethernet interface 01 of the URTICA gateway at ETRANS AG in Switzerland (abbreviation ETR) would have a name

GW_URTICA_ETR01_e01

Similar rules can be established for the power system components comprising IEDs.

4.15.5 Mobility

There is a need of users being connected to their home network when visiting any distant Internet sites. The IP addressing scheme imposes some difficulties for this functionality because every IP address carries both the network and the host part. Routers all over the world are configured to send packages that are addressed to a particular network to this networks "home" location and not to its individual member plugged in another part of the world. Routing based on complete IP-addresses would be impractical, creating enormous routing tables and thus astronomical costs and bad performance.

The solution for it is to create a "home agent" at every site that wants to allow its users to roam. Sites that want to allow visitors will have to create "foreign agents". A mobile host contacts the foreign agent that in turn contacts the host's home agent and gives to it a "care-of address" of the host. This way IP packages addressed to this host and arriving to its home network will be able to locate the host's current whereabouts.

4.16 Routing architecture

The sole function of an IP network is to steer packets throughout the network nodes to its final destination.

The goal of the routing function in an IP network is to direct traffic from the source to the destination in accordance with the specific user requirements and the network restrictions whilst optimising the network resources used to deliver the traffic and supporting the routing function itself.

Routing is not an isolated function; it interacts with other network components and functions in such a way that the final network performance depends not only on the routing but also on the relationship with these other components. Figure 4.11 shows the related network functions and their relations.

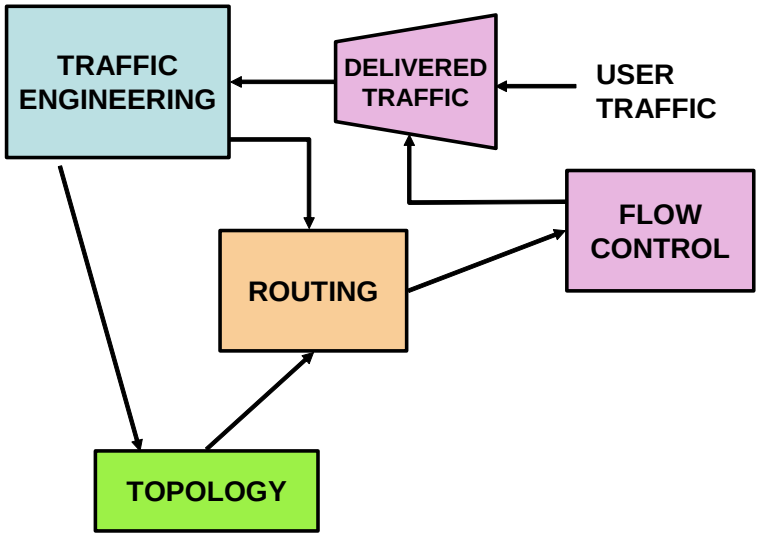


Figure 4.11 Routing Architecture

The first and most important relation is with the network topology. If the topology of the network is not adequate to the routing capabilities and do not provide links with the required capacity, the routing will not be able to perform its functions.

The most common approach to implement an IP network is by using internetworking architecture in such a way that the IP layer uses the service provided by the SDH transport layer or by an ATM layer in the MPLS approach. In most cases, there is a traffic engineering function controlling the network performance. Its function is to modify the capacity of the links between routers as well as the topology of the IP layer by adding or removing virtual links between routers in function of the traffic forecast thereby modifying the relationship between topology and routing. The traffic engineering function has to be aware of the routing function capabilities to properly choose the topology and the particular settings that modify routing behaviour.

Finally, flow control interacts and complements the routing function. More precisely, the function of flow control is to adjust the amount of traffic that is delivered to the network in

function of the capacity of the path selected by the routing algorithm with the goal of preventing network congestion. Flow control is applied at multiple levels within the network. Layer 2 protocols can have its own flow control mechanisms as well as the transport layer, like TCP, and the session or application layer. If the routing function has information about the layer 2 flow control mechanisms, it can make more accurate decision when choosing a path for a non elastic application.

Congestion control, routing and traffic engineering perform similar functions but with a different time scale as shown in figure 4.12.

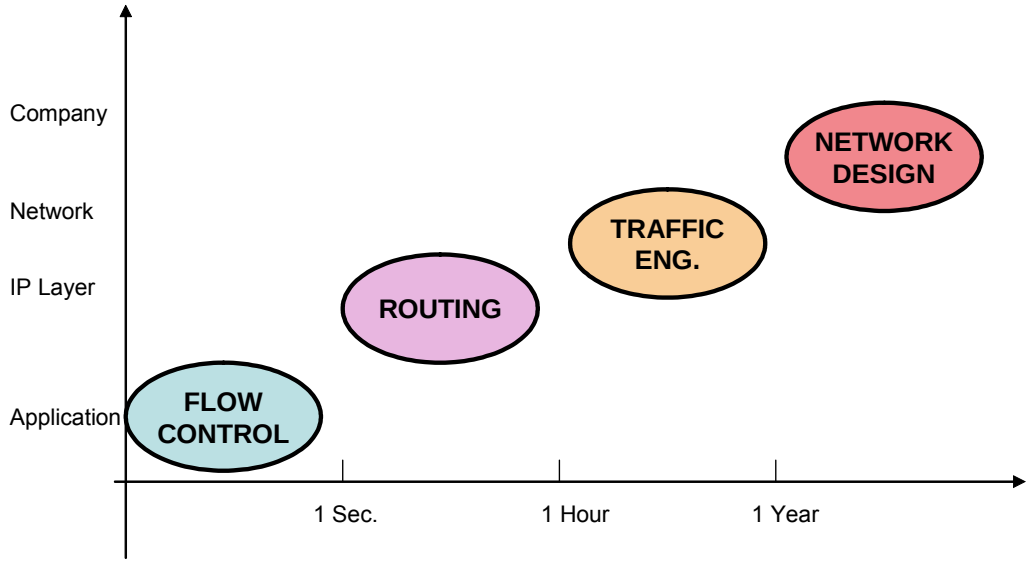


Figure 4.12 Traffic Control Components

As shown in the figure, flow control regulates the traffic in order to complement routing adaptability. Effectively, routing function can determine if the used path is compliant and if there is a better option in the network so the traffic as to be steer through this new path, but this calculation is carried out in the range of seconds to minutes. Flow control acts in real time to prevent transitory network congestion that can drive to network instability. Flow control acts at the application level whereas routing work at the IP layer. Traffic engineering works with a resolution of one hour at the network level, that is to say, at every layer of the network. Finally, the network design process affects all the company since it has to take into account the business model and other company related aspects. It is normally carried out every year or second year with a scope of five year ahead.

Routing algorithm can be static or dynamic.

- Static routing is based on predefined routes that has been pre-calculated off-line and later introduced in the network nodes by means of the network management tool. This type of routing requires only a forwarding function so no real-time computation is required at the network nodes. This type of routing is used in static scenarios when the number of users is stable and the traffic carried by the network is completely known and has a deterministic traffic profile. In this case, routes and topology can be properly defined and dimensioned in advance and will remain valid in the mid- or long-term since no changes are forecasted in the network. An alternative to this working mode is the quasi-static routing approach that, even though maintain its static behaviour, is able to modify traffic routes in response to exceptional events such as outages in links or nodes.

- Dynamic routing autonomously update traffic routing information thus adapting in real-time to changes in user traffic and network state. This working mode requires active participation of network elements to determine network performance, availability of resources and topology as well as user's traffic. In consequence, dynamic routing requires some network capacity to transmit routing update information, memory and computational capacity in the network nodes. Dynamic routing response to the generic routing problem and provides intrinsic resilience being the degree of resilience achieved function of the network topology. It can be distinguished different routing modes in function of the parameters used to determine the path.

    - Distance routing. Every link is associated to an administrative weight; the path selected corresponds to the shortest distance, that is to say, the lowest addition of administrative weights. Therefore, the route choice does not depend directly form the bandwidth, delay, physical distance or any other real parameter but on the criteria settle by the network manager. The definition of the weight of every link has to follow a homogeneous criterion in the entire network. Normally is associated to the bandwidth, which is in some way related with the delay when all the links have similar length.

    - QoS routing. This kind of routing is normally flow-oriented; by means of the RSVP or by means of a traffic classification like in Differentiated Services, the packets are associated to flows that follow the same path along the network. The task of the routing algorithm is to find a suitable path complaint to QoS flow requirements. Link delay and residual bandwidth of the links are considered for the determination of the suitable path to transfer the flow.

    - Constraint routing. This kind of routing limits the number of possible path that can be chosen for a flow in function of the origin of the information, the user, the application, etc. Due to this, a tighter control of the network resources utilisation is achieved.

    - Directory enabled routing. This routing approach selects the path from a directory in function of the user, the application, or any other parameter defined by the network manager. Although this could provide flexibility for LAN or MAN networks its application in WAN has not proved to be operational and stable due to the lack of adaptability to network changes, the difficulty of implementing reliable distributed directories and the time required to update the directory information.

The following table shows the performance of the different routing architectures and the factors that have to be considered in the network design.

	Resiliency	Scalability	Elastic Applications	Non-Elastic Applications	Traffic engineering Interface
Static Routing	NO	NO	YES	No guarantees	Easy to interface
Distance Routing	YES	YES with OSPF Limited with RIP	YES	No guarantees	Easy to interface
QoS Routing	YES	YES	YES	YES	QoS parameters have to be updated by traffic engineering
Constraint Routing	YES	YES	YES	YES	Some difficulty in controlling routing rules

Table 4.1

4.17 Traffic Engineering

4.17.1 Introduction to Traffic Engineering Concepts

It has been shown in previous chapters that the traffic flow intensity together with the origin and destination of every flow is the starting point for the calculation of network, links, and node capacity. The traffic offered to the network is not constant and it is changing over the day and continuously increasing in the long-term time-scale. Therefore, the design of the network has to consider these changing working conditions and in consequence some extra capacity has to be allocated to deal with traffic peaks and outages in order to guarantee that the network would maintain its performance in extreme situations.

There are two basic ways of achieving network performance, by means of network over-dimension or using traffic-engineering techniques.

Network over-dimension is substantially expensive and does not provide firm performance guarantees. It is intrinsically not a sustainable method to offer network performance guarantees since it oblige to a continuous capacity increment in order to stay always in the over-provision situation. When measurement mechanisms are not provided, it is not possible to assert that the network is really over-provisioned so in consequence there is no means to forecast network performance and of course it is not possible to offer any kind of performance guarantee.

On the other hand, traffic engineering provides a set of control mechanisms that work all together to prevent congestion by adding capacity when and where is needed. Thanks to this, network performance can be guaranteed over a long-term period.

Traffic engineering concept was initially developed with the advent of the telephone networks. After the formulation of the Congestion theory and applying these principles to network design the early public telephone networks were deployed. These network relied on hierarchical routing where route were fix and hierarchy was used to accommodate overflow traffic into alternative routes. With the introduction of digital switches more sophisticated routing principles such as dynamic routing or time-dependent routing were introduced.

Datagram networks make traffic-engineering implementation easier since its routing principle is basically dynamic and adaptive. This kind of networks can cope with link or node outages without problems due to the intrinsic adaptability of its routing algorithms. Nevertheless, it has been shown how the routing principle based only on administrative weights is not adequate to prevent congestion since low weighted links attract traffic in such a way that they get congested without the rest of the network being aware of this situation. In order to avoid this pitfall, two basic actions were taken:

- More sophisticated routing algorithms were introduced. These new algorithms considered, amongst other parameter, the residual capacity of the path in such a way that congested areas are avoided.
- The overlay model or internetworking architecture was proposed. Instead of interconnecting the IP routers directly by means of communication links, underlying layers such as SDH for transport and ATM and more recently MPLS were introduced. These layers provide virtual connection between router with the capability of dynamically modifying its capacity and the configuration of the connections so the IP layer topology can by modified on the fly. Thanks to this, capacity and topology can be adapted to the actual traffic requirements almost in real-time.

Traffic engineering is an indispensable network function that controls the way the network responses to changes in the traffic intensity and other internal network changes like outages or topology modifications.

The main goal of traffic engineering is the evaluation and optimisation of the performance of the network in order to achieve a reliable network operation whilst network resources are optimised. The parameters measured to perform traffic engineering include delay, delay variation, packet loss, and throughput. An important objective of traffic engineering is to provide a reliable network operation by including and deploying mechanisms to improve survivability and minimise the effect of outages.

Traffic engineering is performed by controlling how the information flows through the network, thus determining the path the information has to follow to reach its final destination and then providing the required links capacity to support service requirements. Traffic engineering is a process that comprises both off-line network design and run-time operations. In fact the process of designing a network continues once in service. This redesign process, mainly driven by changes in the traffic load carried by the network, is controlled by means of traffic engineering functions. Hence, traffic engineering could be considered a phase of the network design process as well as the main task of the network redesign process. Traffic engineering could be totally or partially automated by using applications that could be distributed amongst the network nodes or installed in the control centre from which the network configuration is controlled.

Figure 4.13 shows the model for network traffic engineering. The input driving the network is the addition of a predicted average traffic load plus an unknown forecast error and other variations that form a noisy traffic load. The basic function of the network is to carry this traffic from its origin to its destination in the most effective way. The traffic engineering process is based on the measurement of network performance data. From this information, corrective actions are taken in order to maximise the performance under all conditions of traffic load shifts and network failures. These corrective actions are carried out by means of the traffic engineering functions that can be classified into three groups: traffic management, capacity management, and network engineering.

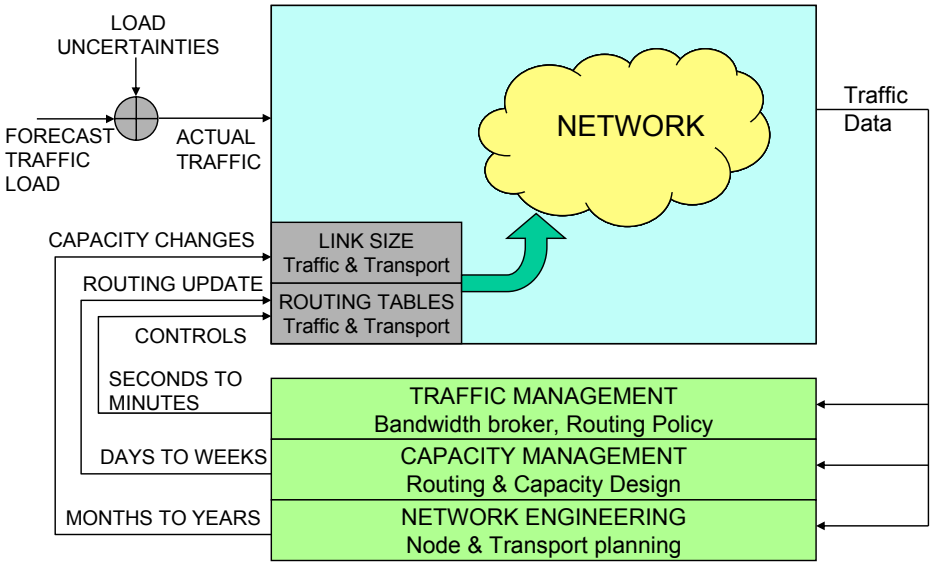


Figure 4.13 Traffic engineering model

Traffic management provides monitoring of network performance and includes traffic management control such as:

- Call routing, which could require number/name translation to routing address. (For circuit switched and connection-oriented networks)
- Connection or bearer path set-up routing methods. (For connection-oriented networks)

- QoS resource management.
- Routing table management.

Traffic management takes short-term actions in the range of seconds to minutes.

Capacity management includes daily and weekly performance monitoring, capacity forecasting, and mid-term, in the range from days to weeks, adjustment.

Network engineering includes long-term node planning and transport network planning. It operates over a horizon of months to years implementing new node and transport capacity.

The final goal of traffic engineering is to prevent network congestion since it is one of the most significant problems in operational IP networks. A network element is congested when it experiences sustained overload over a period of time. Congestion degrades network performance thus the service quality experienced by the user would be affected.

Congestion management policies could be classified in accordance with three different criteria, the response time scale, the working principle -whether preventive or reactive-, and the management scheme whether demand side or supply side.

Congestion management on the long term, weeks to months, is carried out by means of the capacity planning. Future traffic demand and distribution is estimated and the required capacity is provided.

Congestion management in the medium term, minutes to days, could be implemented by means of the combination of several control policies that without increasing the capacity of the network modify traffic routes in order to direct traffic flows to that areas of the network that are less congested. These operations could be implemented in some cases by modifying the connectivity between routers by acting on the underlying layers. The feasibility of changing these connections in real time in related with the internetworking scheme. That is to say, in function of the technology of the underlying layers, SDH, ATM or a MPLS backbone, different capabilities and connection set-up times will be provided.

Congestion management in the short term, seconds to minutes, is carried out by means of buffer management in routers. The most popular approaches are the Random Early Discard (RED) that discard packets in function of the congestion state of the queue, and the Explicit Congestion Notification ECN that signals the congestion state to the end systems.
Congestion management method can be reactive or proactive. The former is based on congestion measurement whilst the latter prevent congestion by taking proactive actions based on traffic forecast.
Congestion can be avoided acting on the demand side or on the supply side. That is to say, restricting the access and the use of the network to the greedy users or expanding or augmenting network capacity to accommodate the offered traffic load. Both methods could be combined in such a way that some group experience committed QoS while some others have a best-effort service that implies reducing the throughput during congestion periods.

The effectiveness of traffic engineering and the range that congestion management methods could prevent the network from a collapse depends on a great extend on the network architecture. It has been shown how traffic engineering acts on the IP network parameters such as routing tables or buffer management; nevertheless, the capacity to accept large traffic variations can only be achieved by acting on the underlying layers that connect routers. Although a SDH transport layer could provide some degree of flexibility, it is only the ATM that could provide the required flexibility to modify both capacity and topology almost in real time.

ATM provides a powerful control plane that could interact with the traffic engineering functions to dynamically modify the bandwidth of the router interconnection links as well as the IP layer topology with a very short latency. The ATM plane could also carry out actions on the long term but it would be more economically efficient to use the SDH or a WDM layer when the capacity managed is very high. MPLS or the new optical version (MPλS) integrates both concepts in a more simple and easy approach. The LDP protocol and its associated

algorithms for path establishment and release make up a powerful control plane that is smoothly integrated in the IP "world". Figure 4.14 shows the typical internetworking architecture as depicted and developed in reference [1].

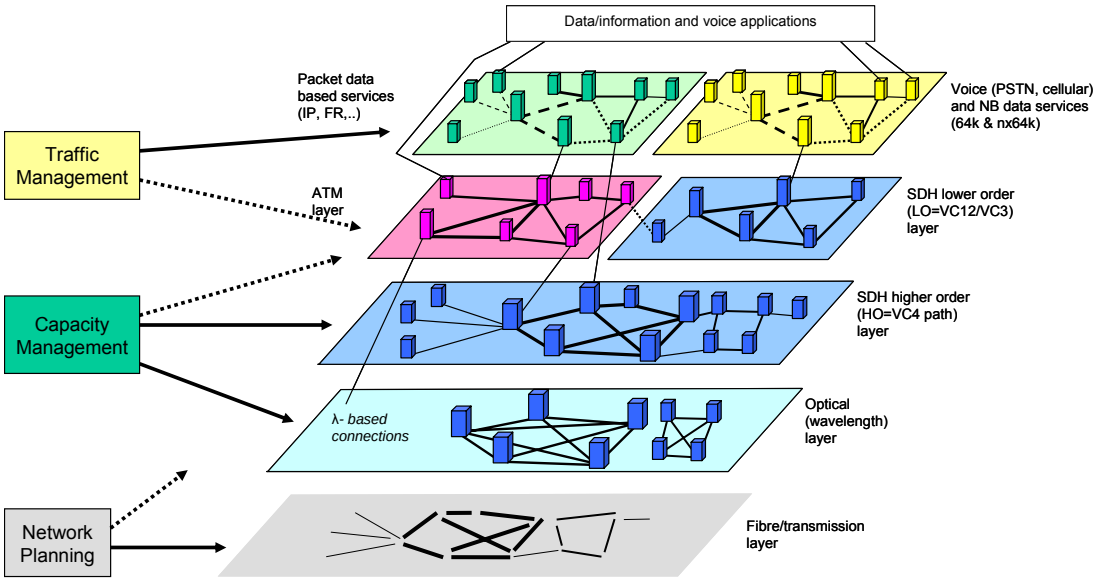


Figure 4.14 The role of the internetworking model

4.17.2 Traffic Engineering Process

The process of implementing a traffic engineering methodology can be broken down into four main phases:

- *Definition of Control Policies*. Traffic engineering should develop the policy of the company that may depend on several factors such as the business model, the cost structure of the network, and the operational constraints related to the offered services.

- *Measurement*. The state of a network can only de determined by means of the measurement. Measurement will only provide raw data, the network engineer will have to define which data are relevant to determine the performance of the network and to measure the QoS offered to network users.

- *Performance analysis*. A number of qualitative and quantitative techniques are used to determine the state of the network and to characterise the traffic workload. The goal of the analysis phase of this process is to investigate the traffic distribution across the network identifying existing or potential bottlenecks and other network flaws that may result from a poor network design or an improper network architecture definition. Simulation or modelling based analysis is sometimes used to carry out this process. Traffic engineering models can be classified as either structural or behavioural. The former depicts the organisation of the network whereas that the latter focus on the network dynamics and the traffic load. Behavioural models are singularly useful for network performance analysis and used together with network simulation tools to analyse the possible existence of any network design flaw such as single point of failure, bottlenecks or hot spots that might require optimisation actions.

- *Performance optimisation*. This phase involves the selection of the optimisation actions that would have to be taken to improve network performance. These actions

could involve either the control of the offered traffic or the distribution of the traffic across the network. Adding additional links or increasing link capacity might be necessary to achieve performance goals. Starting a network planning process to improve the network architecture, network design, network capacity, etc. might be mandatory to accommodate to current and future traffic growth. Network performance optimisation is a continuous process formed by real-time actions and non-real-time network planning processes. The difference between them is the time scale and the granularity of the actions. The former controls the distribution of the actual traffic over the existing network resources whereas the latter initiates actions to evolve architecture, technology, topology and capacity of the network to cope with traffic growth. Network engineering and real-time performance optimisation are mutually complementary activities. A well-designed network makes real-time optimisation easier and more effective.

4.17.3 Traffic Engineering Systems Classification

There are a number of different traffic engineering methodologies that can be classified in different categories in function of its working principle or its final objective.

Time-dependent traffic engineering takes historical information based on periodic variations, hour-to-hour, day-to-day, etc., to pre-program routing plans and other traffic engineering mechanisms. Random variation of the real-time traffic is not considered by this methodology.

State-dependent traffic engineering adapts the routing plans in function of the current state of the network. Constraint-based routing is an example of this kind of mechanisms.

The computation of the routes can be carried out off-line for those scenarios where routing plans are not real-time critical, whereas that on-line computation is required when routing plans have to adapt to the changing network conditions like in state-dependent scenarios. On the other hand, the computation and control can be centralised or distributed.

The traffic engineering control system can be Open-Loop when the traffic engineering actions do not take feedback information from the current state of the network or Closed-Loop when current state is considered in the traffic engineering decisions.

The selection of the traffic engineering method depends on the policy, the business objective, and the constraints of the service offered by the network.

4.17.4 Requirements for IP Network Traffic Engineering

There are a number of high-level generic requirements for IP network traffic engineering that do not affect the functionality but represent quality attributes such as:

- *Usability.* Represents how easy a traffic engineering system is to deploy and operate.
- *Automation*. A traffic engineering system should automate as many function as possible in order to reduce the amount of human effort in operate and maintain the system.
- *Scalability*. A traffic engineering system should have a scaleable architecture in order to be able to remain functional regardless of the traffic and network size growth.
- *Stability*. It is a very important aspect of a traffic engineering system since it has to be able to support sudden traffic or topology changes without losing its performance.
- *Visibility*. A traffic engineering system should include functions to collect statistics from the network in order to analyse the network performance.
- *Security*. Since security is a critical consideration, adequate measures must be taken to protect the integrity of a traffic engineering system.

On the other hand, some basic considerations in those functions that form the core of the traffic engineering system have to be taken into account in order to improve the whole system performance. The functions that have the most impact on system performance are routing and internetworking model architecture.

Routing impacts many of the key performances such as throughput, delay, and utilisation of network resources. Therefore, routing algorithm has to take into account traffic characteristics and network constraints such as topology, residual capacity, delay, etc. during the route selection process. Constraint-based routing is a routing method that adapts to traffic requirements so it is strongly recommended in order to optimise system performance.

Another aspect to be considered is the network survivability that refers to the capability of a network to maintain its service in presence of faults. Survivability is an issue of concern in mission-critical networks. In order to improve this feature, extra capacity and the mechanisms to relocate traffic has to be provided. In the IP layer, re-routing actions are taken by the routing algorithm in order to divert traffic on the event of an outage. When an internetworking model is used, every layer has its own protection and restoration capabilities, the co-ordination across layer it is not always feasible due to possible incompatibilities between technologies and administrative domains. In this case minimisation of function duplication across layers is one way to improve the co-ordination.

4.17.5 Network Engineering

To maintain an operational IP network over a period of several years will require implementing traffic-engineering methodology in order to redesign the network so that it can maintain its performance regardless of the natural increment in the number of users and the intensity of the traffic offered to the network. Nevertheless, traffic engineering have some limitations and when changes in the network are so important network engineering techniques have to be applied in order to update the topology and links capacity.

Network engineering is the long-term process of the more generic traffic engineering one, that deals with the control of the underlying layers in order to provide the required capacity and topology, building a relatively static network that fulfils traffic-engineering requirements. Namely, network engineering adds capacity where it is more profitable for the traffic the network has to carry.

Although most transport networks are static, the common trend nowadays is to use an internetworking approach. This includes an ATM/MPLS layer that provides flexibility and dynamism and converts former dummy pipes into a service of switched connection controlled by a powerful control plane whether by the ATM signalling or by means of the MPLS LDP control plane. This new capability of adding or deleting capacity of the transport network has profound impact on the IP plane since the traffic engineering function can now adjust the network topology according to the traffic carried by the network in order to optimise the overall network performance.

Figure 4.15 shows the control process in a network as a closed-loop process that maintains network performance despite traffic load variation by means of a closed-loop process formed by the traffic engineering function. This steers traffic through the proper routes and the network engineering that provides the right topology and links capacity in function of the traffic engineering request and the actual topology of the network by controlling the underlying layers.

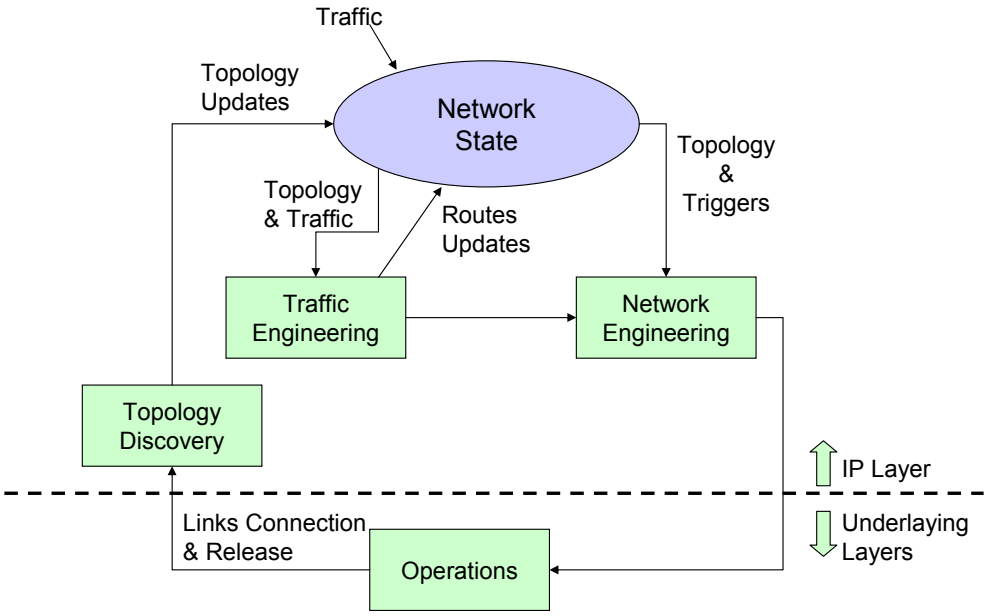


Figure 4.15 Network Engineering Process

Network engineering process could be activated by several reasons:

- A change in the network topology due to an outage or a recovery from an outage.
- On a congestion condition that could not be controlled by the traffic engineering function.
- On a sustained link overload condition since, in this case is desirable to increase the link capacity, the network engineering function can increase the capacity or add another link in parallel.
- On a regular basis to assure that the network is making the most efficient use of its resources.

Network engineering function is particularly interesting when network resources, especially links, are not self-provided and therefore to release a link for some time implies some saving in the operation of the network.

4.18 *Simulation*

The decision of carrying out a network simulation should be guided by many criteria:

- The measure that are of interest to be predicted.
- Acceptable runtime of the simulation.
- Working conditions that are of interest to be analysed.
- Networking technologies since some technologies may not require a simulation process.

The primary goal of the network simulation is to validate the network design by testing different working conditions. Worst case conditions and the busy hour traffic load are normally applied to verify the capability of the network design.

The goal of this test is not only to test the network performance but also to verify the service availability or, when required, find out what are the service performance limitations.

When required, by applying emergency scenario conditions to the network model, contingency planning can be checked.

The flexibility of a network model and the capabilities of most simulators allow QoS performance as well as Service Level Agreement compliance to be verified under different working conditions. It is important to understand the working principle of the networking technologies involved in the network to test those aspects that could potentially impair the network performance in order to rationalise the network test process and therefore prevent and endless simulation process.

The simulation process could also be used to experiment new working conditions like integration of new services or changes in user or server location analysing the impact these changes could have on the network performance.

Finally the simulation could also analyse the scalability of the network technology and architecture. It is feasible to increase both the number of users and the traffic load of the network several order of magnitudes to test the scalability and try to find the limit of the architecture under study.

The simulation process starts with the definition of the network model that includes the following topics:

- Topology definition.
- Links capacity and transmission characteristics defined by:
  - Bit rate
  - Propagation delay
  - Bit error rate
  - Availability expressed by means of MTBF and MTTR
- Switching nodes capacity and technical characteristics defined by:
  - Throughput
  - Transit delay
  - Memory
  - Availability expressed by means of MTBF and MTTR
- Location of users and server defining the access interface.
- Routing criteria used in the network.
- Network and transport protocols as well as the link layer protocol that has to be used in every type of links. The configuration parameters of every protocol could be changed in very simulation run to test and validate the settings that will have to be used in the real implementation.
- Traffic definition. It has to be studied and defined every kind of traffic source, that is to say, every type of data transaction. The source of this information is the traffic matrix that depicts every data flow transfer through the network. The mode information is transfer and the intrinsic data format determines the data traffic profile generated by the traffic source. It can be distinguished four basic information transfer methods:
  - File transfer. Data to be transmitted are content in a file. Delay or data integrity applies to the file not to every packet or block transferred through the network. The traffic profile is defined in function of the data file size. The inter-arrival time and probabilistic distribution of the file generation event is also a relevant parameter to define the file transfer data model.
  - Connection-oriented session. Data packets are transmitted randomly. In order to define the traffic profile, the inter-arrival time and probabilistic distribution of packet generation as well as the packet size probabilistic distribution, have to be provided.

- Event-driven data transmission. It models the case of spontaneous data transmission like alarms or other notifications. In order to model this type of data sources, inter-arrival time and probabilistic distribution of packet generation as well as the packet size probabilistic distribution, have to be provided.

- Pooling as a special case of a connection-oriented session. It is an almost deterministic case of a connection-oriented session that models the case of a communication session established between a control centre and a number of remote stations. In order to model this session, the pooling frequency as well as packets sizes has to be provided.

The worst case traffic load has to be used to carry out the simulation. This condition occurs normally at the busy hour. Nevertheless, for networks carrying bursty traffic, defining traffic generator with the average load of the busy hour might not be the worst case due to the smoothing effect of the average process. For this kind of traffic profiles, worst case has to be identified by analysing real time traffic.

Once defined all the parameter that will define the network model, the simulator technology has to be chosen.

The simulation process can be carried out using three basic techniques:

- Discrete event simulation. This kind of simulation process represents the real world in great details. The actual behaviour of the network is represented taking into account every detail, analysing the network state packet by packet, byte by byte or bit by bit in function of the simulator or the working mode chosen. The result will be as accurate as desired provided that the description of network components and traffic sources correspond to the behaviour of the real devices. The simulation will present what will happen in the real network but at the cost of a great computational load that will be higher in function of the accuracy desired.

- Analytical modelling. This mode of simulation abstracts the real world into systems of equations that can be solved directly or via algorithms. Using this model, data flows transported by the network are assumed to obey some probabilistic distribution defined by a set of parameters. Analytical queuing and theoretical models are used to compute the performance of the network. Delay, delay variation and losses obtained from the simulation process are statistical results. Its degree of accuracy depends on how close would be the real devices from the theoretical models. However, only statistical results can be obtained from this type of models whereas discrete event simulation can evaluate maximum guarantee delays and any other guaranteed parameter. The computational cost of an analytical simulation is much lower that the required by a discrete event and less dependent of the traffic load and size of the network.

- Hybrid modelling. This mode of simulation takes the advantages of the two previous modes presented above but trying to avoid their disadvantages. By using analytical modelling for those networking technologies that are intrinsically more deterministic and discrete event simulation for those events that present a stochastic behaviour the simulation process speeds up without jeopardising the accuracy of the results.

The presentation of the simulation results depends on the tool used. In general, tables compiling the results are presented and tools to perform statistical calculations are provided. Furthermore, when event simulation is carried out, real-time graphical representation of chosen parameters can be obtained whether on the fly or after the simulation is finished. Although graphical representation of results could introduce a lack of precision since we lost the exact figures, it clearly shows what is happening in real time in the network. The averaging of the results of a packet network simulation is very dangerous since the smoothing effect of the averaging function prevents real time problems like spurious lack of QoS to be shown and detected.

As shown in figure 4.16, despite the fact that the average load of this link is not so high, there are short periods of time in which the line is fully busy so an extra delay of up to 5 seconds could be introduced in some packets. This type of graphics helps identifying the source of unexpected spurious delays.

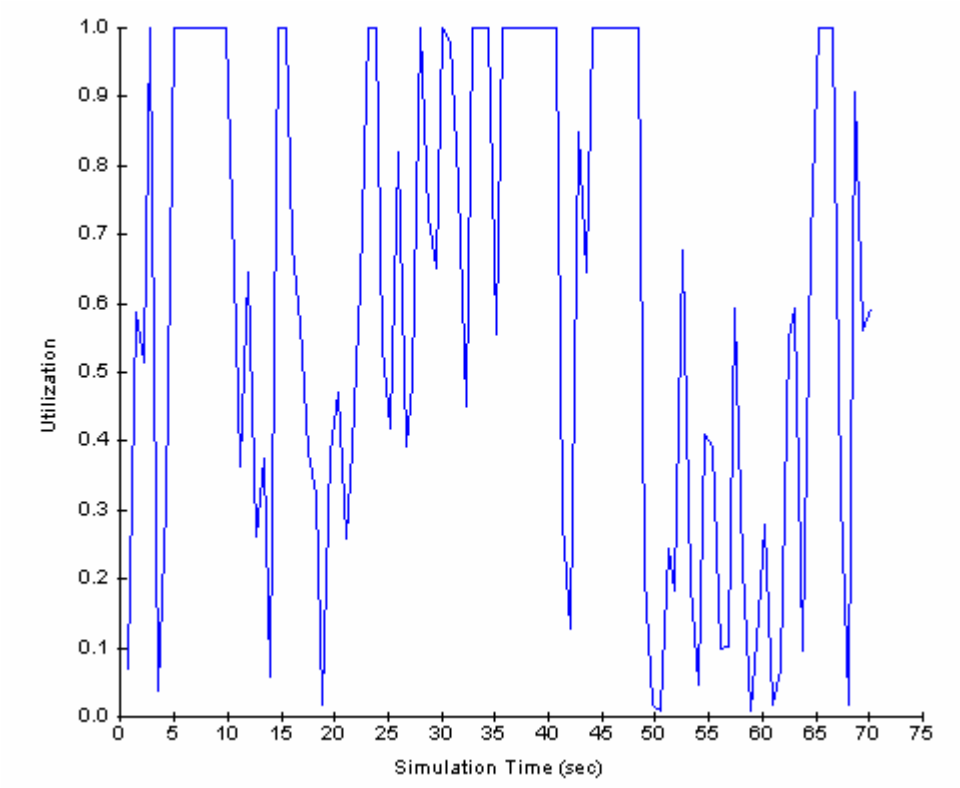


Figure 4.16 Real-time trace out

The study of the results should include a routing stability analysis as well as a measurement of the convergence time of the routing algorithm. These parameters are normally measured when a fault in a link is simulated. In response to this event, the network has to divert the traffic to other links that might cause overload and subsequent traffic diversion until a new stable working point is found. The time needed to find this new stable working point and the compliance of the SLAs during this transient period has to be analysed in order to validate the network design.

5 Network Implementation

5.1 Introduction

Most utilities have a telecom network that is dedicated to mainly operational services like SCADA,/EMS, teleprotection and utility internal telephony. Today, many companies may already have an administrative IP network, either using their own telecommunication infrastructure or leasing communication services from third parties (public operators).

An IP network serving *operational* applications within a utility is far more stringent in its requirements than an IP network serving *corporate* internal IT applications, in particular with respect to real-time requirements and service availability. A bridging of corporate and operational networks will have to be considered to provide a unified network serving all applications. This bridging is sometimes referred to as a converged corporate network solution, and a successful implementation must be based on a well-defined strategy with respect to integration of legacy infrastructures and new networking technologies.

5.2 Implementation options

The options considered here are *new site*s that offer the best opportunity for installing new IP technology, and *existing sites* that need to deal with the integration of legacy infrastructures and services.

5.2.1 New sites

New sites can be broadly characterised as follows regarding communication:

- Introduction of substation LANs based on Ethernet technology
- Installation of IEDs with Ethernet/IP LAN connectivity
- Remote supervision and remote settings of equipment / IEDs
- New communication architectures as defined in IEC61850
- Reduced number of proprietary buses and protocols
- Access to a wide-area backbone network (WAN)

However, in almost all cases even new substations are part of the existing power grid and connect to an existing WAN, and this implies that connectivity over the WAN to other sites has to be ensured.

This means that even Greenfield sites (see chapter 2) cannot be considered as self-contained islands; there are implications on the existing telecom infrastructure as well as on the prevailing applications like network control and protection systems. The strategy applied to Greenfield sites needs therefore take into account all aspects of embedding the new site into an existing larger environment.

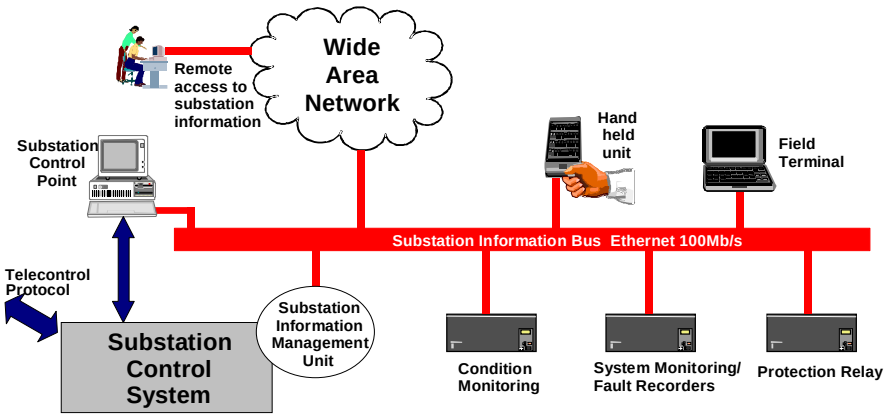


Figure 5.1 Greenfield Site with full Ethernet Connectivity

The figure above illustrates a possible configuration for an informative network. Operational data such as remote control commands are still communicated via a separate point-to-point data link. This restricted use of the IP network offers increased operational security and lower risk than a fully integrated network. It may be the initial choice until network performance and security for operational use is more clearly understood.

The Information Management Unit (IMU) collects data from connected devices and if necessary reformats the data into a WEB browser format. The device will be essential in existing sites as discussed in the next section (5.2.2).

To ensure reliability of data in the substation environment and to eliminate the effects of ground potential differences under fault conditions optical fibre will be the preferred transmission media. Optical fibres will also ensure that the LAN infrastructure is to some extent future proof and will allow higher bit rate upgrade as requirements and the available technology progresses. Optical data formats are readily available for Ethernet 10 Base FL and 100 Base FX for 10 Mbps and 100 Mbps transmission speeds respectively.

Performance requirements will depend on the use for the LAN. For information purposes 10 Mbps with shared hubs will probably suffice. For operational data IEC 61850 specifies the performance requirements. Under a power system fault condition typically 90 data messages will be generated within 1 ms and should be delivered within 4 ms. To achieve this level of performance 10 Mbps network with switched hubs or 100 Mbps with shared hubs will be required.

When building a new substation there are two main procurement options, firstly to award a contract to a major manufacturer that can supply both primary and secondary equipment that are compatible with IP technology, or secondly employ a system integrator who will specify equipment from a range of manufacturers. The level of IP connectivity for the greenfield site will depend upon the procurement method chosen. Many manufacturers have their own favourite field bus for interconnecting equipment at bay level, for example Modbus or Profibus with an Ethernet IP connection at station level. If a systems integration approach is chosen it is more likely that equipment will be interconnected using an Ethernet IP LAN both at bay level and station level.

5.2.2 Migration

In developing the migration strategy for changing the communications architecture in a substation, there is a need to examine the different approaches possible and to match the

best process retrofitting in the presence of legacy systems and to ensure that the correct constraints are taken into account.

At a general level, the key phases involved in such a project are:

- Checking existing assets at bay and substation levels, i.e. collating the drawings, identifying the interfaces and functions involved in the changeover, power supply requirements, as well as any associated issues, such as obsolescence of equipment/systems etc.

- Evaluating retrofit constraints such as the maximum and minimum outage duration possible, identifying whether any key functions are going to be degraded and the risks associated with this, the testing principles to be employed, etc.

- Definition of preferred strategy, e.g. total or partial replacement, big-bang or step-by-step, the introduction of new features, etc.

- Cost/Benefit evaluation and prioritisation (lifetime cost, performance indicators, return on investment).

- Detailed design may be necessary for the handling of Protection and Control changeover, depending on the requirements and the scale of the project.

- Optimal maintenance procedures should be identified and possibly designed into the project, such as reliability centred maintenance, work orders management, etc.

Further practical constraints for projects of this nature include:

- The need to keep the SCADA interface untouched.
- Maximising the reuse of existing devices with regard to overall costs.
- Ensuring compatibility with legacy systems and environment.

Costs associated with retrofit programs include:

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

Migrating from existing technology to new IP capable plant whilst protecting existing investment will require careful planning and management. The investment in legacy devices will be considerable; they will not be replaced overnight. The investment made will be written off over a number of years precluding their immediate replacement with more modern devices and systems. Moving to a system interconnected with IP technology is not just about building a network. It is planning the replacement of equipment and plant and integrating existing technologies with new IP products as they are installed.

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

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

Legacy devices present two problems when connecting them to a LAN. The information, if at all available, will be in a variety of formats and most equipment will have a serial port. The minimum that will be required is for the communication ports and data transmission formats to be converted into an Ethernet 10/100 Base T (copper) or FL (optical fibre) formats.

The simplest solution for a small number of legacy devices to be accessed is to use a stand-alone Terminal Server. This provides serial to Ethernet conversion for individual devices. A Telnet session can be established between the remote user and the device to be accessed. Where there are a number of serial devices to be interfaced it may be more appropriate to use devices with multiple ports. Multiport Terminal Servers are available with multiple serial ports to one Ethernet port.

Information from legacy devices will usually be in a manufacturer's proprietary format. To make the information more widely accessible an Information Management Unit (IMU) or Information Server can be installed at the substation. This device may interface directly with the existing serial ports and provide information storage and processing facilities.

An IMU can interrogate legacy devices via a serial port or interrogate Ethernet device via the LAN and store information from them. With appropriate programming the information can be reformatted into an HTML Web page for display using a standard Web Browser. Without the IMU facility accessing and managing data from legacy devices it will be difficult to achieve the benefits associated with IP technology.

Telecontrol services can be implemented over an IP network. Commonly used standard protocols are:

- DNP 3.0
- IEC 60870-5-101/104 for telecontrol systems
- IEC 60870-6 TASE.2 for control centre interconnection.

With DNP 3.0 direct connection is achieved by using the 'Protocol Encapsulation Function'. With IEC 870-5-101 a Packet Assembly Disassembly (PAD) is required which will encapsulate 870-5-101 messages into IP packets, and carry out the address translation function. With IEC 870-5-104 RTUs, RFC 1006 "ISO transport services on top of the TCP" refers. Direct connection using the Ethernet/IP interface is possible. With IEC 61850 compliant IED, direct connection is possible through an Ethernet/IP interface.

The migration solution has in any case to ensure that the requested QoS (Quality of Service) is achieved with the mixed architecture, and that the performance monitoring facilities are available. QoS in the context of operational applications is mainly related to delays (latency), cycle times, service availability and error performance.

Connection of the S/S LAN to the WAN will normally be accomplished via a Gateway/Router. Services like voice, teleprotection or SCADA employing point-to-point communication will connect via a number of serial interfaces to the WAN.

On an existing site the LAN can be station wide or may be installed just to serve particular items of equipment that have an informative interface, extending the network as and when new equipment is installed.

More on the subject on Migration can be found in the CIGRE Paper "Substation Migration into an IP Network", Paper C35 presented by WG35.07 in CIGRE Paris 2002 session.

The migration of the WAN infrastructure that is not related to substation communication, such as transmission or transport equipment, should be carried out on a network-layering basis. The suitability of using existing equipment is determined during the network design phase. Specific migration plans would need to be developed depending on the complexity and number of changes that would be required to implement the new network design.

5.3 Installation and commissioning considerations

Three areas need to be addressed that require special attention:

- Operational environment
- Power supply
- Cabling

The operational environment in the presence of high voltage plant is harsher than the standard office environment that most networking equipment is designed for. Equipment designed for the office environment will have to meet the requirements of EN 50081-1 and EN 50082-1 (Residential commercial and light industry) whereas equipment installed in the harsher electromagnetic environment on a high voltage site compliance with EN 60970 (Telecontrol equipment and systems) may be more appropriate. There are however a few suppliers of industrial Ethernet equipment who manufacture hubs and routers primarily for the process industries, these equipment should be compliant with EN 50081-2 and EN 50082-2 (This standard is not as onerous as the requirements of EN 60970 but may be suitable for most applications). Industrial network devices have a better EMC performance than the standard products intended for office environment and are generally housed in rack mounting or DIN rail mounting enclosures.

Many of these industrial Ethernet products can also be powered from battery backed DC supplies that will offer enhanced security. Power supply requirements may be for 48VDC, 110 to 125VDC, 220 to 240VDC, 110VAC or 230VAC nominal voltage, depending on the particular substation.

EMC problems at the substation will come mainly from interference conducted along power supply connections and signal lines. Power supply connections are relatively easy to filter especially if DC supplies are specified. Signal lines however are very difficult to filter allowing electrical interference to enter the equipment with the potential of causing a mal-operation. There are also ground potential differences that will occur in the substation especially if there is a power system fault. To protect against EMC and ground potential problems optical fibre connections can be specified for the Ethernet and WAN ports.

Considering the Ethernet interface optical fibre interconnections can be at 10 Mbps using 10 Base FL or at 100 Mbps using 100 Base FX. Installations *between buildings* should always specify an optical fibre connection. The installation should standardise on one style of optical connector. ST connectors are widely available and used by many equipment manufacturers for multimode fibre connections. Fibre cables between buildings will probably be installed in existing cable trenches together with other services. Rugged duct cables should be specified with due regard to the physical environment in which they will exist. Most operational sites will be subject to a rise of earth potential if there is a power system fault. Here an optical cable is ideal if it has no metallic elements, an all-dielectric cable should be specified. A number of companies make suitable cables for this application.

Where local Ethernet connections are made *between equipment* within the same room copper connections may be appropriate. In this case the physical interface will be 10 Base T or 100 Base T with an RJ45 connector on a cat 5 cable. For copper connection cabling and connectors should be screened.

For maximum availability the LAN may logically be built in a ring format, or dual-LANs may be specified. Should one segment of the ring fail then a connection can be established in the opposite direction around the ring. This may be more difficult to manage especially when new connections are added to the network. Initially only a small number of outbuildings on a site may be connected, with additional outbuildings being connected as the equipment they house is refurbished. Although logically a ring may be desirable, it may be easier to manage alterations and new connections to the network if the ring is constructed physically as a star network by installing dual cable to each outbuilding and looping back as appropriate.

Interconnections within a building may be specified to be either fibre or copper depending on the building location with respect to the high voltage plant. Optical cables between equipment within a building can be made with flexible patch leads. If equipment is not adjacent to each other then flexible cords should be protected in flexible conduit. This approach makes the installation easier, outdoor cables can be very ridged and difficult to work with especially if space is limited.

If copper connections are suitable, for example where connection distances are short or EMC problems are known to be low, then 10 Base T or 100 Base T interfaces using cat 5 cables can be used. Care should be taken to specify shielded cables and connectors when copper cables are used. Shielded cables, connectors and other components, although generally available, are not normally specified in the IT environment.

Speed and type of WAN connections to the substation should also be specified. The speed of the WAN connection to the substation will depend on the substation size and the number and type of service to be supported. The minimum speed for operational services will be some kbps. A major substation may require up to 2 Mbps or even more, depending on the need for broadband services like high-resolution real-time video. An optical connection to the WAN-provider is preferable although line isolation units can be fitted to a copper connection to protect against rise of earth potential. Digital Power Line Carrier (DPLC) may be a cost-effective WAN alternative compared to the deployment of optical fibres, provided that the requested data rate is not too demanding.

5.3.1 Commissioning

Commissioning may be usefully divided into two activities. Considering the local area network, physical connectivity from point to point will need to be verified. Whether copper or optical fibre connections have been employed test requirements are well established and will verify the health of a point-to-point link. Once the network has been physically certified its operation needs to be checked using Protocol and Communications analysers.

Staff commissioning the local area and wide area networks need to be experienced in setting networks to work. At the local area traffic flows need to be monitored to ensure that connected equipment is behaving correctly and not sending rogue packets or otherwise congesting the network. The LAN-WAN connection via a router is also critical to the network operation and performance routers contain settings tables that have many variables making the setting up relatively complex. Settings may need to be fine-tuned to achieve the desired results.

Company staff will best understand the application and should specify connectivity and routing requirements. Routers have many configurable options and expert knowledge will be required to successfully set the router to work. A consultant expert in conjunction with company staff can best perform this function.

5.3.2 Tools and equipment

The majority of tools required to install the LAN cabling and other components will be in a standard installer's tool kit. For installing optical fibres some additional specialist tools will be required such as an optical fibre clever and a fusion splicer.

There is a range of test equipment available that will assess the operation of LAN and WAN networks. Hand held devices that will quickly analyse connectivity and traffic problems are manufactured by a number of companies. They will perform a wide range of tests and can be left in place monitoring the operation of a network over a period of time, collecting data at regular intervals and raising alarms if network parameters go outside of predetermined limits.

Additional transmission equipment may be required to test the parameters of the WAN, however, if the WAN is provided by a PTO, they will be responsible for ensuring its performance.

As well as measuring and checking the network performance, optical cabling will need to be checked to ensure that good quality splices have been made and that there are no micro-bends that will cause high attenuation. An Optical Time Domain Reflectometer OTDR is used to perform these checks.

5.4 Implementation risks

At the substation or power station the engineering challenges to design a local area network with commercially available networking products will be the greatest. Most network products are designed for the office environment and may not give the desired availability especially for operational purposes at high voltage sites. At operational sites the use of a network is closely related to field bus technology, which has evolved mainly in the process industries. The wide availability of Ethernet hardware and networking products has lead to the growing acceptance of using Ethernet in traditional field bus applications. Some manufactures now offer industrial Ethernet products that are more suited to the operational environment.

When considering the levels of risk associated with networking operational systems, it may be decided that a low risk approach is adopted. Information applications are a lower risk and in most cases will not directly impact on the operation of the power system. Once the IP network is in place and its operation reliability is proved, operational applications can be migrated. Following this strategy the LAN infrastructure should be designed at the outset with operational requirements in mind.

Most of these risks can be kept under control by appropriate planning and equipment selection. In the implementation phase, however, one still needs to pay particular attention to the prevention of common mode failures, electromagnetic interference phenomena and security.

Sources of common mode failures are for example alternate routes (wires of fibres) laid in the same cable duct, or redundant power supply arrangements sharing common terminals or wires. Common mode failures may even well planned redundancy concepts render totally ineffective. Even if redundancy and diversity have been included in the design concept, it has to be ensured that it is not jeopardised by the implementation. For example with automatic re-routing there is a real possibility that both routes could eventually end up being transported over the same bearer, hence destroying the "complete diversity" concept. Special measures may have to be taken to ensure that this eventuality cannot arise, e.g. define two pre-defined physically separate and independent paths.

Electromagnetic interference may adversely affect high-speed broadband circuits, as the disturbance power grows with increasing bandwidth. Cable screening and shielding together with a proper grounding concept is a prerequisite and a challenging engineering and installation task.

Security is not only related to data security and -integrity. A security concept will also consider access to equipment and installations. Access Control mechanisms ensure that only authenticated and authorised users can perform specified actions on objects. Physical protection of the system components (buildings, transmission lines, substations) is an important first line of defence against attacks. Methods depend on the local conditions. The IEEE Guide for Electric Power Substation Physical and Electronic Security (IEEE Std 1402-2000) identifies a number of physical protection measures such as fences and video surveillance systems.

Finally, it is noted that security issues are not confined to the network design and implementation phase. The provision of security is rather a permanent task, as tools and methods for malicious attacks develop at the same speed as the technology itself. It is therefore imperative that the network implementers - be it internal or external - has a clear understanding of the security requirements and has strictly followed the security policy and verified the effectiveness of the same.

6 Network Management and Operation

6.1 Introduction

Management and operation is the last step in providing the service performance agreed with network users.

The chapter is addressed to network managers and covers aspects of management and operation, including contingency planning.

6.2 Operational Risks

Once risk analysis has been taken into account in the process of network design and implementation, it is necessary to consider operational risks from the point of view of management and operation.

A strategic plan for management of the entire network and the services delivered over it is required. This plan needs to define for example who is going to detect the failure, remotely or locally repair it, redistribute traffic in the event of congestion and contact customers. In addition, processes for service level agreements with customers, service providers and internal support organisations need to be developed. A Network Management Centre (NMC) will form the core of these processes.

The Network Management Centre allows the centralisation of the control of the entire network, and also optimises the number of people required for the management function. Other advantages include:

- To reduce the need to send people to remote sites to carry out maintenance.
- To facilitate the outsourcing of the elements of the service delivery, such as fieldwork.

Operating a NMC brings a new risk associated with the loss of control of the NMC itself, which could impact the performance of the network and the services delivered. A backup Network Management Centre or implementing a hierarchical structure of network management Centres may help.

It is necessary to balance the cost of providing a backup NMC compared to the moving to another other building, with new machines, and new telecommunication channels, together with loading all the software and recovery data from backups.

Contingency planning, redundancy of control communication channels and redundancy of machines and application of management in the Network Management Centre reduce these risks. It is necessary to realise that the local equipment is only part of a broader network and service depends on the end-to-end performance.

Other relevant and hidden aspects from the point of view of management and operation are software maintenance. Management machines and telecommunications equipment, especially if talking about an Integrated Service Network, have complex software that needs to be upgraded at regular periods.

If all services are implemented on the same kind of equipment and there is a problem with migration of new software, the entire network, and therefore all services can be affected. The

major problem is that it is very difficult to test in an experimental network the behaviour of new software in the real network.

It is recommended that in addition to extensive pre-testing, to ensure that there are well developed plans that undo the changes, and to have support people ready to mobilise in case of problems.

For the more critical services, it may be necessary to have two different communications and technological based channels.

To resolve hardware problems spare cards and equipment are required and need to be distributed to strategic locations. It is important to decide when services can be out of service in order to have a compromise between risk and costs.

6.3 Network Management Tools

Once the level of integration of the management tools (see section 4.12.2) has been decided, implementation needs to take place. If the option of using one management tool for each system has been selected, this task is easier. However, more people and more training courses will be needed. Obtaining information will also be more difficult.

If implementing a customised system has been chosen, some functionality may be lost, but it is possible to obtain more homogeneous information. An important aspect is that the management tool has to be as modular and open as possible to make easy any future implementation of new functionality and to manage new equipment. The programming language, the platform used and the telecommunication protocols should be based on standards.

Of course there are mix solutions, which are usually the best solutions.

Nowadays the most standard management protocol is SNMP. Practically all equipment available has a mixture of variables joined in a tree based structure called Management Information Base (MIB). If this MIB is loaded in management software, it will be possible to ask the equipment for the values of these variables. The two main commands of SNMP is GET (read a variable) and SET (writes a variable).

The management software is simply an application that asks and receives using SNMP the values of some variables. Then it translates the values in a representative way that presents a view of the state of the equipment, the traffic over the different channels, etc. In addition, it translates all the configuration orders into SET SNMP orders. As SNMP gets the present situation of equipment, the management software usually has a database to record past information and the configuration of the equipment that has involved the SET SNMP orders.

Another important aspect of the management tools is security. Many management tools allow the creation of different profiles with different privileges.

Some of the proprietary management software does not develop the software from zero, but are based on generic software that can be modified and upgraded.

If you are considering deploying unique software for management of different equipment, it is possible to use standard products that will have to be upgraded with the libraries of equipment that needs to be managed. This may require some development work.

It is generally worthwhile to have a unique alarm window to give a global vision of the network to the operators. Some correlation software can be very helpful, especially if it can correlate alarms of different systems. On the other hand it is sometimes difficult to define the rules for correlation.

Some management programs can simulate the behaviour of the network in case of failure or traffic increase.

It is important to have backup systems that can take control in case of outages. It is worth considering having two machines for management or having some particular management functions that can be done from different machines. This has to be considered in the implementation stage.

It is possible to have two machines that have the same applications running but only one of them acts as master. If the slave machine detects that the other has failed, it takes the control. A variation of this one in order to balance the load of the machines and the management network is that one of the machines acts as a master for some of the equipment and as slave for the other. Another solution is to have two symmetrical machines that share the data, and if something is wrong manually turn off the application of the faulty one and turn on the other. An array of disks is necessary to implement this solution. Another cheaper solution is to have a spare machine or and in case of problems, load the data and applications of control. A geographical redundancy for the management tools can be applied.

Redundancy can be a costly approach, so it is important to evaluate the security requirements of the telecommunication equipment. It is important to consider that if redundancy of telecontrol equipment exists, the security for the telecommunications equipment may be reduced.

6.4 Service Level Management

The main function of a network management system is to maintain service level performance. Consequently, it is very important to know how alarms, outages, and other events affect the services provided by the network.

Modern management tools perform their function at the service level in order to maintain the performance specified with every particular SLA.

6.4.1 Service Level Management Tools

With the use of SLAs it is necessary to measure the quality of the services.

The definition of the quality of the service has been done in the SLA (Service Level Agreement). An introduction to some of the parameters that can be defined can be found in the chapter 3.

The main objective is to verify that these parameters are always satisfied. There are software applications that can measure some of them, but may be only oriented to the IP world.

For service providers, there are tools than simulate the most typical software applications and measure network behaviour. If a variable does not comply with the SLA value, it reports an alarm.

Nowadays measuring SLA's may present difficulties at the boundary between a customer and their service provider if this is not clearly defined. In many cases planned work is not taken into account for penalties.

6.4.2 Reporting Systems

The management system provides reports for both customer and network managers. The reporting system is closely related to the management system and may be an integrated application.

There are external applications that can connect to databases or collect alarms in SNMP and build reports with all the data. The reporting system has to provide a wide range of reports and present a global vision of the network.

It is very important that reports to the senior management facilitate operational, planning and investment decisions. It is also important that reports are aligned with the services. While it is important to know what equipment failures occur and to have adequate notification of network performance degradations, it is critical to know the impact on the services delivered.

A key function for the reporting system is an inventory system for all the services, equipment and installations that a company possesses.

6.4.3 Configuration and Change Management

The configuration and change of management is a functionality of the management software, but some times companies develop new software to ease the massive amount of configuration required, in order to save time and reduce the possibility of error. A generic profile is defined, and later applied.

In other cases, this application acts as repository software. It has the configuration of all the equipment, and perhaps older types too. It is possible to modify different values off-line, and later load them to the selected equipment.

6.5 Maintenance Plan

The performance of the network will be monitored by internal functions built into the routing and other communications devices within the network. The various devices should have RMON and SNMP functions to provide monitoring and management functions. A network management centre equipped with a network management facility handling the network supervision will be central to the maintenance concept.

Network faults will either be associated with network devices or the interconnections between devices. When a communication fault occurs the network management system may be able to identify a fault within a network device or its power supply, but there will also be many occasions that the fault is indeterminate from the alarms received. A site visit will be required to determine the nature of the fault.

Most equipment faults can be dealt with by replacement. The replacement devices will however need to be programmed before being set to work. For network device failures the minimum MTTR will be 24 hours at remote sites. Where there are on site support engineers, MTTR times of 2-4 hours can be expected.

If there is a fault in the interconnections between equipment then the MTTR can be much longer, especially if new outdoor cables have to be installed. In this case an MTTR of at least 2 days can be expected if replacement cable is in stock. If cables have to be ordered then repair times of 2 weeks can be expected. There should be procedures in place for making temporary repairs to infrastructure cables. This method of working will tend to keep the return to service time down to nearer 2 days even if the MTTR time for a permanent repair goes out to 2 weeks or more.

Faults that occur in the wide area network may be due to faults on the telecommunication provider's network. Again there are two aspects of failure, a failure of the transmission system or a failure of routers interconnecting the wide area links. If the telecomm company provides a routed network service then WAN failures will be managed externally. These

faults once reported are cleared by the telecomm company. The MTTR will be dependent on the service contract that has been agreed upon.

Network servers will also require routine maintenance. Updates will be required to software and databases and as the network is more heavily used additional hard disk storage will be required. This can normally be planned to happen overnight or at weekends and should not affect normal services.

As well as problems alarmed by network devices, users will also report problems or failures. These fault reports will have to be managed by a call centre, which is be closely linked with the network management centre. For effective operation users should be given a service level agreement that defines return to service times for different categories of faults. Each fault report will have to be tracked and followed up until it is cleared.

6.6 Staff Requirement

Staff requirements will depend upon the company's philosophy for providing services. Are they to be contracted out to suppliers or will in-house staff be used. Installations at high voltage sites will require contract staff to be supervised by a competent person in order to meet the safety regulations. This requirement may lead the project manger to conclude that internal staff should be used rather than to supervise contract staff.

On the grand scale, considering a nation-wide project, another constraint is the time scales for installation of the network. If the network is to be installed over a period of 3 years resources may dictate that contractors are employed, whereas if the network is rolled out over a period of 10-12 years as plants are refurbished and replaced then internal staff may be the choice.

At a local level on a site-by-site consideration it is the experience of the author's company that the resource required for installation and commissioning of a bay is typically 5 man-days. For an average size substation this equates to100 man-days. These estimates are based on installation across several different types of site within a high voltage transmission system operating at 400/275 kV. Distribution sites much smaller in size with less equipment will need much less manpower.

Once the infrastructure has been installed at a site bringing into service a new piece of equipment should be relatively quick. It will depend on how close the point of service is to the equipment. Assuming that there is no adjacent Ethernet port for the new equipment and a connection will have to be made back to the nearest hub, it will take less than 1 person-day
There is of course an overhead associated with the provision of new services and equally important ceasing of services no longer required. As well as planning the installation work, the network design has to be considered. If a new service will lead to network congestion maybe the WAN connection to the site needs to be reinforced.

6.7 Staff Training

Many of the skills required are similar to that required to managing a traditional telecomm network. Companies that have this staff resource available will need to plan some cross training to ensure that they are effective. Staff with only experience in light current equipment will need considerable retraining and they will need to work alongside staff experienced in IP networks. The costs of this will obviously vary from company to company depending on the skills base available. Training in networking skills is widely available. Courses are available at varying levels in short modules, typically of 2-5 days.

Test equipment required to commission and maintain the network may also be unfamiliar to staff and training will need to be given. Manufacturers of the equipment will usually be able to recommend certified specialist training for their products.

If a company is to manage its own optical installations, staff will need training in the splicing and testing of optical fibres. Although optical installation and test equipment is largely automated, some specialist knowledge and hands on practice is required, especially in fibre splicing to ensure consistent and good quality splices.

Appendices

A. TRAFFIC MODELS

This appendix briefly present the main traffic models in use today, relating each of them to the assumptions underneath and to the analysis method suitable for them.

1. Stochastic

Stochastic traffic models try to capture the inherent time-varying behaviour of traffic sources model each traffic source as a discrete stochastic process [17].

Most used processes are:

- ***Poisson Processes***

Poisson processes are a special (simple) case of renewal processes which are used to model the times at which packets enter a system (a node, the network, …) by means of characterizing the inter-arrival intervals (time between packet arrivals). The inter-arrival intervals are independent identically distributed positive random variables.

- *Definition*

  Poisson processes are renewal processes in which the inter-arrival distribution function is the exponential distribution:

$$F_X(x) = 1 - e^{-\lambda x}$$

  The parameter λ is called the rate and corresponds to the mean number of packet arrivals.

- *Properties*

  Poisson processes have the following properties:

  - It is a memoryless process: The traffic source behaviour at a specific moment is independent to the behaviour in the past.
  - Multiplexing two Poisson processes produces a traffic stream that is also a Poisson process with a rate equal to the sum of all the individual multiplexed streams.

- *Analysis tools*

  This process has been extensively used to design circuit switching networks where the SLA could be represented by just one parameter, the blocking probability, and switch connection admission process could be modelled as a single server queue.

  The assumptions in which this model is based are reasonably correct in this type of networks:

  - Independent inter-arrival times: Users made calls independently from one another.
  - Memoryless: Number of calls generated at 8:00 o'clock does not depend in any way on the number of calls generated last week or month.

  The simple mathematical expression for the inter-arrival times and the multiplexing property leads to a very simple mathematical treatment.

  All this properties have made this model widely used also in packet networks where the assumptions used could be strongly questioned.

• ***General renewal processes***

To overcome the lack of matching of Poisson processes to other types of traffic profiles, some more general process have also been used in conjunction with queuing analysis.
Between them, we could mention the following:

- *Non homogeneous Poisson processes*

  These processes are Poisson processes where the arrival time is not constant but a function of time $\lambda = \lambda(t)$.

- *General Renewal processes*

  These are renewal processes with distribution functions other than the exponential and have been used in queuing theory to generalise some result obtained with Poisson processes.

2. Markov Models

The need for models which takes into account the fact that traffic sources are generally not memoryless (the traffic generated at a specific point in time is not independent of the traffic generated until that moment).

Markov models rely on the use of Markov chains that are stochastic processes defined only at integer values of time. At each integer time, there is a random variable called the state at that time. For example, a traffic source which could send packets at a specific set of rates could be modelled by a Markov chain with as many states as possible rates with defined transition probabilities between rates (states).

Markov model analysis leads naturally to the matrix-geometric approach [18,19]. Another possible approach is to use moment generating functions (transforms of the probabilities) as in [20].
This kind of models is useful to studying the statistical multiplexing, packet loss, admission and access control.

The most frequently used models of this type are:

• ***Birth-Death Models***

Birth-death models are based on birth-death processes that are a Markov processes on nonnegative integers in which the only allowed transitions are from state n to the next one, state n+1, or the previous one n-1.

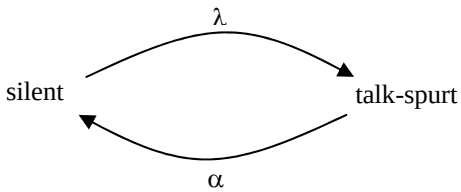
Classical queuing models based on Poisson and renewal processes (M/M/1, M/G/1 …) could also be modelled as birth-death processes and the same known results could be obtained through matrix analytical methods.

These models have also been used to directly model traffic sources as in the following cases:

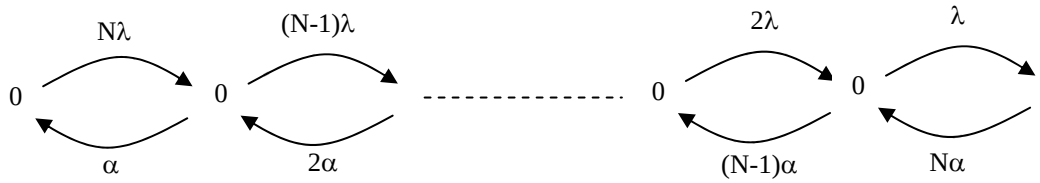
- *On-Off Models*

  Modern packet voice technologies with silent suppression have extensively made use of a two-state model where one of the states represents a talk spurt where the source is active and sending packets at a constant rate, and the other one is linked to the silent periods where the source is inactive and no packets are sent [21].

  Both states are assumed to be exponentially distributed, being λ and α the rate (probability) of transition from one state to the other:



This model allows to easily modelling a multiplexed voice stream of N independent sources as follows:



- *Markov-Modulated Poisson Processes*

MMPP processes have been used to model video traffic and is defined to be one having n states, with the process, while in any state i, $1 \geq i \geq n$, behaving as a Poisson process with a state-dependent rate parameter λ_i. Transitions between states are governed by an underlying continuous-time Markov chain.

3. Fluid models

Another family of models assumes that the traffic generated and link capacities are so large that the discreteness of the network elements (buffers) may be neglected and traffic flow becomes a "continuous" variable acting like a fluid flow.
This "continuous models" could be analyzed using techniques like the eigenvalue analysis and analytical results could be derived for complex situations. The drawback however is that the underlying assumption of continuity could lead to results far from the practical ones and a further step of "discretization" needs to be done. One clear example of that is the design of GPS schedules that are could not be implemented in practice and some discrete approaches like WFQ have to be designed.

4. Filtering approach

Another type of models that try to capture the correlation between the packets generated by a traffic source, overcoming the stochastic independence, is the autoregressive stochastic family of models.
This approximation is mainly used to derive networks performance via simulations where traffic is generated using analytical formulas derived for these models that correspond to the filter counterparts used in digital signal processing.

• *Auto-Regresive process*

To show how these models could be used, let's consider the simplest case: the Autoregressive process (AR) model applied to video modelling.
The definition for this process is:

$$x(n) = X_M + y(n)$$

$$y(n) = \sum_{m=1}^{M} a(m)\,y(n-m) + be(n) \qquad \text{Eq. (1)}$$

Where x(n) is the information volume (in bits) per frame for the n^{th} frame, X_M is the average value of x(n), e(n) is a normally distributed random number with average value 0 and variance 1, M is the degree of the model and the coefficients a(m) are parameters of the model.
In order to use this model, a(m), b and X_M are adjusted in a way that the model statistics (average rate, variance, correlation, etc.) match those of actual video sequences. Once adjusted, eq. 1 is then used to generate the traffic flow in the simulation [22].

- ***Other AR processes***

Other more complex process used which could model more accurately complex traffic statistics are the Autorregressive Moving Average (ARMA) used in [23].

5. Self-similarity

Markov and autoregressive models allow us to capture both the memory and the short term correlation properties of the usual traffic sources. However, data is send through the networks using different protocols is a layered model so in fact, the actual traffic offered to the network has somewhat different characteristics than the source itself.

In the "classical" paper by Leland, Willinguer, Taqqu and Wilson [25], the self-similarity (long term traffic correlations do not tend to 0) of Ethernet traffic is shown and other recent works have proven that Wide Area Network traffic exhibit the same properties.

To cope with this Long Rage Dependence (LRD) new models have been proposed and are one of today's hot-issues in teletraffic research [26]. The models initially derived that possess self similar characteristics are derived from the previously presented frameworks.

- ***Fractional Gaussian Noise***

Introduced by Mandelbrot and Van Ness in 1968 and popular in hydrological modelling (fluid modelling) has a rigid correlation structure and well known methods exist to estimate its parameters in order to fit the measured values from the actual data.

- ***Fractional ARIMA***

Fractional Auto-regressive Integrated Moving Average (fractional ARIMA) presented in [24] is an autoregresive model that exhibits not only short range correlation but also long range correlation. Well-known methods to estimate its parameters are also available.

- ***Aggregation of Renewal Reward Processes***

In this case, the model tries to take into account the underlying physical processes that are at the roots of the self-similar nature of the traffic but this link is difficult to found in the case of telecommunications *networks.*

6. Regulated models

All models presented so far share a common assumption: we are trying to model a traffic source from which we know some fundamental parameters, being the average rate in the simplest case or the average rate, the different moments of the time series (correlations) and a self similar parameter in the most complex one.

However in real life those parameters are difficult to know in advance and its frequently not possible to work them out in real time to design and adaptive framework so its use could at least be questioned.

One recent approach to this problem is to model the traffic entering the network not from the point of view of the source itself but as the output of some "regulating" device located between the source and the network that "forces" the traffic stream entering the network to respond to certain profile.

The most widely used traffic regulator is the "leaky bucket" [4] and a simple traffic model called (σ,ρ)-upper constrained model could be used for the regulated traffic:

$$A(t) - A(s) \leq \rho \cdot (t - s) + \sigma \qquad for\ all\ 0 \leq s \leq t$$

A complete theory based on the min-plus algebra has been developed for providing deterministic (hard) guarantees to this kind of traffic and on the effective-bandwidth concept for providing stochastic (soft) guarantees [27].

B. TOPOLOGY PLANNING AND DIMENSIONING

The mean task of optimizing the network topology (including dimensioning) is to specify the complete structure of a IP-Network with Routing strategy and Link Capacities.

It is important to optimize the Network for a functional goal, while several side terms has to be considered. The following approach is focused on optimizing the costs for the Network. The overall costs are calculated by summing up the cost for the single Links. Costs for Router and Server are not taken into account. As a side condition the End-to-End Packet delay has to be considered (it is not allowed to exceed a maximum value).

This step of the Network Planning Process includes the following key topics:

- Location of the Nodes
- Selection of the needed Links
- Optimization of the routing
- Capacity allocation
- Dimensioning of the Nodes

The selection of the location for Access Nodes, Server and Router is a principle problem of the Topology planning. The most common example for these difficulties is the positioning of Dial-In Nodes. On the one hand it is favourable to place the crossing point from telephone line and IP-Network near to the end user (based on Traffic-Flow Theories). On the other hand there are tremendous costs emerging if every Local-Voice-Exchange will be upgraded with Remote Access Equipment.

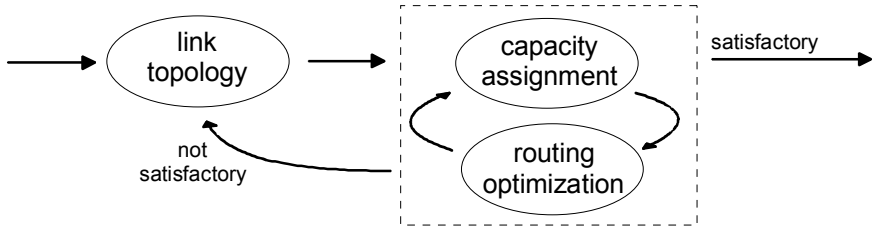
For the location of Servers it is important to know the amount of Traffic this server will generate. By means of appropriate location within the Network it is possible to avoid Bottlenecks in advance.

The location of the Routers is also a very important item, but practical experience shows that there are several restrictions. The location of external Routers is related to the location of the Boarder-Router of the Peering-Partner. The location of other Router Types is more or less predefined by already existing locations.

After positioning the links (mesh) between the Nodes have to be planned. At this point of time it is not possible to define the optimum Topology regarding the overall costs. The cost calculation is not possible until the dimensioning of the links is done (for which the Routing scheme is needed).

To optimize the routing it is necessary to have a specific Network Topology with known Link Capacities. It is understandable that the three part of the problem are associated, and non of them can be solved separately.

The strategy described below can be described with “divide and rule”. The overall problem is divided into parts. These parts of the problem will be handled alternating in autonomous steps (see figure below).



The following sections will describe the different steps in detail. As a last step the Server and Router has to be dimensioned regarding the expected load, to avoid Bottlenecks within the network.

1. Link-Capacity-Optimization

- ***Problem definition***

The figure below shows a specific definition of the Link-Capacity-Assignment problem. Starting point is a specific topology with a known Traffic Matrix and a defined Routing method. The overall link costs **D** shall be minimized, while it is not allowed to exceed the limit $\mathbf{T_{max}}$ for the average packet delay **T**.

The condition $\mathbf{T \le T_{max}}$ implicitly includes that the Bit Rates for the Links has to be lower than the particular Capacity.

• Given	Topology Traffic Matrix Routing-Method (Link-Flow-Vektor $f = (f_1, f_2, ..., f_b)$)
• Minimize Cost Funktion	$D = \sum_{i=1}^{b} d_i(C_i)$
• By means of assigning	$C = (C_1, C_2, ..., C_b)$
• Side Condition	$f \le C$ $T = \frac{1}{\gamma} \sum_{i=1}^{b} \frac{f_i}{C_i - f_i} \le T_{\max}$

The overall costs **D** consists of the capacity costs $\mathbf{d_i(C_i)}$ of all **b** Links, with $\mathbf{C_i}$ indicating the capacity of the Link **i** . To calculate the average End-to-End delay the Router will be modeled as M/M/1-Systems with Output-Queues. Furthermore it is expected, that the Links are independent from each other. The parameter $\mathbf{f_i}$ depicts the Average Bit-rate of Link **i**. The Bit-rates can be gathered from the Traffic Matrix and from the Routing Method. The Parameter γ characterizes the sum of all Traffic flows (packets per second) between all Pairs of Source/Destination.

• ***Solution Approach***

The proceeding to solve the problem of allocating capacities depends on what kind of cost function is available. If there is a linear context between costs and capacity $\mathbf{d_i(C_i) = d_iC_i + d_{i0}}$, the problem can be solved easily by means of the Lagrange Method. The optimum Link Capacity can be calculated with the following formula:

$$C_i = f_i + \frac{\sum_{j=1}^{b} \sqrt{d_j f_j}}{\gamma T_{max}} \sqrt{\frac{f_i}{d_i}} \quad .$$

For a concave cost function it is just possible to guarantee an optimal solution for specific cases. For discreet Capacities and therefore also for discreet Cost Functions we can choose between different approaches. One of the possible approaches is the "serial merge" algorithm which is based on dynamical programming. This algorithm is optimal for small, up to medium size networks. For large networks the preferred algorithm will be the proceeding developed by Greedy, which is based on the method of "Langrange Relaxation".

2. Optimization of Routing

• ***Problem definition***

The optimization of the routing shall minimize the End-to-End Delay by steering the Traffic Flows through the Network (between two End-Systems). It is possible to split the Traffic Flow by using different paths (Load Sharing).

• Given	Topology Link Capacity $\{C_i\}$ Traffic Matrix	
• Minimize Delay	$T = \frac{1}{\gamma} \sum_{i=1}^{b} f_i \left[\frac{1}{C_i - f_i} + \mu \, (P_i + K_i) \right]$	P_i *delay on Link i* K_i *processing timewithin node*
• By means of assigning	$f = (f_1 , f_2 , ..., f_b)$	
• Side Condition	a) f is Multicommodity Flow, according to Traffic Matrix b) $f \leq C$	

The figure above shows the mathematical representation of the routing problem. The meaning of the parameters **T, f_i** and **C_i** was still described in the chapter above. **P_i** is equivalent to the delay of the packets on Link **i**. **K_i** describes the time to process a packet within the node that represents the Endpoint of Link **i**. **$1/\mu$** is the average Packet-Length in Bits per Packet.

• ***Solution Approach***

The Routing optimization is a Convex Multicommodity Flow Problem with convex Side Conditions. There is a clear local minimum existing, also representing the global minimum. Therefore, the Routing Problem can be solved in a optimal way by means of the so called "Downhill Search" proceeding. There are different methods available. One of these methods is the Flow Deviation Algorithm. Based on a valid, but not yet optimized routing scheme, a redistribution of the Traffic from heavy loaded Links to less loaded Links is done. Goal of this redistribution is the minimization of the delay. If there is no more improvement regarding the

delay, the algorithm is stopped. The method presented by Gafni, Bertsekas and Gallager is also based on the redistribution of Traffic Load. However the chosen Method is more efficient, and leads to an improved behaviour regarding *convergence.*

3. Assigning Capacity and optimization of Routing

• Problem definition

Assigning of Capacity and optimization of Routing as described in the last two chapters are now observed as a related item. Starting from a Link-Topology the Routes and the Capacities has to be defined in a way to minimize the costs, and to stick with the side conditions regarding average packet delay.

• Given	Topology Traffic Matrix Cost-Capacity-Funktion $d_i\,(C_i)$
• Minimize Cost Function	$D = \sum_{i=1}^{b} d_i(C_i)$
• By means of assigning	f, C
• Side Conditions	a) f is Multicommodity Flow, according to Traffic Matrix b) $f \leq C$ c) $T = \frac{1}{\gamma}\sum_{i=1}^{b} \frac{f_i}{C_i - f_i} \leq T_{\max}$

• Solution Approach

Since there is no closed method to handle both problems simultaneous, it is advisable to solve the problems iterative. There are some algorithms that can be used:

- Minimum Link Assignment.

The Traffic Flows are routed through the network without considering the capacity. Therefore the shortest and least loaded paths are chosen. Afterwards the necessary capacity to fulfil the minimum requirement for the side conditions is defined. The next step is the optimization of the Routing with the aim to increase the overall throughput.

- Bottom Up Algorithm

As a starting point a minimum Capacity is assigned to each Link. Based on this, the Routing is optimized, with the aim to increase the overall throughput, while also following the Side Condition $\mathbf{T < T_{max}}$. If the value of the throughput fits with the requirements, the algorithm is stopped. Otherwise the most loaded Links will be exceeded and the optimization of the Routing will be continued.

- Top Down Algorithm

The maximum possible Capacity is assigned to each of the Links. Equal to the Botton Up Algorithm the Routing is optimized for maximum throughput. If the reached throughput exceeds the demanded value for the throughput, the Capacity for the Link with the lowest load will be decreased.

All the described Methods do not guarantee an optimal result. The determination of the optimum solution is difficult, because there are a number of existing local minimums.

4. Topology Planning

The Topology Planning includes the following tasks:

- Routing
- Capacity Assignment
- Link Selection

Based on this it is not possible to calculate optimal solutions for a network of a realistic size. All methods mentioned in the literary are based on heuristics. The following chapter describes two examples.

– Branch Exchange

The Branch Exchange Algorithm takes any Link-Topology which is valid regarding Connectivity as a base. The depending Capacities and the Routing will be determined based on this Topology. Afterwards the attempt is to optimize Costs and Packet Running Times by means of adding and removing of Links. The decision whether to add or remove a link is depending on the relating results regarding optimization. If it is possible to reduce costs for Capacity as well as the values for the Packet Delay, the Link will be added or removed. If there is an improvement just for one aspect, the advantageous aspect has to be compared with the handicaps.

Increasing the Packet Running Times might be possible in case the Packet Delay is still lower then the maximum value. On the other hand it might be necessary to improve the Packet Delay by increasing the Capacity Costs.

For the planning of large Networks the Branch Exchange Algorithms are just partially usable, because takes too long to calculate the network. To evaluate a possible change for a Link it is necessary to do a Capacity assignment and a Routing optimization. Another disadvantage of Branch Exchange Algorithms is the way they are scanning the area of possible solutions to identify the optimum solution. Since the starting point is a given Topology the scanning area for the optimum solution is just the surrounding of the given Topology. Therefore, the result of the search is strongly depending on the chosen Topology.

- MENTOR

The MENTOR Algorithm was developed by Kershenbaum, Kermani and Grover. In principle it is a heuristic with low complexity, and therefore relatively low running time. Goal of the method is to find a meshed, hierarchical structured Network with the following characteristics:

- The Traffic Flow is routed through the Network on relatively direct paths.
- The Traffic Load of each Links has to be meaningful. Heavy Traffic Load has to be avoided because of the increasing Packet Delay and the increasing Packet loss. Low Traffic Load also must be avoided because of the dropping cost efficiency.
- The single Link Capacities is chosen as big as possible to make use of the Cost Advantages of these Capacities.

The MENTOR Algorithm is composed from several parts (algorithms). The functionality of these algorithms is explained very briefly below:

- The first Algorithm specifies the emphasis of the network. All Nodes will be assessed regarding their Traffic Load, and afterwards the „Center of Mass"-Method will be done.

- The second Algorithm chooses the Backbone-Nodes, and assigns the remaining Nodes to one of these Backbone-Nodes.

- The „Center of Mass“ Algorithm will be executed again, just assessing the Backbone-Nodes. The resulting “Median” replaces the Emphasis Node of the first step.

- The next step is the creation of the hierarchy. A tree structure is assigned to the network, covering all Nodes. The solution procedure is a combination of Prim's „Minimum Spanning Tree“and Dijkstra's „Shortest Path Tree“Algorithm.

- The Tree Structure finally will be extended to a meshed structure.

The big advantage of the MENTOR Algorithm is the short time for the execution. Therefore it is possible to execute the Algorithm several times (if necessary) to select the best solution. Furthermore, it is possible to integrate the MENTOR Algorithm within an overall Algorithm.

C. GUIDELINE FOR THE DEFINITION OF A TRAFFIC MODEL

1.1 Traffic matrix.

Traffic characteristic analyze is the foundation work of the IP network design. It's one of the determinative factors for network topologic, layer structure, link capacity, and resiliency design. A useful method to represent the traffic characteristic in a mathematical formulation is the Traffic Matrix.

The Traffic Matrix provides a visual representation of the network traffic by specifying the traffic load between each pair of nodes using the vectors and matrix. For a network including x nodes: N1 ~ Nx, it's Traffic Matrix is defined as a N*N matrix T, with the elements tij at the i row and j column of the matrix to represent the traffic load from the node Ni destined to the node Nj.
For example, a network with the graph described in Figure C.1,

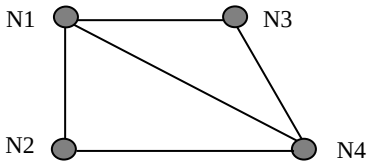


Figure C.1 Network Graph

Its Traffic Matrix is:

$$T = \begin{bmatrix} 0 & t_{12} & t_{13} & t_{14} \\ t_{21} & 0 & t_{23} & t_{24} \\ t_{31} & t_{32} & 0 & t_{34} \\ t_{41} & t_{42} & t_{43} & 0 \end{bmatrix}$$

In general, we can assume that the traffic matrix is symmetric, while tij = tji, for convenience. However, the traffic may be asymmetric in fact, because of the traffic containing point-point and well as multicast and broadcast traffic. And, the diagonal tij elements of the traffic are defined as zero since it does not require link capacity.

Traffic Matrix in Network Design

Link capacity matrix

Link capacity matrix describes the link capacity of a network with the mathematical formulation. It's defined as a matrix C, with the elements Cij at the i row and j column of the matrix to represent the capacity of the link < i , j > connecting the node Ni and the node Nj. If no connection exists between nodes, then the link capacity Cij=0. Moreover, we uses symmetric link capacities here, viz. Cij= Cji .
For the same network topology used in the previous examples, Figure C.1, the corresponding link capacity matrix can be defined as:

$$C = \begin{bmatrix} 0 & c_{12} & c_{13} & c_{14} \\ c_{21} & 0 & c_{23} & c_{24} \\ c_{31} & c_{32} & 0 & c_{34} \\ c_{41} & c_{42} & c_{43} & 0 \end{bmatrix}$$

Maximum-Flow, Minimum-Cut Set

According the link capacity matrix, the maximum flow allowed between two nodes can be calculated using the maximum-flow-minimum-cut theorem.. A i-j cut is a set of links, when they are removed completely from a connected network, the network will be divided into two separate parts, one containing node Ni and the other containing node Nj. The minimum i-j cut has the smallest sum of capacity values for the removed links, which defines the maximum flow between nodes Ni and Nj, marked as MFij.

For the example network in Figure C.1 and the given link capacity matrix above, Figure C.2 illustrates the minimum-cut-maximum-flow between nodes N1 and N4.

The minimum-cut-set includes the links <1,3>, <1,4>, and <2,4>. The sum capacity over the cut is 10+40+10=60. Therefore, the maximum traffic flow between nodes, N1 and N4 is 60.

However, the maximum-flow-minimum-cut only considers the community of a single pair of nodes, not the traffic between all nodes.

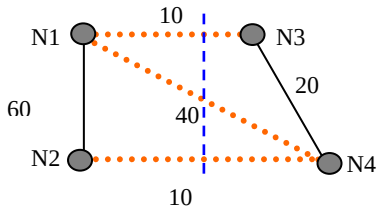


Figure C.2 Minimum-cut-maximum-flow MF_{14}

Link capacity constraints

Considering the traffic matrix defined early, the two basic constraints for link capacity design are:

For the every existing link < i , j > (Cij > 0), Cij must bigger than Tij and Tji, it's the per-link constraint.

For the every node Ni, ∑Cij (1≤j≤n) must bigger than ∑Tij (1≤j≤n) and ∑Tji (1≤j≤n),. it's the per-node constraint.

For the every pair nodes Ni and Nj, the minimum-cut-maximum-flow MFij must bigger than Tij. it's the per-pair constraint.

Minimum cost path Constraint

Further more, since the most IP MAN and WAN network run the OSPF or IS-IS as their IGP protocol, in most of cases there is only one active routing path for packet forwarding from one node to the other, although there are multi physical path between them actually. The OSPF or IS-IS protocol determines the minimum cost spanning tree rooted at each source node. The tree should carry the all traffic from the root node to others determined by the row of the traffic matrix T corresponding to the root node. Starting at the leaf nodes, the required link capacity is simply the traffic generated by root node N1 for that node. Moving backward toward the root node, the required link capacity includes the offered traffic for downstream leaf nodes in addition to traffic destined to intermediate branching nodes. The overall capacity required on each link direction is the sum of the required link capacities across the minimum cost spanning trees rooted at each node.

For the example networks with given link weights, the minimum-cost spanning tree for node N1 is illustrated in Figure C.3.

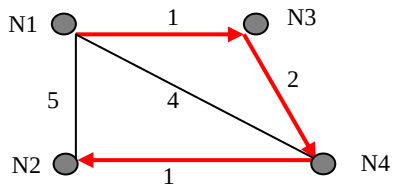


Figure C.3 Network with given links weights

Then the resulting link capacity requirement for the traffic originating from node N1 to all other nodes are:

C42 ≥T24 ;
C34 ≥ T24 + T34 ;
C13 ≥ T24 + T34+ T13 ;

However, when the routing paths for the all nodes are considered, things get more complex, because one single link <i,j> may belong to more than one spanning trees.

Furthermore, for the network running the OSPF/OSPF-TE or IS-IS/IS-IS-TE, there are may be multiple active forwarding paths for the traffic from one node to another, the traffic load can be balanced over these paths. In this case, the capacity constrains is more complex.

Beside these constrains, the network performance (i.e. the delay, Packet lost rate, and jitter either of the point-to-point link and end-to-end network) and network resource utility also should be considered. High network resource utility means heavy traffic load which results in increasing delay and packet loss rate , while high performance requires light load which means decreasing cost efficiency .

Single point Failure

Anther aspect related to traffic matrix should be considered in network design is network resilience. When the failure of one or more nodes or links occurs, network must have sufficient capacity still available to serve the offered traffic.

One commonly, the networks design should meet at least a N-1 reliability and resiliency requirement, it means that the networks is still have enough capacity to support the traffic load defined by traffic matrix under the condition of any single link or node failure.

Assuming that the network topologic design meets the N-1 reliability requirement, although it's difficult to achieve because the physical routing of every link is required to be completely diverse from the physical routing of every other link., and the link capacity design meet all above constrains without the failure. When any single link or node failure occurred, the routing table is recalculated, and the new forwarding paths are created. Then the rest network links should also meet above capacity constrains to guarantee the capability serving the load defined by traffic matrix under new paths.

Note: The traffic matrix itself is a kind of statistical description, it may not suitable for the situations such as traffic bursting.
The constraints we discussed here are also not suitable for the network with traffic engineering deployed.

D. REFERENCES

[1] CIGRE TB-153 '*The Use of IP Technology in the Power Utility Environment'*, WG35.07 April 2000.
[2] *'ATM Switching and IP Routing Integration'*. IEEE Communication Magazine, April 1998.
[3] *'Evolution of Multiprotocol Label Switching'.* IEEE Communication Magazine, May 1998.
[4] WG35.07, "*IP Cost Versus Risk Special Report*", Internal CIGRE SC35 report. August 2000.
[5] S. Kent and R. Atkinson. RFC 2401, "*Security Architecture for the Internet Protocol*". November 1998.
[6] R. Thayer, N. Doraswamy and R. Glenn. RFC 2411, "*IP Security Document Roadmap*". November 1998.
[7] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn and B. Palter. RFC 2661, " *Layer Two Tunneling Protocol L2TP*". August 1999.
[8] Eric C. Rosen, Arun Viswanathan and Ross Callon. "*Multiprotocol Label Switching Architecture*". July 2000.
[9] ATM Forum. "*LAN Emulation over ATM 1.0*". af-lane-0021.000, January 1995.
[10] S. Kent and R. Atkinson. RFC 2406, "IP *Encapsulating Security Payload (ESP)*". November 1998.
[11] Timo Kosonen. "*URTICA Network ConceptV1.4"*. ETRANS AG, Switzerland 2000.
[12] D. Awduche, J. Malcolm, M. O'Dell and J. McManus. RFC 2702, "Requirements *for Traffic Engineering Over MPLS*", September 1999.
[13] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao. "*A Framework for Traffic Engineering*". IETF Draft. May 2001
[14] G. Ash. "*Traffic Engineering&QoS Methods for IP, ATM, and TDM-based Multiservice Networks*". IETF Draft. March 2000.
[15] A. Feldmann and J. Rexford, " *IP Network Configuration for Traffic Engineering*". AT&T Labs Research. May 2000.
[16] L. Cheng, J. Ellson, and Y. Xu. "*A Framework for Internet Network Engineering*". IETF Draft. July 2001.
[17] Robert G. Gallager, "*Discrete Stochastic Processes*", Kluwer Academic Publishers, 1996.
[18] Marcel F. Neuts, "*Matrix-Geometric Solutions in Stochastic Models. An Algorithmic Approach*", Dover Publications, 1994.
[19] G. Latouche and V. Ramaswami, "*Introduction to Matrix Analytic Methods in Stochastic Modeling*", ASA-SIAM, 1999.
[20] Misha Schwartz, "*Telecommunication Networks: Protocols, Modeling, and Analysis*", Reading, MA: Addison-Wesley, 1987.
[21] Misha Schwartz, "*Broadband Integrated Networks*", Prentice Hall, 1996.
[22] Naohisa Ohta, "*Packet Video, Modeling and Signal Processing*", Artech House, 1994.
[23] Hiroshi Saito, "*Teletraffic Technologies in ATM Networks*", Artech House, 1994.
[24] A. Adas and Amarnath Mukherjee, "On resource Management and QoS Guarantees for Long Range Dependent Traffic", *Proceedings of INFOCOM'95*.
[25] W.E. Leland, M.S. Taqqu, W. Willinguer and D.V. Wilson, "On the self-similar nature of Ethernet traffic (extended version)", *IEEE Transactions on Networking*, February 1994.
[26] Kihong Park and Walter Willinger (Eds.), "*Self-Similar Network Traffic and Performance Evaluation*", John Wiley & Sons, August 2000.
[27] Cheng-Shang Chang, "*Performance Guarantees in Communication Networks*", Springer Verlag, 2000
[28] J.M. Pitts and J.A. Schormans, "*Introduction to ATM: Design and Performance*", John Wiley & Sons, 1996.
[29] S.Kent and R.Atkinson, RFC2401. "Security Architecture for the Internet Protocol" November 1998.