321

OPERATIONAL SERVICES USING IP VIRTUAL PRIVATE NETWORKS

Task Force
D2.10

June 2007

Operational Services using IP Virtual Private Networks

Task Force D2.10

Members		Corresponding members	
Jorge Fonseca	Portugal	Peter Cristaudo	Australia
Günter Endlich	Germany	Bernhard Gutmann	Germany
Anders Runesson	Sweden	Jan Piotrowski	Poland
Mehrdad Mesbah	France	Rodolfo Pellizzoni	Argentina
Daniel Gonzalez	Spain	Milena Matic	Yugoslavia
Enrique Garcia	Spain	Claudio Trigo	Brazil
Hermann Spiess	Switzerland	Hironaga Yamazaki	Japan
Carlos Samitier *(Convener)*	Spain	Stuart Mann	UK
		Fernando Gonzalo	Spain
William Caffrey *(Secretary)*	Ireland	Maurizio Monti	France
		Mirjana Stojanovic	Serbia
		Wan Azlan	Malaysia
		Allan Riesz	Australia

ISBN : N° 978-2-85873-012-4

TABLE OF CONTENTS

1 INTRODUCTION

VPN is a technology that connects two or more separate sites over private or public multiservice infrastructure, and allows different connections to work as if they were a single private network. The software of VPN guarantees that although packets transport across the network, the contents remain private.

A VPN can be defined as the emulation of a Wide Area Network using an IP infrastructure, which includes from a simple point-to-point link to a complex IP infrastructure integrating multiple services.

The integration of corporate and operational services is one of the issues of most concern for Power Utilities nowadays. VPN is one of the technologies that would enable this integration. The use of extra bandwidth capacity and the allocation of other services with service isolation guarantees is another motivation to deploy a VPN.

One of the major concerns of multiservice integration is the lack of privacy and service separation. If a company's network comprises multiple sites, the contents of the traffic transported between the sites can be at risk from external parties if it passes through network elements owned by other companies. Layered architecture can distinguish between different internal traffic as well as external traffic. The goal is to keep internal traffic private while still allowing external communication.

A complete isolation from the global internet is not always desirable for various reasons (cost, accessibility, etc). Many companies choose a network with a hybrid architecture which combines the strengths of a private network with its advantages of the connections to the global internet.

There are a number of different techniques that can be employed in order to implement a VPN, such as tunnelling or encryption. VPN uses the idea of defining a tunnel across the IP-network between routers in each side, and use encapsulation to forward traffic across the tunnel. To guarantee privacy a VPN encrypts each outgoing data packets before the encapsulation. These are discussed in chapter 3.

2 VPN SURVEY

To get an overview of the present use of IP-VPNs for Power Systems operational applications, TF D2-10 conducted a survey of CIGRE members.

2.1 BACKGROUND TO THE QUESTIONNAIRE

The SC D2 has commissioned the TF D2.10 to study the provision of operational services using IP Virtual Private Networks.

The survey has been carried out with the collaboration of the Task Force and D2 committee members. The survey sought to answer who is using VPNs, for which services, how they have implemented it, what business benefits they are

getting, and for those who have not, why not? And whether they are planning to?

In addition, the goal of this questionnaire was to obtain first hand information about the key issues related with VPN as well as the expectations of existing and potential users.

There were 23 responses from the following continents:

Algeria(1)	Japan (7)
Argentina (2)	Poland (1)
Australia (1)	Malaysia (1)
Belgium(1)	New Zealand (1)
Brazil (3)	Saudi Arabia (1)
Canada (1)	Spain (1)
Finland (1)	Switzerland (1)
Ireland (1)	

A primary assumption was that all respondents have an IP network for at least their corporate traffic.

The operational applications considered were:

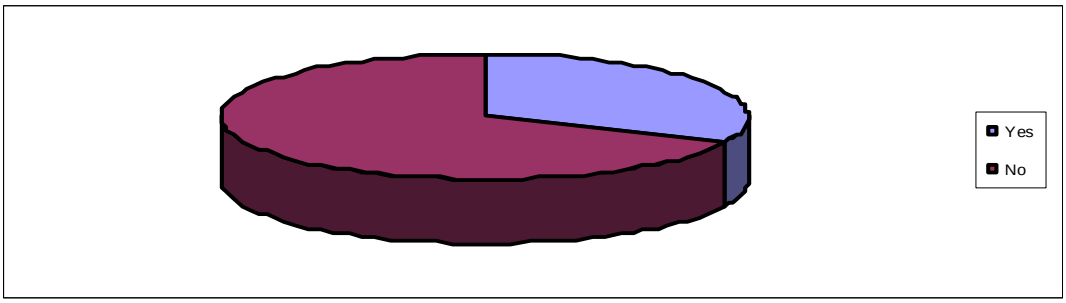
- SCADA/EMS
- Inter Control Centre Communications
- Station Alarm Systems
- Operational Telephony
- Equipment Management (Device Settings and monitoring of equipment)
- Workforce Management
- Energy Market
- Management of telecommunications systems
- Facilitating Outsourced service providers

The questionnaire used for the survey can be found in appendix A.

2.2 RESULTS & CONCLUSIONS OF THE QUESTIONNAIRE

The following are the main findings and key conclusions.

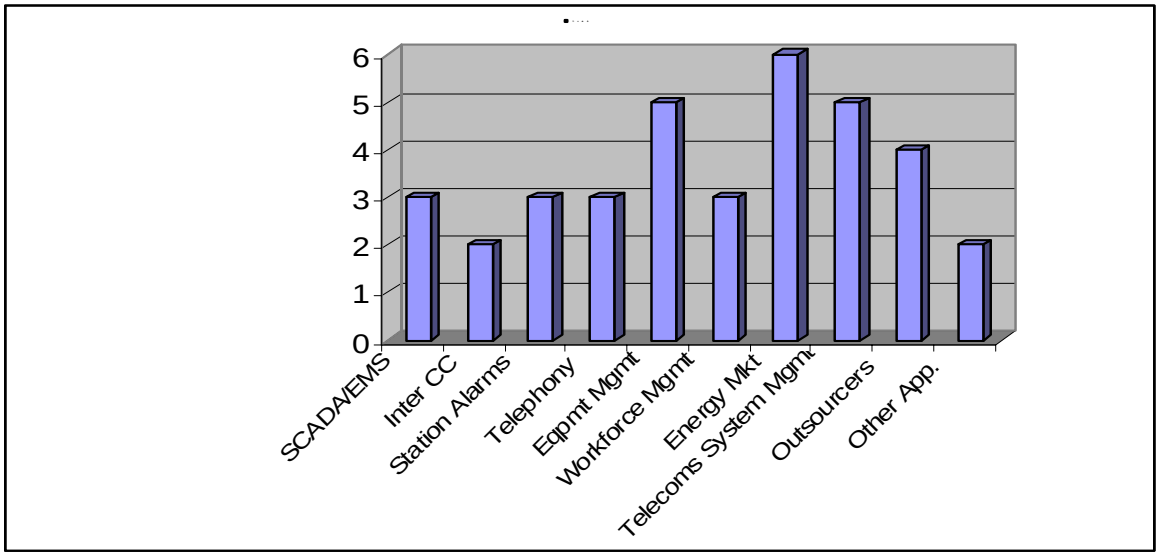
Q1: Are you using IP-VPN for operational applications at present?



Survey Response	Comments & Conclusions
Seven (7) companies confirmed that they are using IP-VPNs for operational applications	*This was considered high given that it is a new technology.*

Q2-11: What type of applications used IP-VPNs?

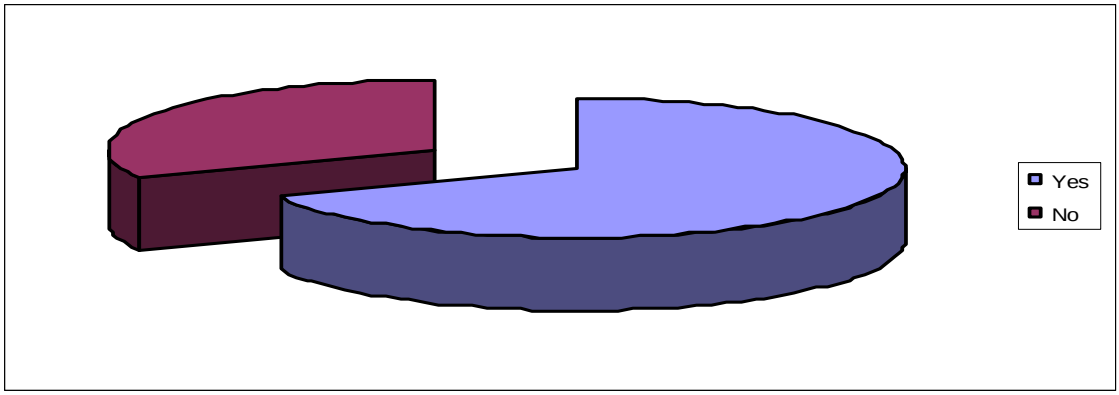
This set of questions determined the types of operational applications using IP-VPNs. Of this seven (7) the breakdown was:



Survey Response	Comments & Conclusions
(3) are using it for SCADA/EMS purposes	*(i) There is a considerable mix of applications involved.*

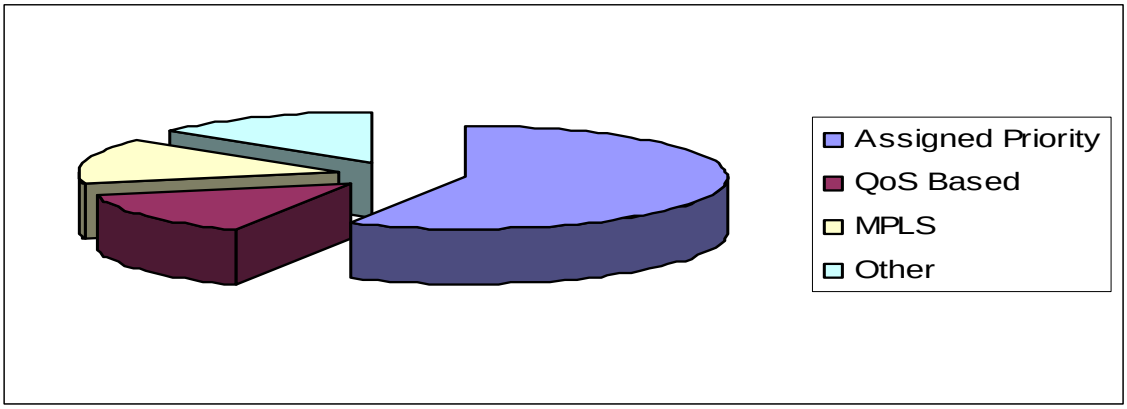
(1) are using it for Inter control Centre communications (2) are using it for Station Alarm Systems (3) are using it for operational telephony (4) are using it for equipment management (3) are using it for workforce management (4) are using it for energy market communications (4) are using it for telecommunications system management (4) are using it for outsourcers (2) apply to other non-specified areas	*(ii) Of the applications listed, there are very few critical ones using IP-VPNs.* *(iii) Those companies using IP-VPNs for SCADA, use it for medium voltage networks.*

Q12: Do you have separate IP networks for Corporate and Operational services?



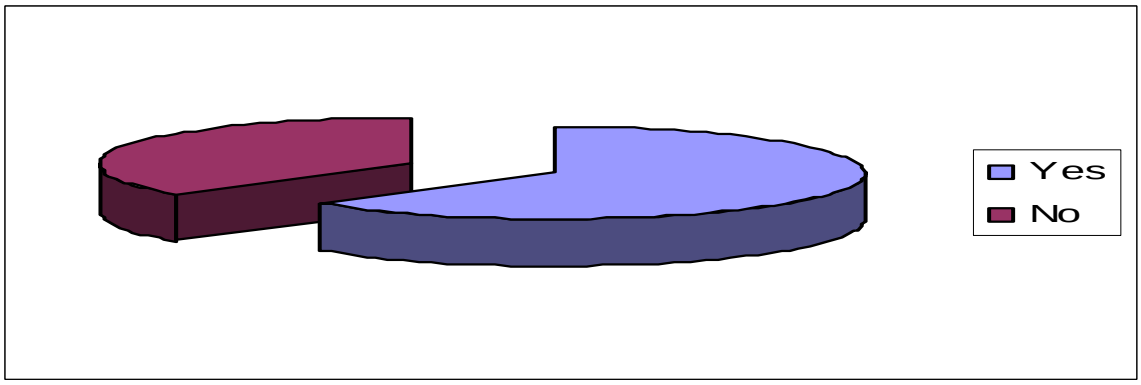
Survey Response	Comments & Conclusions
Yes:15 No:7	*The majority use separate IP networks*

Q13: How do you separate the provision of different services over the IP Network?



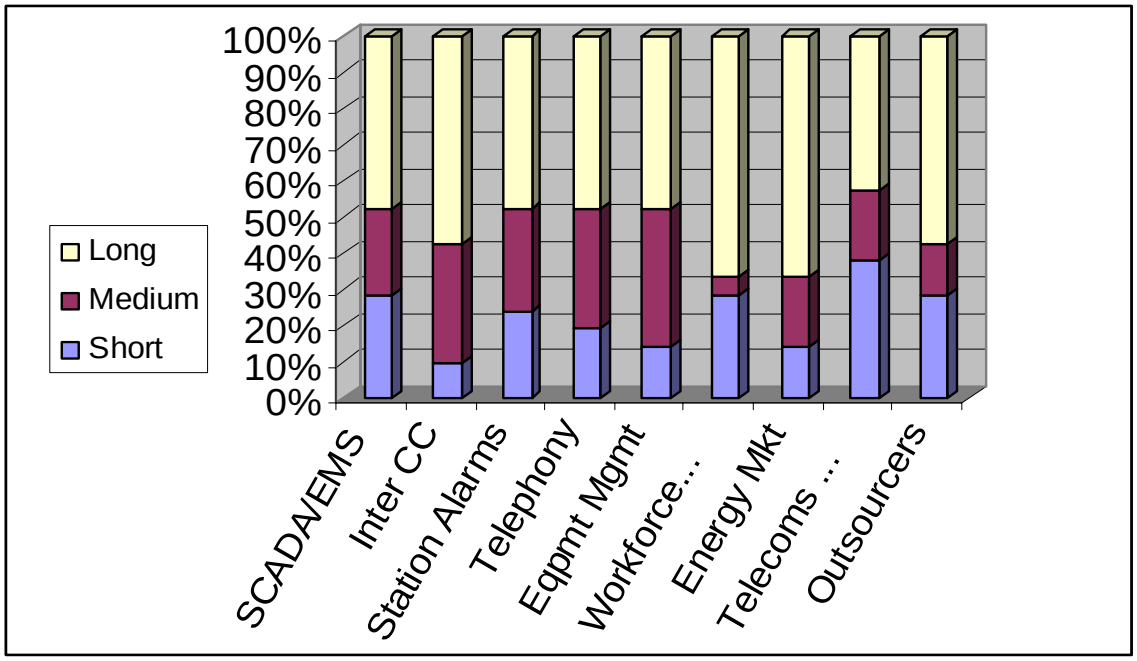
Survey Response	Comments & Conclusions
Assigned Priority: 12 QoS Based System: 3 MPLS Implementation: 4 Other: 2	*The majority uses some form of Priority Assigned system for segregating the different services.*

Q14: Are you planning to use IP-VPNs in the future?



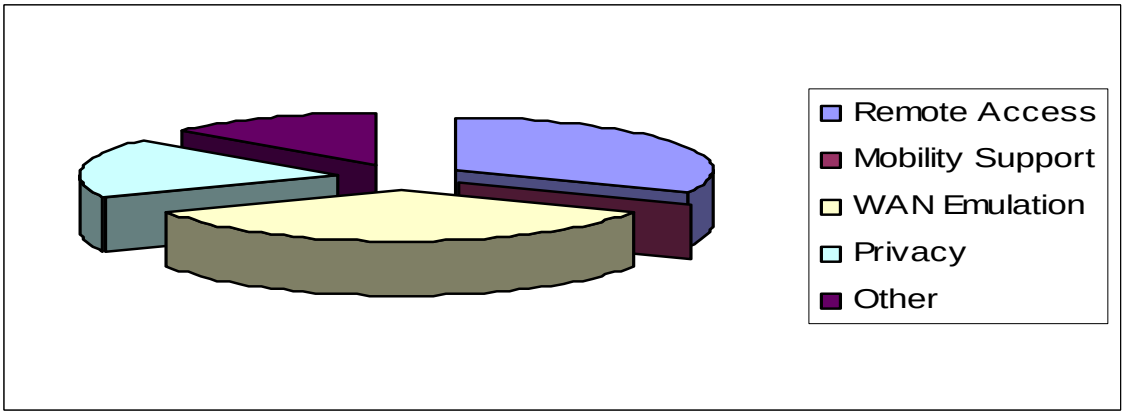
Survey Response	Comments & Conclusions
	The majority of those that are presently not using IP-VPN for operational applications have plans to use it in the future.

Q15-23: What types of operational applications are you planning to apply to IP_VPNs?



Survey Response	Comments & Conclusions
	(i)Of those companies either presently or planning to use IP-VPNs, the majority have plans to use IP-VPNs for operational purposes in the short to medium term.

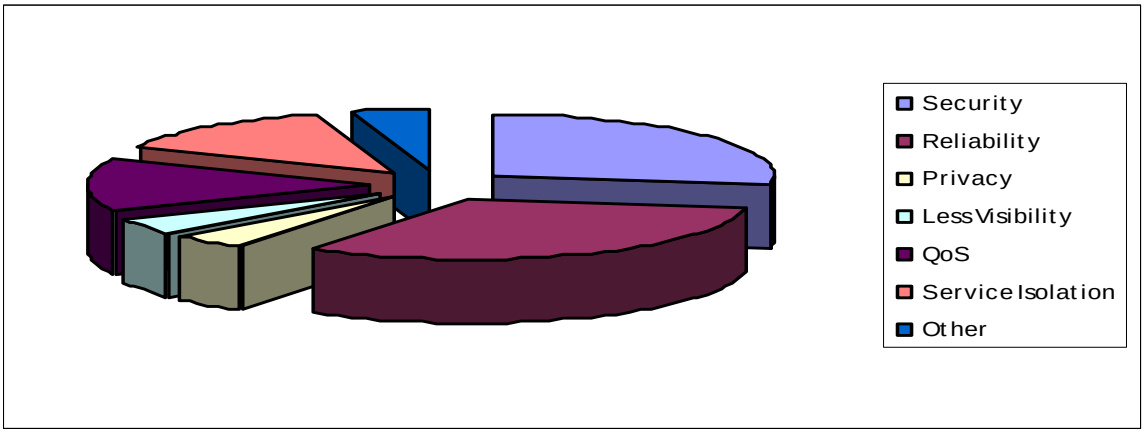
Q25: What is the present purpose of VPNs?



Survey Response	Comments & Conclusions
	(i) The present purpose of using IP-VPNs is primarily 'WAN Emulation' or

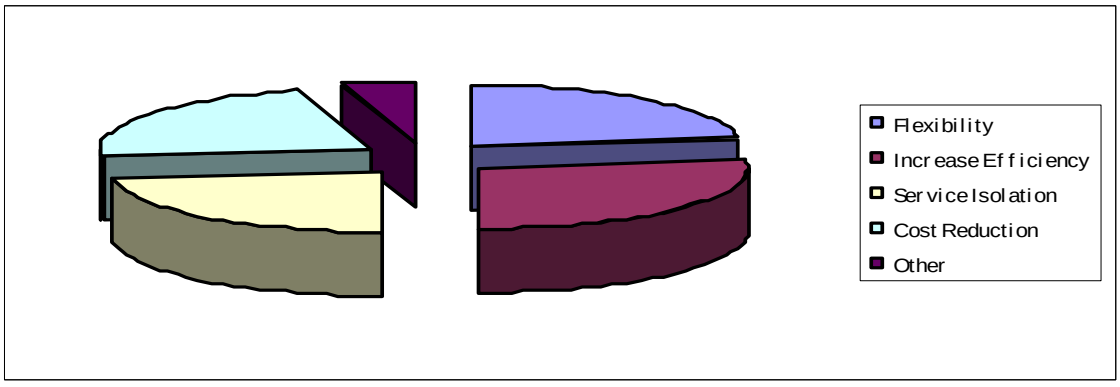
	'Remote Access', for both corporate and operational purposes. *(ii) Q26 dealt with the Future purposes of VPNs and the responses were practically the same.*

Q27: What are the main concerns with using VPNs?



Survey Response	Comments & Conclusions
	(i) The major concerns associated with using VPNs are Reliability and Security. *(ii) It was not clear if these were concerns with IP and/or VPNs*

Q28: What are the expected benefits of using VPNs?



Survey Response	Comments & Conclusions
	The expected benefits of implementing IP-VPNs are equally: flexibility, increased efficiency, isolation of services, and cost reduction.

2.3 General Analysis and Conclusions

The responses to Q1 *(Are you using IP-VPN for operational applications at present?)* AND Q12 *(Do you have separate IP networks for Corporate and Operational services?),* could be interpreted as follows:

(1) There are some companies that do not use IP networks for Operational services.
(2) There are some companies that do use IP Networks for Operational services and Corporate services but they are separate IP Networks.
(3) Similar to (2), some companies that do use separate IP Networks for Operational services and Corporate services, use VPNs within each network to provide discrete services.
(4) And there are relatively few that use the same IP network to provide both Operational and Corporate services and use some form of VPN to separate the services.

(1) No IP Networks for Operational services at present. - Algeria - Argentina(2) - Australia	(2) Separate IP Networks for Operational and Corporate services: - Canada - Japan (6) - Brazil (1) - Malaysia - Spain
(3) Separate IP Networks for Operational and Corporate services, but with VPN used for different services: - Belgium - Poland - Finland - Brazil (1) - Japan (1)	(4) Separate Operational and Corporate services through use of VPN. - New Zealand - Ireland - Saudi Arabia

One obvious conclusion is that there are different implementations and approaches.

In addition, the responses to Q1 *(Are you using IP-VPN for operational applications at present?)* AND Q12 *(Do you have separate IP networks for Corporate and Operational services?)* combined with Q14 *(Are you planning to use IP-VPNs in the future?)* indicates that there are some companies that are not and have no plans to use IP-VPNs for Operational services.

3 IMPLEMENTATION OF VPN

3.1 Key concepts in VPN provision

VPN is a generic term that may be used to determine different networking solutions. VPNs can be classified according to three different concepts:
- The working principle. That is to say, how VPN is established and implemented.
- The layer which supports the VPN
- How VPN is operated. In this case, the main factor to be considered is who controls the establishment, maintenance & management of VPN.

When the working principle is considered, four main possibilities for VPN implementation are:

- Virtual Leased Line. A VPN implemented as a virtual leased line consist of a virtual point-to-point link that connects two access points.
- Virtual Private Routed Network. A VPN implemented as virtual private routed network is the emulation of an IP WAN. It connects number of IP access points providing IP service and full connectivity as in a real IP network.
- Virtual Private Dial Network. In a virtual private dial network, connections are only established on demand. It is used to connect pairs of terminals (Dial-up modems and point-to point access links).
- Virtual Private LAN Segment. A virtual private LAN segment provides Ethernet service and connectivity in a number of locations connected by a WAN. All the Ethernet access points of the virtual private LAN segment become a single Ethernet segment which offers full Ethernet functionality as in real LANs except the propagation delay between access which depends on the geographical extension and the implementation of the WAN that supports the emulated segment.

When considering the network layer that implements the VPN, it can be distinguished two possibilities:
- Layer 2 VPN. It is a VPN implemented at the link layer and provides Ethernet functionality as previously discussed. This type of VPNs provides protocol transparency but has a limited scalability. In fact, it is an emulation of a distributed Ethernet LAN.
- Layer 3 VPN. It is a routable IP network emulation providing IP services as previously discussed.

If the operation of the service is taken into account, VPNs can be classified into two types:

- *Customer controlled VPN*. In this case, the core network is not aware of existence of the VPN. This scheme provides address isolation and security so it is normally used for remote access to the corporate IP WAN.

- *Service provider controlled VPN*. In this case, the service provider fully controls and manages the VPN. The customer has no control on the performance and working principle of the VPN provided. The definition of a well-defined SLA is strongly recommended.

3.2 VPN components

Since a VPN is the emulation of a WAN, there is a parallelism between the components of both WAN and VPN. As any network, a VPN is formed by links, switching nodes and access points. In this particular case, the links are tunnels, the switching nodes are virtual routers and the access points are the physical interfaces where VPN users are connected.

A tunnel is a transport mechanism that allows IP packets to cross IP networks in such a way that the user is not aware of the IP network characteristics as routing, addressing, etc. Although it provides a virtual point-to-point connection, this does not imply that the packets crossing the tunnel should follow a fixed path. It only defines the egress port of the IP WAN where the packet will be delivered.

There are different mechanisms to support IP tunnelling. The most commonly used include:

- IP/IP Basic encapsulation based on the RFC 2003.
- Generic Routing Encapsulation (GRE) based on the RFC 2784.
- Layer 2 Tunnelling Protocol (L2TP) based on the RFC 2661.
- IPSec based on the RFC 2401.
- Multiprotocol Label Switching (MPLS) based on RFC 3031 and other related RFCs.

The virtual router functionality can be implemented by a specific function allocated in a single router anywhere in the core IP WAN. In this approach, the virtual router implements a virtual IP network with star topology with the virtual router being the central switching node.

A virtual router may also be implemented as a distributed function implemented in a number of node of the core IP WAN. This solution requires specific overlaid routing mechanism that may interact with the routing procedures of the core IP WAN.

3.3 VPN requirements

The main requirements that have to be fulfilled by a VPN are opaque transport, data security, and QoS support.

The transport service provided by a VPN has to be unrelated with the core IP WAN which supports the VPN. This implies that both addressing schemes and routing procedures have to be unrelated. This is normally achieved by using tunnelling techniques as explained in previous chapter.

The security of a VPN can be implemented by the customer or by the service provider. In the first case, the customer has to install firewalls and deploy secure tunnels. In the second case, service provider has to define the degree of security and how it is manage and maintained.

The provision of QoS guarantees by a VPN is strongly related with the implementation of the core IP WAN that supports the VPN and its capabilities to provide QoS. In general, when standard IP WAN network is used to provide VPN service, the QoS aspects such as bandwidth and delay cannot be guaranteed. It can be shown that the QoS performance of a VPN will always be worse than the QoS of the core IP WAN that supports the VPN.

Other QoS aspects, such as availability, depend on the degree of redundancy and the resiliency of the underlying layers. This resiliency can be achieved by different methods:

- Using SDH rings with spare bandwidth.
- Using MPLS backbones with extra capacity in the routes that connects the sites involved in the VPN.
- Using constrained routing in the IP layer. This requires and IP WAN designed with enough capacity in the routes that connects VPN sites.
- Any combination of the above-mentioned alternatives.

3.4 Provision of operational services

The provision of operational services using VPNs presents advantages and disadvantages the most relevant being:

Advantages

- Service isolation allows corporate network to be used by operational service and vice versa.

Disadvantages

- QoS guarantees are not provided by VPN implemented over a plain IP WAN. MPLS is required which may imply an extra cost.
- WAN-VPN interactions. WAN traffic and congestion control mechanisms may not be aware neither have any control on the traffic carried by the VPN. This may impact the performance if not considered in the WAN design phase.

Consequently, service isolation requires not only addressing and security but also traffic engineering and congestion control isolation mechanisms to really guarantee no interactions between services.

The above-mentioned disadvantages can be diminished by using a MPLS core. MPLS also provides traffic-engineering mechanisms that efficiently isolate different services. The need for a MPLS core is not a drawback since most of the WAN integrating services are already based on this type of backbones. The working principles and implementation of MPLS backbone is out of the scope of this document.

4 CONCLUSIONS

Service integration allows network resources to be optimised. Nevertheless, mechanisms to provide service isolation have to be provided. VPNs provide service integration in a secure and isolated environment. Because of this, there is a growing interest in using VPN solutions in the future. Although present VPN applications are focused on a limited range of applications such as mobility, WAN emulation, privacy and security improvement; the survey shows that in the medium term VPN will be used to support every type of control applications.

VPN is a new functionality of the basic IP protocol suite that opens a number of very interesting applications and opportunities to enhance the functionality of existing IP infrastructures.

The large number of possibilities offered by VPNs has driven the TFD2.10 to direct a survey to find out the most relevant applications in the Power Utility environment. This may be implemented within the utility's own infrastructure or through a service provider's network or a mixture of both.

The new capabilities opened by VPNs may be of great interest in the support and deployment of operational services. In fact, the survey shows that the use of VPNs for operational service provision is emerging. Management and maintenance are going to be the first services supported.

The reliability and performance of a VPN depends on the characteristics of the underlying infrastructure, such as restoration time, latency, disaster recovery requirements, standby power capability, etc, and not only on the technology employed to implement the VPN service.

The implementation of critical real-time operational services using VPNs requires a proper WAN/VPN design. Technologies such as MPLS or VPLS are the most common approaches to the deployment of VPN that provides QoS guarantees.

Appendix A – Case Studies

1. European Grid Company VPN built during 2005-06

Case Study Company A – An Electric Utility in Northern Europe

IP WAN/LAN Network

1. INTRODUCTION

The utility owns an exclusive fibre network built in the power lines. Transmission equipment for STM-1 or STM-4 is installed between most substations. The fibre network totally contains more than 8000 km and 150 nodes all over the country.

The high demand for higher capacity for different Ethernet/IP services from users have made it necessary to implement a WAN/LAN to all substations with fibre network. In 2005, the company implemented a trial network with 50 substations. In late 2006, another 90 stations will be implemented in the network.
Examples of services which will be provided in the network:

- IP Telephony for operational use
- Monitoring power network
- Video and security system in substations and power stations
- SCADA (some services)
- Corporate services

2. NETWORK ARCHITECTURE

The WAN/LAN will use the SDH network as bearer. The WAN/LAN network is divided in core and access levels. For the core there are four nodes and access routers installed on 50 sites. Late 2006 the network will be extended with some more core nodes and 90 new Access Routers. Afterwards it is planned to connect the remaining substations when fibre network will be installed. Totally, the utility has connections to more than 200 substations.

In the core network, all nodes are connected to each other in a ring structure. All access nodes are connected with separate connection to two core routers. Connections between access node and core node is established with minimum 1 + 1 E1 (2 Mb/s) connection. Access nodes are in mostly cascaded from 2 nodes up to maximum 5 nodes.

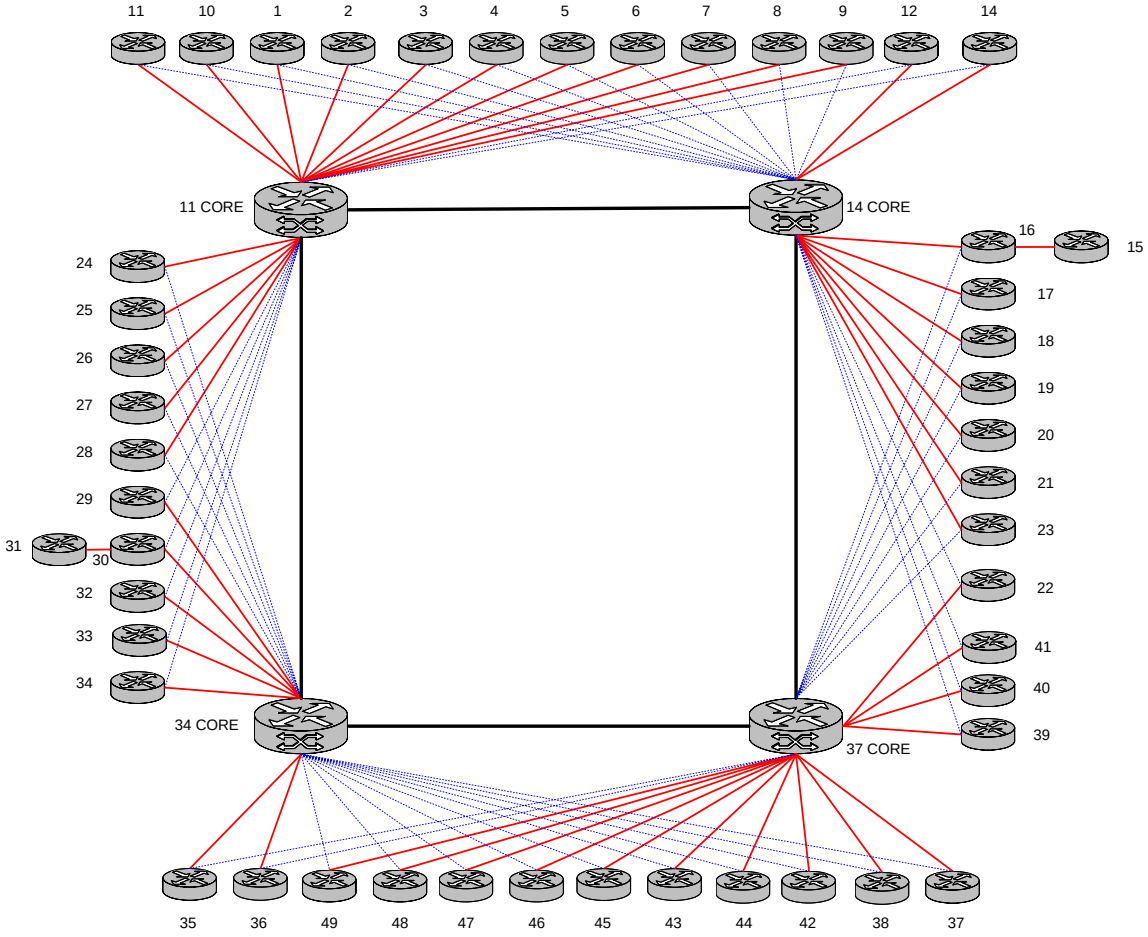


Figure 1 – Logical view of IP WAN Network

3. VPN SERVICE

All VPN services will be controlled by the IT department of the utility. Presently, one type of VPN is offered at access layer, VPN with IP addresses provided by the IT department. Depending on services and customer demand in the future additional services will be available.

4. SECURITY

In the substations, all connections of the IP WAN Networks are using firewalls. Different types of traffic is separated at access level using V-LANs
The network is using SNMP 3 for configuration and supervision. SNMP 3 is much safer than earlier versions.

2. MPLS VPN Network

Case Study Company B - An Electric Utility in the Gulf Region

The following are the various users/applications of the MPLS VPN network of an electric utility in the Gulf Region:

- Power Systems Monitoring and Control
    - Inter Control Centre communication, which is the ICCP traffic between different Control Centres.
    - Dynamic System Monitor (DSM): Communication of DSM RTU (s) located at various substations with the DSM Server located at a central point over MPLS VPN.
    - Transient Fault Recorder System (TFR): Communication of Transient Fault Recorders located at various substations with TFR Server located at a central point over MPLS VPN. This system acts as an analyzer of power system faults and the TFR (s) are used to record these faults. The recorded data from the fault recorders is transmitted to the Server through the VPN.
    - Communication of RTU (s) at various substations & power plants with the centrally located Master Station using IEC-60870-5-104 Protocol.
    - In future, Communication of SCADA RTU (s) at various substations & power plants with the Energy Management System Master Station using IEC-60870-5-104 SCADA protocol for Power Systems Monitoring and Control.
    - Substation Automation traffic in future
- Administrative
    - Administrative/Normal users working on various applications (both real-time & non real-time traffic) such internet/intranet/email/mainframe and video conferencing.
- Network Systems Operations & Monitoring
    - Medium Density Fibre Optics Terminal Equipment (MDFOTE) Network Management System (NMS) access over MPLS VPN, with the Network Management Server at a central location (Telecommunications Network Control Centre) and the MDFOTE at various Substations/local offices.

- Extension of MDFOTE urgent and non-urgent alarms plus the substation housekeeping alarms to Network Management Supervisory (Protek, which is under implementation) at a central location (Telecommunications Network Control Centre) over MPLS VPN using RTUs (IMCI) at various substations.

- Communication of a centrally located PABX NMS (Optivity Telephony Manager) with the PABX at various Power Plants and substations over MPLS VPN.

- Security and Surveillance
  - Communication of security devices/systems such as card readers, door monitoring sensors, cameras etc installed at remote substations and/or power plants with centrally located control servers and monitoring workstations over MPLS VPN.

3. IP WAN Substations Network

Case Study Company C - An Electric Utility in Southern Europe

1. INTRODUCTION

Company C is a Transmission System Operator (TSO) responsible for the electricity transmission in its country, and situated in the southern Europe.

The evolution of energy system controllers and the business continuity made heavy pressure to the existing telecommunication network forcing its evolution in order to spread broadband communication services to all points of presence and the introduction of the Ethernet/IP technology.

For this purpose the utility is implementing an Ethernet/IP network with the objective of providing interconnection services for industrial operations in the substations.

The services that will be provided in the starting phase are:

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

2. NETWORK ARCHITECTURE

The Ethernet/IP network is divided in core and access levels. The core level is composed by seven nodes with routing and switching equipment. The access level is present at twenty sites (~30% of high voltage utility substations), with switching equipment. Afterwards is planned to extend the access to the remaining substations having in account that the core is already prepared for this evolution.

The core network has two main nodes (A and B) connected to each other and where all others core nodes are connected, as shown in Figure 1. The connections between the nodes are established in GbE links by internal transmission platforms.

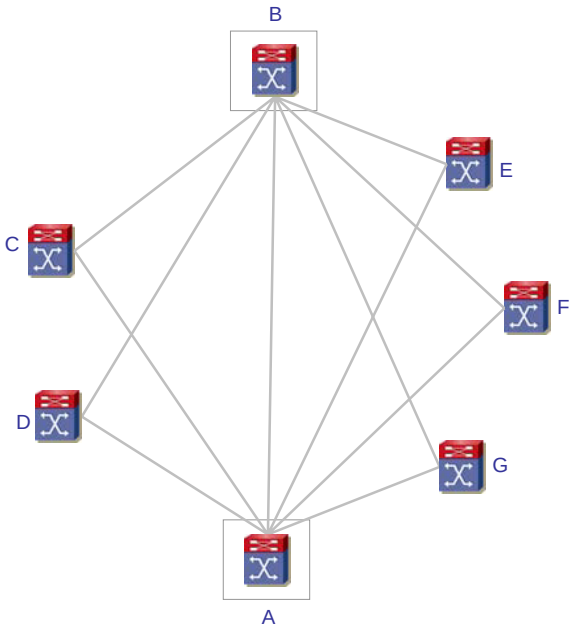


Figure 1 – Core Network

The access network is composed by twenty nodes connected to two core nodes, as shown in Figure 2. The connections between access and core nodes are established in dedicated point-to-point Fast Ethernet links also provided by internal transmission networks.

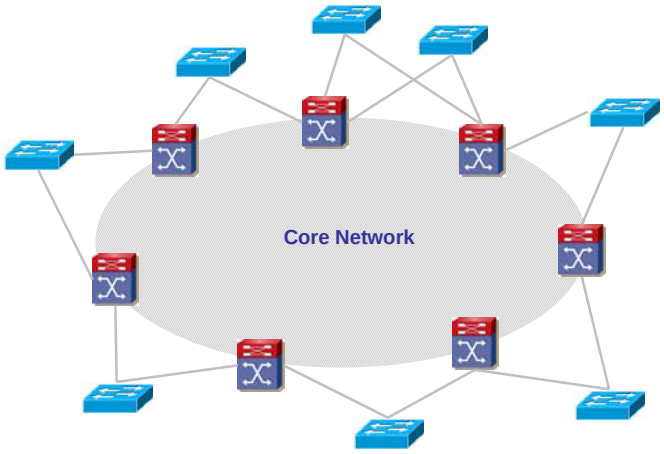


Figure 2 – Access Network

In the Figure above is represented only some access sites each connected to two different core sites in order to increase network reliability.

The main characteristics of this network are:

- The core runs IP/MPLS providing Layer 3 VPN MPLS services;
- The access layer established in this phase is dedicated to the electrical transmission substation services using Layer 2 VLAN;

- The different services are supported by dedicated VPN MPLS in the core and by VLAN in the access level to provide the required traffic isolation;
- The access layer equipment is adapted to the harsh substation environment by using special switches in strategic points.

3. VPN SERVICE

The VPNs are totally controlled by the utility Telecommunication Department and offers an opaque transport, data security isolation and QoS support. There are two main type of VPNs offered at the access layer:

- VPNs with IP addresses provided by Telecommunication Department – centralized IP address management;
- VPNs with IP addresses provided by final client and invisible to the network and other clients – IP address planning and management are client responsibility.

4. SECURITY

The corporate IP network and the IP WAN Substations Network are connected trough a link using firewalls and others security devices in one main site, to allow some traffic to flow between the networks.

The separation between the different types of services at access level is done using VLANs, when IP traffic reach the core is inserted into a VPN MPLS, Figure 3.
In all sites where each service is present a VPN MPLS provides the necessary connections among them. If VPN routing is necessary this is done in one dedicated firewall.

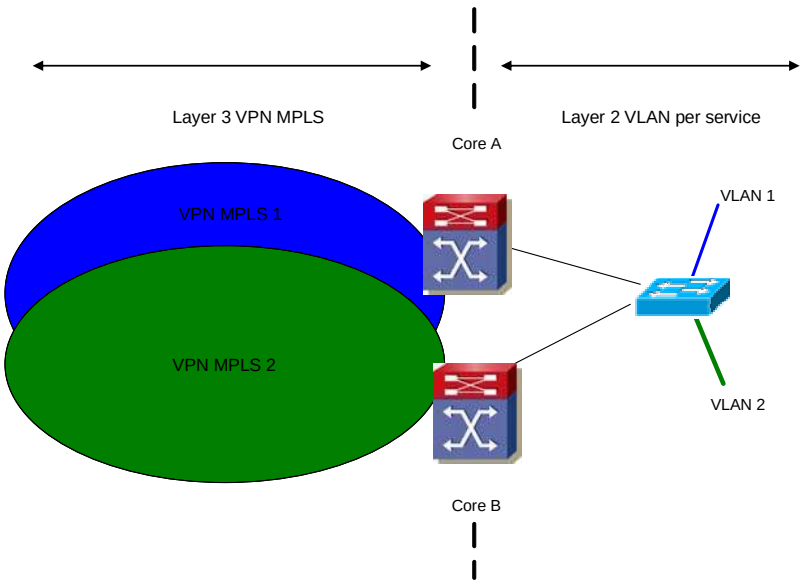


Figure 3 – VPN provisioning

Future services, of other kind, will be connected to the core through dedicated routers. In the core is then defined a new VPN MPLS for those new services.

5. COMPLEMENTARY SERVICES

This network has its own centralised management system with the capability of total control and surveillance of the equipments. Additionally it was integrated with the utility's Openview system to support utility helpdesk service in the monitoring of the network alarms and providing user support.

Appendix B – Survey Questionnaire

1. Are you using IP-VPN for operational applications (Y/N) (If yes, check all that apply)
    a. SCADA /EMS
    b. Inter Control Centre communications
    c. Station Alarm system
    d. Telephony
    e. Equipment management (device settings and monitoring)
    f. Workforce management
    g. Energy market (Market agents communication)
    h. Management of Telecommunication systems
    i. Outsourcing support (Communications needed by outsourced service provider)
    j. Other – please specify

2. Do you have separate IP networks for Corporate and Operational services (Y/N)

3. How do you separate the provision of different services over your IP Networks?
    a. Assigned priority system
    b. QoS based system
    c. Implementation of MPLS
    d. Other – please specify

4. Are you planning to use IP-VPN (Y/N) (If yes, check all that apply)

	SHORT TERM	MEDIUM TERM	LONG TERM
SCADA/EMS			
Inter Control Centre communications			
Station Alarm system			
Telephony			
Equipment management (device settings and monitoring)			
Workforce management			
Energy market			
Management of Telecommunication systems			
Outsourcing support			
Other - please specify			

5. Present purpose of VPN
    a. Remote access
    b. Mobility support
    c. WAN emulation
    d. Privacy
    e. Other - please specify

6. Future purpose of VPN
    a. Remote access
    b. Mobility support
    c. WAN emulation
    d. Privacy
    e. Other - please specify

7. Concerns using VPNs
    a. Security
    b. Reliability
    c. Privacy
    d. Less visibility
    e. QoS
    f. Service isolation
    g. Other – please specify

8. Expected benefits of VPNs
    a. Flexibility
    b. Increased efficiency of network resources
    c. Service isolation
    d. Cost reduction
    e. Other - please specify

List of Standards

The following is from the Virtual Private Network Consortium (http://www.vpnc.org/vpn-standards.html)

For **secure VPNs**, the technologies that VPNC supports are

- IPsec with encryption
- L2TP inside of IPsec
- SSL with encryption

For **trusted VPNs**, the technologies that VPNC supports are:

- MPLS with constrained distribution of routing information through BGP ("layer 3 VPNs")
- Transport of layer 2 frames over MPLS ("layer 2 VPNs")

The relevant IETF Working Groups for the protocols used by secure VPNs and trusted VPNs are:

- Profiling Use of PKI in IPsec Working Group
- IKEv2 Mobility and Multihoming Working Group
- Transport Layer Security Working Group
- Layer 2 Virtual Private Networks (l2vpn) Working Group
- Layer 3 Virtual Private Networks (l2vpn) Working Group
- Pseudo Wire Emulation Edge to Edge (pwe3) Working Group

Note that the IPsec Working Group was disbanded in April, 2005.

The documents are arranged by the general categories they apply to. These categories are:

For secure VPNs:

- General IPsec
- ESP and AH (encryption and authentication headers)
- Key exchange (ISAKMP, IKE, and others)
- Cryptographic algorithms
- IPsec policy handling
- Remote access
- SSL and TLS

For trusted VPNs:

- General MPLS
- MPLS constrained by BGP routing
- Transport of layer 2 frames over MPLS
- Virtual routers

4.1 General IPsec

RFC 4301	Security Architecture for the Internet Protocol	Proposed standard
RFC 3554	On the Use of SCTP with IPsec	Proposed standard
RFC 3723	Securing Block Storage Protocols over IP	Proposed standard
RFC 3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	Proposed standard

4.2 ESP and AH Headers

RFC 4302	IP Authentication Header	Proposed standard
RFC 4303	Encapsulating Security Payload (ESP)	Proposed standard
RFC 4304	Extended Sequence Number Addendum to IPsec DOI for ISAKMP	Proposed standard
RFC 4305	Cryptographic Algorithm Implementation Requirements For ESP And AH	Proposed standard

4.3 Key Exchange

RFC 4306	Internet Key Exchange (IKEv2) Protocol	Proposed standard, being updated by draft-hoffman-ikev2-1
RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	Proposed standard
RFC 4308	Cryptographic Suites for IPsec	Proposed standard
RFC 4109	Algorithms for IKEv1	Proposed standard
RFC 3948	UDP Encapsulation of IPsec Packets	Proposed standard

RFC 3947	Negotiation of NAT-Traversal in the IKE	Proposed standard
RFC 3766	Determining Strengths For Public Keys Used For Exchanging Symmetric Keys	Best Current Practice (BCP 86)
RFC 4025	Method for storing IPsec keying material in DNS	Proposed standard
RFC 3547	Group Domain of Interpretation	Proposed standard

4.4 Cryptographic Algorithms

RFC 2405	ESP DES-CBC Cipher Algorithm With Explicit IV	Proposed standard
RFC 2451	ESP CBC-Mode Cipher Algorithms	Proposed standard
RFC 2403	Use of HMAC-MD5-96 within ESP and AH	Proposed standard
RFC 2404	Use of HMAC-SHA-1-96 within ESP and AH	Proposed standard
RFC 2857	Use of HMAC-RIPEMD-160-96 within ESP and AH	Proposed standard
RFC 2410	NULL Encryption Algorithm and Its Use With IPsec	Proposed standard
RFC 1828	IP Authentication using Keyed MD5 (may be moved to Historic)	Proposed standard
RFC 1829	ESP DES-CBC Transform (may be moved to Historic)	Proposed standard
RFC 2085	HMAC-MD5 IP Authentication with Replay Prevention	Proposed standard
RFC 3173	IP Payload Compression Protocol (IPComp)	Proposed standard
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups	Proposed standard

	for Internet Key Exchange (IKE)	
RFC 3566	AES-XCBC-MAC-96 Algorithm and Its Use With IPsec	Proposed standard
RFC 3602	AES-CBC Cipher Algorithm and Its Use With IPsec	Proposed standard
RFC 3664	AES-XCBC-PRF-128 algorithm for IKE	Proposed standard, being updated by draft-hoffman-rfc3664bis, which is accepted as a Proposed Standard
RFC 3686	Using AES Counter Mode With IPsec ESP	Proposed standard
RFC 4309	Using AES CCM Mode With IPsec ESP	Proposed standard
RFC 4196	SEED Cipher Algorithm and Its Use With IPSec	Proposed standard
RFC 4312	The Camellia Cipher Algorithm and Its Use With IPsec	Proposed standard
RFC 4106	Use of Galois Message Authentication Code (GMAC) in IPsec ESP	Proposed standard
draft-ietf-msec-ipsec-signatures	Use of RSA/SHA-1 Signatures within ESP and AH	Approved as a Proposed Standard

4.5 IPsec policy handling

RFC 3585	IPsec Configuration Policy Information Model	Proposed standard
RFC 3586	IP Security Policy Requirements	Proposed standard

4.6 Remote access

RFC 2661	Layer Two Tunneling Protocol (L2TP)	Proposed standard
RFC 3193	Securing L2TP using IPsec	Proposed standard

RFC 3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode	Proposed standard

4.7 SSL and TLS

RFC 2246	The TLS Protocol Version 1.0	Proposed standard, being updated to version 1.1 by draft-ietf-tls-rfc2246-bis
RFC 3546	TLS Extensions	Proposed standard, being updated by draft-ietf-tls-rfc3546bis
RFC 4279	Pre-Shared Key Ciphersuites for TLS	Proposed standard

4.8 General MPLS

RFC 3031	Multiprotocol Label Switching Architecture	Full standard
RFC 3032	MPLS Label Stack Encoding	Full standard
RFC 3036	Label Distribution Protocol (LDP) Specification	Full standard

4.9 MPLS constrained by BGP routing

RFC 2547	BGP/MPLS VPNs	Informational RFC -- being updated by draft-ietf-l3vpn-rfc2547bis, which has been accepted as a proposed standard
RFC 4265	Definition of Textual Conventions for Virtual Private Network (VPN) Management	Proposed standard
draft-ietf-l3vpn-rt-constrain	Constrained VPN route distribution	In IETF Last Call

4.10 Transport of layer 2 frames over MPLS

draft-ietf-pwe3-control-protocol	Transport of Layer 2 Frames Over MPLS	Approved as a Proposed Standard

---

4.11 Virtual Routers

draft-ietf-l3vpn-as-vr	Applicability Statement for Virtual Router-based Layer 3 PPVPN approaches	
draft-ietf-l3vpn-vpn-vr	Network based IP VPN Architecture using Virtual Routers	
draft-ietf-l3vpn-vr-mib	Virtual Router Management Information Base Using SMIv2	

References

[1] CIGRE Technical Brochure: 'Integrated Services Networks for Utilities' by Cigre Working Group 07 of Study Committee D2 – August 2003.