INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1311.1

(07/2001)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

Internet protocol aspects – Transport

Network-based IP VPN over MPLS architecture

ITU-T Recommendation Y.1311.1

(Formerly CCITT Recommendation)

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Y.1311.1

Network-based IP VPN over MPLS architecture

Summary

This Recommendation specifies service requirements and a number of architectural approaches that are applicable to the provision of network-based virtual private networks by Service Providers using IP technology over an underlying MPLS-based infrastructure.

Source

ITU-T Recommendation Y.1311.1 was prepared by ITU-T Study Group 13 (2001-2004) and approved under the WTSA Resolution 1 procedure on 13 July 2001.

Keywords

Internetwork Protocol (IP), IP VPN, Multiprotocol Label Switching (MPLS), Virtual Private Network (VPN).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Page

ITU-T Recommendation Y.1311.1

Network-based IP VPN over MPLS architecture

1 Introduction

A crucial need exists to specify mechanisms to support IP virtual private networks over MPLS networks. Furthermore, it is clear that Recommendations must describe and specify ways of developing interoperable implementations in order to allow end-to-end service delivery across multi-vendor service provider infrastructures.

Service providers have urgent needs to deploy IP VPN services over MPLS infrastructure and they require carrier-class and fully interoperable implementations.

2 Scope

This Recommendation provides a general description of network-based IP VPN services and requirements including network architectures and interworking aspects between a set of possible approaches.

The IP VPN service requirements and supporting network architectures are intended to provide input and guidelines for the definition of protocol enhancements which may be developed by the IETF and other standardization entities for the support of IP VPNs.

Although this description primarily addresses MPLS-based networks, it is envisaged that some of these requirements may also apply to other IP-based network architectures using other technologies for the creation of network-based IP VPNs. Examples of these include GRE, IP within IP, IPSEC.

Another Recommendation, ITU-T Y.1311, currently under development, will provide a generic architecture and service requirements for IP VPNs.

3 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated are valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

3.1 Normative references

[1] ITU-T Y.1241 (2001), *Support of IP based services using IP transfer capabilities*.

[2] ITU-T Y.1310 (2000), *Transport of IP over ATM in public networks*.

3.2 Informative references

[3] IETF RFC 2764 (2000), *A Framework for IP Based Virtual Private Networks*.

[4] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[5] IETF RFC 2547 (1999), *BGP/MPLS VPNs*.

[6] IETF RFC 2917 (2000), *A Core MPLS IP VPN Architecture*.

[7] IETF RFC 2998 (2000), *A Framework for Integrated Services Operation over Diffserv Networks*.

[8] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

[9] IEEE802.1Q (1998), *IEEE Standard for local and metropolitan area networks: virtual bridged local area network.*

[10] ITU-T Y.1311 (Draft), *IP VPNs – Generic architecture and service requirements.*

[11] ITU-T Y.iptc (Draft), *Traffic control and congestion control in IP networks.*

[12] ITU-T Y.1720 (Draft), *Protection switching for MPLS networks.*

4 Abbreviations

This Recommendation uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
ATM	Asynchronous Transfer Mode
BAS	Broadband Access Server
BGP	Border Gateway Protocol
CE	Customer Edge (device)
CHAP	Challenge Handshake Authentication Protocol
CoS	Class of Service
CR-LDP	Constraint-based Routing Label Distribution Protocol
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Circuit Identifier
DNS	Domain Name Server
DS	Differentiated Services
DSCP	Differentiated Service Code Point
DSL	Digital Subscriber Line
DVMRP	Distance Vector Multicast Routing Protocol
EXP	MPLS Experimental Field
FR	Frame Relay
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP VPN	IP Virtual Private Network
IP	Internet Protocol
IPSEC	IP Security
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System

L2TP	Layer 2 Tunnelling Protocol
LDAP	Lightweight Directory Access Protocol
LSP	Label Switched Path
LSR	Label Switching Router
MD5	Message Digest 5
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
NAS	Network Access Server
NAT	Network Address Translation
NNTP	Network News Transfer Protocol
OAM	Operations, Administration and Maintenance
OSPF	Open Shortest Path First
P	Provider (Core router)
PAP	Password Authentication Protocol
PE	Provider Edge (router)
PHB	Per Hop Behaviour
PHP	Penultimate Hop Popping
PIM	Protocol Independent Multicasting
POS	Packet Over Sonet/SDH
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RSVP	Resource Reservation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Provider
TACACS	Terminal Access Controller Access Control System
TCI	Tag Control Information
TE	Traffic Engineering
TMN	Telecommunications Management Network
TOS	Type of Service
VCC	Virtual Channel Connection
VCI	Virtual Circuit Identifier

VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VPN-ID	VPN Identifier
VR	Virtual Router

5 Network-based IP VPN over MPLS reference model

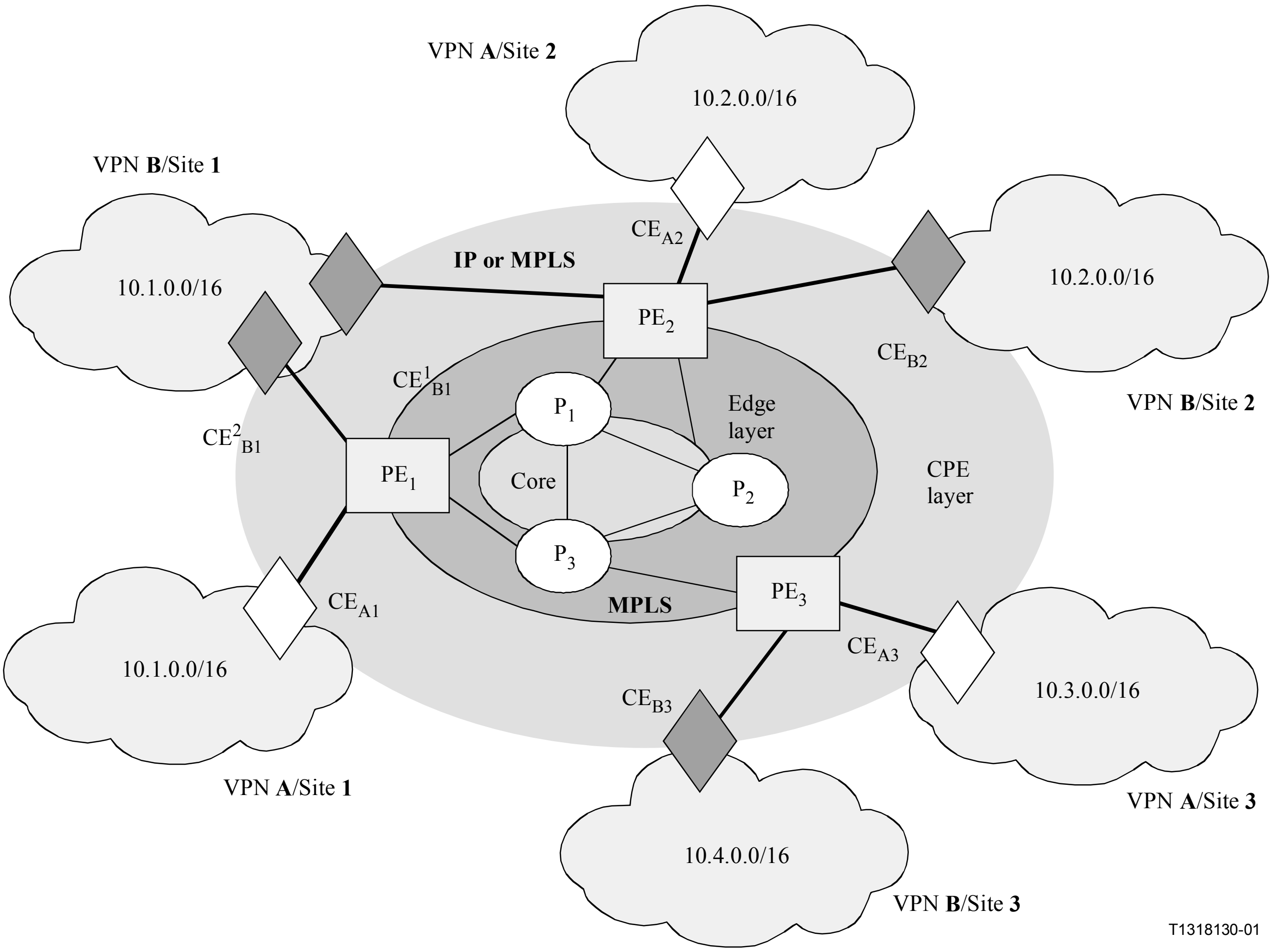

Figure 1/Y.1311.1 – Network-based IP VPN over MPLS reference model

NOTE – Figure 1 uses IPv4 address network prefix notation.

6 Service definition

6.1 Functional definition of a "network-based IP VPN (over MPLS)"

A network-based IP VPN provides a layer 3 service to customers.

A customer site is connected to the Service Provider network-based IP VPN, and the IP VPN takes care of routing packets to the correct customer destination. With a network-based IP VPN, the provider edge routers are responsible for learning and distributing among themselves the customer layer 3 reachability information.

Consider a set of "sites" which are attached to a common network which may be called the "backbone". If some policy is applied to create a number of subsets of that set with the following rule: two sites may have IP interconnectivity over that backbone only if at least one of these subsets contains them both. The resulting subsets are "Virtual Private Networks" (VPNs). Two sites have IP connectivity over the common backbone only if there is some VPN which contains them both. Two sites which have no VPN in common have no connectivity over that backbone.

If all the sites in a VPN are owned by the same enterprise, the VPN is a corporate "intranet". If the various sites in a VPN are owned by different enterprises, the VPN is an "extranet". A site can be in more than one VPN, e.g. in an intranet and in several extranets. In general, the use of the term VPN does not distinguish between intranets and extranets.

Consider the case in which the backbone is owned and operated by one or more Service Providers (SPs). The owners of the sites are the "customers" of the SPs. The policies that determine whether a particular collection of sites is a VPN are the policies of the customers. Some customers will want the implementation of these policies to be entirely the responsibility of the SP. Other customers may want to implement these policies themselves, or to share with the SP the responsibility for implementing these policies.

The mechanisms that may be used to implement these policies are a primary focus of this Recommendation. The described mechanisms are general enough to allow these policies to be implemented either by the SP alone, or by a VPN customer together with the SP. Most of the discussion is focused on the former case, however.

The case of interest here is where the common backbone offers an IP service. The focus is not on the case where the common backbone is part of the public Internet, but rather on the case where it is the backbone network of an SP or set of SPs with which the customer maintains contractual relationships. That is, the customer is explicitly purchasing VPN service from the SP, rather than purchasing Internet access from it. (The customer may or may not be purchasing Internet access from the same SP as well.)

The customer itself may be a single enterprise, a set of enterprises needing an extranet, an Internet SP, an application SP, or even another SP which offers the same kind of VPN service to its own customers.

6.2 Quantitative definition of a "network-based IP VPN (over MPLS)"

The dimensioning parameters characterizing a network-based IP VPN service offer can be expressed as the number of expected customers, the number of expected users/sites (permanent and temporary access) per customer, the total number of expected IP VPNs to be deployed (a site may have more than one VPN).

7 Service requirements

A VPN solution should support the following service requirements:

7.1 Multi-vendor interoperability

- Multi-vendor interoperability at network element, network and service levels.
- Support of Internet standards (including compatibility, modularity, backward compatibility, protocol extensions, etc.).

- The solution should be multi-vendor interoperable within the SP network infrastructure and with the customer network equipment and services making usage of the VPN service offered by the SP.

7.2 Service management capabilities

Management functions are usually distributed according to the TMN model which identifies four macroscopic management layers (business, service, network and elements management).

In case of VPN management, which evolves in this model, setting up the VPN and managing the deployed devices requires taking care of three main aspects:

- connectivity: configuring, provisioning and managing the devices, especially when topology can change;
- network monitoring (particularly performance and capacity monitoring) in order to meter resources usage and to anticipate scalability problems;
- security: authentication, authorization and overall policies (including security risks introduced by policy inconsistency).

Some examples of service management capabilities:

- per VPN and per device MIB availability;
- per VPN fault management (e.g. core network failures);
- per VPN SLA management;
- per VPN policy profiles management;
- per VPN security profiles management;
- management of various customer site connectivity scenarios;
- management of various topologies;
- management of various service deployment scenarios;
- management of various types of customer IP traffic (IPv4, IPv6, unicast, multicast, etc.);
- per VPN configuration should not impact other sites/VPNs;
  - addition/Deletion of a site should not involve changing configuration on PEs other than the PE the site is connected to;
  - addition/Deletion of a site of a given VPN should have no negative impact on other VPNs, including VPNs whose site(s) are connected to the same PE as the site that has been added/deleted.

Automated operations and interoperability with standard management platforms should be pursued.

NOTE – The specification of a management information base (MIB) describing the detailed configuration of network elements involved in the provisioning of VPN services is a key requirement in network provisioning, but will not be handled within the scope of this Recommendation.

In order to facilitate the service management, a logical view of the network indicating VPN topology above the backbone topology is useful. It can be used for provisioning and verification of connectivity, verification of configuration/privacy, fault management and performance management.

7.2.1 Network connectivity

Following the VPN growth, new devices must be configured according to service templates defined by the provider and such a task is quite repetitive. The management system could centralize such a process to guarantee coherence of parameters and accelerate deployment by automating configuration.

As VPN configuration and topology is highly dependent on the customer's organization, provisioning templates have to apply to the customer's specific requirements (remote accesses, security policy, QoS). The management system could rely on centralized information to get all needed parameters for optimal adaptation of templates to specific needs. It could even assure some path optimization in routing tables.

Such a system may increase the network reactivity in case of failure or policy violation. It can reduce provisioning delay in case of current VPN configuration requested by the customer (add, modify, delete), which can be a very heavy task in terms of routing tables update.

In a multi-domain environment, the end-to-end QoS depends on the QoS provided by each domain. In case of a VPN spanning across two domains, QoS provisioning may reach its limit and such a problem seems difficult to solve.

7.2.1.1 Verification of the connectivity

It is desirable that a capability to verify the connectivity between user sites within a VPN is provided. If a logical view of a VPN is provided and the result of this verification is shown in this view, the operator can understand the result easily.

7.2.1.2 Verification of configuration and privacy

It is desirable that a capability to verify the configuration and privacy of a VPN is provided. Privacy here means that the VPN cannot be accessed from outside of this VPN. If a logical view of a VPN is provided, and the result of this verification is shown in this view, the operator can understand the result easily.

7.2.2 Service monitoring

Network monitoring in the VPN perspective includes the classical items such as fault management, service level management and accounting.

7.2.2.1 Fault management

As VPNs rely on a common network infrastructure, the network management system should provide means to inform the provider on the consequences of a device failure for the VPNs it supported. The NM should provide a logical view of the network indicating VPN topology above the backbone topology. It should provide pointers to the related configuration and customer's requirement information so as to ease fault isolation and take corrective action as impact on traffic engineering and security considerations may be important.

To summarize, fault management includes:

- customers information of failures;
- faults detection (incidents reports, alarms, failures visualization, SLA violation);
- faults localization (analysis of alarms reports, diagnosis);
- incidents recording, logs (creation and following of the trouble ticket);
- corrective actions (traffic, routing, resources, etc.).

7.2.2.2 Performance management

The performance management system should be able to monitor network behaviour in order to evaluate performance metrics that form part of the service level agreements. Multiple different VPN services are subscribed by the customers and the system should be able to deploy specific measurement techniques depending on the activated service components (security, multicast, remote access). These techniques may be either intrusive or non-intrusive depending on the parameters or service being considered.

QoS deployment and SLA monitoring may be coupled by monitoring policies that:

- describe QoS mechanisms and the associated metrics that should be activated;
- control monitoring resources such as probes and remote agents.

Remote agents may be a key to the network monitoring as it allows the collection of statistics directly at the network access points used by customers and mobile users. A logical view of the network indicating the VPN topology helps operators to understand the result of the performance management activities.

To summarize, performance management includes:

- real time performance measurements (indicators and thresholds initialization and modification, data collection);
- real time monitoring (resources utilization), VPN status (up/down);
- analysis (bandwidth, response time, availability, packet loss);
- statistics and trends based on collected metrics.

Additionally, the performance management system should have a "Dynamic bandwidth management" capability:

- Dynamic bandwidth management should allow real time response to customer requests for changes of allocated bandwidth (control plane should be flexible to accommodate real time changes).

Performances (e.g. bandwidth allocation) should be traceable.

NOTE – Dynamic bandwidth allocation would normally occur within the ranges and bounds specified in the Service Level Agreement (SLA), possibly using internal SP mechanisms to check appropriate allocation.

7.2.2.3 Accounting

Being able to associate service profiles to customers, and to the resources providing these services may facilitate accounting which can be a key feature of subscribed services. The accounting system has to be able to sort among the huge amount of usage information and correlate this information to performance and fault management information to produce billing according to the real provided service. It should be noted that accounting requirements may conflict with security requirements.

To summarize, accounting process includes:

- measurements of resources utilization;
- production of accounting information;
- measurement storage (files creation and administration);
- quotas control per customer (current consumption update, consumption authorizations checking).

7.2.3 Security management features

The security management system of a VPN solution must include features to guarantee the security of network connections, the privacy and integrity of data.

7.2.3.1 Access control

Access control dictates the amount of freedom a VPN user has, and controls the access of other users to applications and different parts of the network.

A VPN without access control only protects the security of the transported data but not the network. Access control capabilities protect the entire network to ensure that VPN users have complete access to the applications, but only to these resources.

In case of negotiated customer bandwidth, the access control at network level should ensure that each customer doesn't violate his contract.

7.2.3.2 Authentication

Authentication is the process of verifying that the sender is actually who he says he is. The security management system should enforce authentication.

Support for strong authentication schemes is particularly important to ensure the privacy of both VPN access point-to-VPN access point (PE-to-PE) and client-to-VPN Access point (CPE-to-PE) communications. This is particularly important to prevent VPN access point spoofing (e.g. PE fake to enter a specific, or a set of, VPN(s)) in the presence of auto-discovery mechanisms.

Nomadic access implying dynamic evolution of PEs serving a specific VPN is another situation which requires such authentication schemes in the presence of autodiscovery mechanisms. A variety of authentication methods are available to meet the needs of particular VPN deployments, including username/password authentication, RADIUS or TACACS servers, LDAP directory servers, X.509 digital certificates, smart cards, etc.

Scalability is critical when the number of nomadic/mobile clients is increasing. The authentication scheme implemented for such deployments must be both manageable and easily deployed for large numbers of users and VPN access points.

7.2.3.3 Data privacy

A VPN solution should protect the privacy of the data being transmitted. The security management system could participate in the enforcement of the data privacy.

Data privacy could be provided by encryption or by other mechanisms, e.g. data separation.

The solution may support multiple encryption algorithms and encryption schemes, including DES, 3DES, and the IPSec standards. Encryption, decryption, and key management could be included in profiles that may be enforced by a policy-based management system. It should be possible to activate encryption on specific services.

7.2.3.4 Dynamic advertisement of security information

The capability to dynamically advertise the security mechanisms to be applied to some specified user data traffic (per VPN, per route, etc.) would be a helpful management feature. This functionality should be provided in a scalable manner.

The automatic communication of security information related to a certain part of the data traffic would be an added value to the VPN deployment model. This would mean that a PE device that peers with a certain customer site, would announce to its peer PE devices the security information (e.g. tunnel type) related to the traffic to be sent to the considered site.

This announced security information could be associated to all the VPN traffic sent to the announcing PE, to the traffic sent to a specific VPN, or to the traffic sent to a specific VPN route.

7.2.4 SLA and QoS management features

Service Level Agreements, per VPN and/or per VPN site, and/or per VPN route should include [1]:

- Service Level Objectives comprising some or all of:
  - IP Transfer Capability;
  - QoS parameters;
  - Availability;
  - Reliability;
  - Delivery confirmation;

  - Mobility and Portability support;
  - Security;
  - Bandwidth;
  - Priority;
  - Authentication;
  - Protocols supported;
  - Flexibility – scaling and connectivity;
  - Life of the SLA.
- Service monitoring objectives:
  - QoS monitoring – comparison against objectives;
  - Flow tracking;
  - Reports as necessary.
- Financial compensation objectives:
  - Billing option;
  - Penalties;
  - Pricing;
  - Early termination charges.

NOTE – General SLA requirements are more fully described in ITU-T Y.1241 [1].

The Service Level Specification is a part of the more general Service Level Agreement. A Service Level Specification captures the transport properties required by the customer for a correlated set of packets between specified ingress and egress interface(s) to the VPN.

A VPN customer should be able to negotiate the performance characteristics of one ore more flows between its VPN sites with the VPN Service Provider.

The following lists a number of conditions which should be met by a SLS negotiation procedure.

The SLS negotiation procedure must allow for:

- Original service requests, according the components of the specified SLS.
- Service acknowledgement, indicating agreement with the requested service level.
- Service rejection but indicating the possibility of offering a closely related service (or indication of alternative DSCP to use for a particular service). The reply message may indicate the related offering by overwriting the proposed SLS attributes (hints).
- Service rejection indicating the incapability of providing the service.
- Service modification from both user and SP.
- The negotiation procedure should be able to interact with feedback of events related to the service. For example performance degradation may result in renegotiation of the SLS.

More details regarding possible parameters that constitute the SLS are given in 7.4.

7.3 Security functions

7.3.1 Introduction

Security mechanisms deployed to support the IP VPN service offer should be as transparent as possible for the end-user except maybe for remote end-users accessing the IP VPN through ISDN, PSTN, xDSL or Internet for which AAA services may have to be deployed.

Users of an IP VPN should be able, and allowed to, deploy their own internal security mechanisms, in addition to those deployed by the Service Provider, in order to secure specific applications or internal IP VPN traffic. Those internal security services should ideally have to conform to operator requirements, especially when Quality of Service SLA has been contracted between the customer and the SP. In such a case, the security solution deployed by the customer should not hide information used by the SP to set up Quality of Service features. Generally, the constraint for the SP, in accordance with the privacy feature of the IP VPN, is to ensure, as far as possible, that internal security mechanisms which could be deployed within an IP VPN have a good chance to be transparently supported by the IP VPN service offer.

The IP VPN will generally be secured according to the customer's requirements in order to enforce the privacy characteristic of his IP VPN. This implies that the SP shall, in particular, ensure that:

- Every equipment (e.g. router) involved in the set up of an IP VPN shall be able to identify and authenticate each other so that the traffic exchanged within the scope of an IP VPN can be routed. Depending on the nature of this traffic, and the nature of the equipment involved to process it, this identification and authentication would have to be achieved between CEs, and/or between CEs and PE/P routers, and/or between PE/P routers.
- Privacy services shall be provided and integrated as a service element by the operator. Confidentiality and integrity services shall apply to:
  – either, all IP VPN traffic exchanged above the IP backbone between the different sites;
  – or, some limited IP VPN traffic identified by a combination of source and/or destination IP addresses and/ or protocols and/or applications (e.g. PE-PE security, per-route security, etc.);
  – administration traffic since this latter can contain sensitive information related to IP VPN configuration, users, security, accounting.
- Isolation of each IP VPN shall be strictly ensured and the operator shall at least have some visibility on intrusion attempts in order to stop those intrusions.
- In the same way, access to the various equipment deployed to support the IP VPN service shall be strongly secured in order to prevent unauthorized users to access the IP VPN resources. In particular, the access to the (switching) resources which are managed by the SP will have to be secured to prevent any kind of malicious attack, that may well come from any kind of hacker (Internet users or others).
- The security service elements offered should be flexible in order to accommodate the fact that some data may require stronger protection than other data.

The following security functions should be considered in an IP VPN service offering:

- isolation;
- user identification;
- user authentication;
- security of the flow;
- peer identification;
- peer authentication;
- site protection.

These functions are described hereafter.

7.3.2 VPN isolation

From the service provider perspective, and at a high level of description, the VPN isolation function consists in ensuring that all traffic exchanged within the scope of an IP VPN remains unknown and protected from other users of the backbone, and insensitive with regard to traffic transported over the supporting IP backbone.

From this perspective, the service provider shall ensure, when deploying the service, that it conforms to the following characteristics:

- Only a set of predefined users can access the IP VPN.
- QoS SLA shall be guaranteed whatever the state of the traffic experienced in the supporting IP backbone and especially when this traffic is generated by other customers within or outside the scope of the IP VPN service.
- IP connectivity shall be deployed in such a way that only recorded IP VPN sites, and registered remote users, can exchange traffic within the IP VPN. This may lead peer equipment to identify/authenticate each other at different level of the IP VPN service.
- Traffic exchanged might be secured thanks to encryption and/or authentication functions.
- IP VPN management functions shall not impact other IP VPN or services.

This isolation function is achieved by application of a combination of functions related to architecture, Quality of Service, security and administration functional domains. This set of functions, correctly deployed, constitutes a generic function called "VPN isolation". This function is nevertheless classified within the security domain due to the strong implication of security features in the realization of such a global isolation function.

7.3.3 VPN user identification

Among users of IP VPN can be found travelling people who are not permanently attached to one of the sites of the IP VPN. In order to control the access of those users to the IP VPN, it is necessary to identify them. This identification shall apply within the various deployment contexts which have been identified (intranet, extranet, etc.), keeping in mind that some of these users can have an access to several distinct IP VPNs. This identification function can be used to automate or trigger all technical actions which are necessary to establish the communication with the IP VPN the user wishes to connect to.

Two main identification contexts have to be considered:

- Identification in case of "mobility", whether it is an intra-site or inter-site mobility.
- Identification when the user tries to reach his IP VPN from a public or private access point through a NAS/BAS server, or even from a network having an Internet access to which he has a temporary access.

This function can be implemented by the IP VPN service provider either in totality, or partially. Roaming capabilities would probably have to be set up between the provider and the customer, who might well decide to perform the IP VPN user identification in the case where he does not accept to outsource the identification/authentication service. In fact, this identification will be used by the access service provider who needs to identify the user to provide the IP connectivity, and by the IP VPN user identification service in order to accept the IP VPN connection. The two mechanisms can be linked.

In this case, the access provider and the IP VPN service provider resources have to cooperate and an agreement has to be reached on common identification specification.

All information necessary to identify the users will have to be stored and should ideally be maintained by the customer. This information should be made available to the access provider for controlling the IP access.

7.3.4 VPN user authentication

The scope of this authentication function is the same as that above and concerns users in a remote access situation. This authentication function will consist in ensuring, with a good level of confidence, that the declared user is the one he/she is claiming to be.

Various authentication protocols might be used for that purpose depending on the level of security wished by the customer, but at least PAP, CHAP and challenged mechanisms should be supported since they are currently widely used in a large range of equipment and services.

This authentication function may be executed completely or partially by the IP VPN service provider. In the latter case, the authentication phase can be relayed to the customer access point according to the terms of the contract.

7.3.5 Securing the flows

Within the present context, which consists in deploying a VPN over a public IP backbone (which is part of the Internet), the sole routing functions are not sufficient to secure the flows of a given customer. As a matter of fact, even if the flows are correctly routed between the sites (including remote users), the corresponding traffic might be intercepted and consequently read or altered.

Securing the flows should be enforced at the network layer to ensure the two main characteristics:

- Privacy of the traffic, so that only authorized equipment can decrypt it.
- Integrity, to protect recipients from alteration which could have been introduced during the transport.

These two functions shall apply to, what is called here, the "data traffic" of the customer which includes the traffic exchanged between sites, between remote users and sites and even between remote users. But it shall also apply to "control traffic", which is not necessarily perceived by the customer but which is, nevertheless, essential to maintain his IP VPN.

Even if it is strongly recommended to deploy those functions in an operational context, these functions shall not be considered as mandatory and should be activated only if requested by the customer. Also, those functions should be as flexible as possible so that they can be deployed independently from each other and applied to some part of the traffic (security level may differ depending the traffic which is considered, performance considerations may also lead to secure a subset of the traffic).

7.3.6 Peer identification

Traffic exchanged within the scope of IP VPN may involve several categories of equipment that need to cooperate together to provide the service. These network elements can be CE, firewalls, backbone routers, servers, management stations, etc.

Each time two network elements need to cooperate, it is necessary for the peer to proceed to an identification (enforced by an authentication if needed, see below) before accepting to process the received traffic, or to provide the requested service. This identification can be used as a trigger to adapt the way the service will be provided but, in most cases, to control the access to the network resources.

This peer identification function is intended here to apply only to network elements participating in the IP VPN setup. All identification needs related to users' applications, are not included here.

Examples of such peer identification could apply to:

- traffic between a CE and a service provider access point (P/PE access point);
- traffic between CEs belonging to the same IP VPN;
- routers dealing with route announcement (these routers could be a CE and P/PE router or two CEs exchanging routing information);

- policy server and a network element;
- management station and an SNMP agent.

This identification function shall not be considered as an atomic function since, generally, it is distributed and probably implemented differently depending on network elements which are considered. But globally, the IP VPN service shall provide a peer identification function in defining, where it is necessary, how it shall be implemented, how secure it shall be, and the way to deploy and maintain identification information necessary to operate the service.

7.3.7 Peer authentication

This function is the prolongation, in security terms, of the above function. It aims at authenticating the peer, following the same philosophy adopted for user identification and authentication.

7.3.8 Site protection

As we saw before, a site might be involved in various ways within the scope of IP VPN. It can be part of an IP VPN deployed to support an Intranet (in that case he is interconnected with sites belonging to the same company), part of an IP VPN deployed between different companies to support an extranet, or both.

Within this context, a site might be subject to various attacks coming from different sources. These potential sources are:

- users connected to the supporting public IP backbone, since by definition an IP VPN is built over a public and shared IP infrastructure;
- users from the Internet, if the IP backbone offers an Internet access;
- users from remote sites belonging to the same IP VPN.

Risks that a site may encounter are the following:

- service denial (when a hacker acts in such a way that a service cannot be used: mail spamming and access line overloading for instance.);
- viruses.

Intrusions

In order to prevent these risks, the IP VPN service provider shall deploy functions that control access to the site, thanks to the deployment of filtering functions provided by firewall for instance, but also in monitoring, alerting and eventually logging all suspicious activities in order to detect all possible attacks.

7.4 Support of various Quality of Service requirements

The technical specification of the corresponding traffic parameters and QoS commitments are referred to as the "Service Level Specification" (SLS).

- SLS for Best-effort.
- SLS for DiffServ models:
  - Point-to-Cloud SLS (Hose model)

    The solution should support a "point-to-cloud" SLS. This means that the traffic parameters as well as the QoS commitment are specified on the basis of traffic exchanged between a VPN Site and the MPLS VPN Backbone (as opposed to on the basis of traffic exchanged between two VPN Sites). This is also referred to as the "Hose" model. An MPLS VPN SLS which defines compliance to the traffic contract by measurement of all the packets transmitted from a given VPN Site towards the MPLS VPN backbone on an aggregate basis (i.e. regardless of the destination MPLS VPN Site of each packet) is an example of "point-to-cloud" SLS.

  - Point-to-Point SLS (Pipe model)

    The solution should support a "point-to-point" SLS. This means that the traffic parameters as well as the QoS commitment are specified on the basis of traffic exchanged between two VPN Sites. This is also referred to as the "Pipe" model. "Point-to-point" SLSs are analogous to the SLS typically supported over layer 2 technologies such as Frame Relay and ATM. An MPLS VPN SLS which defines compliance to the traffic contract by separate measurement of the packets transmitted from a given VPN Site towards each remote destination VPN Site is an example of "point-to-point" SLS.

  - Point-to-Multisite SLS and Multisite-to-Point SLS

    The solution should support a "point-to-multisite" SLS and a "multisite-to-point" SLS. This means that the traffic parameters as well as the QoS commitment are specified on the basis of traffic exchanged between a VPN Site and a subset of the other VPN sites.

  - CoS transparency

    The solution should support "CoS transparency". This means that the public MPLS VPN service should be able to set the IP DS field at the egress of the MPLS VPN to the same value as it was on the ingress of the MPLS VPN service. Rationale for such requirement is provided in 10.3.

- SLS for IntServ model.
- Per VPN (measurable) SLAs.

General SLA requirements for IP-based networks are described in ITU-T Y.1241 [1]. Some of these SLA components may be applicable for IP VPNs.

- Strict QoS (guaranteed bandwidth VPN).
- QoS support in more complex scenarios:
  - Mapping of QoS Class between VPNs in case of VPN interworking.
  - Mapping of QoS Class in case of Inter-Provider VPNs.

The following describes which SLS parameters should be specified to enable the SP to support the defined VPN SLS types. The correlated set of packets is denoted as flow. The means by which packets are correlated to be part of a flow are described in the "Flow Descriptor".

The service to be guaranteed to the flow over the VPN is bound by the scope of the service, indicating the set of ingress and egress interfaces between which the transport properties are to be guaranteed.

In order to achieve the guaranteed transport properties, the flow should adhere to the traffic conformance parameters. Conforming traffic will receive performance guarantees as contracted. Traffic exceeding the traffic conformance test will receive an excess treatment.

The transport service can further be associated with service schedule, and service reliability parameters.

More detailed information can be found via references in Appendix II.

7.5 Support of various routing protocols (at edge and core levels of the SP network)

- There should be no restriction on the routing protocols used between CE and PE routers.
- The choice of Service Provider's IGP must not depend on the routing protocol(s) used between PE and CE routers. Furthermore, that choice should be flexible, not limited to a single routing protocol.

7.6 Scalable routing capabilities

- The amount of routing and/or scheduling state in a P router must be independent of the total number of VPNs supported by a Service Provider, and of the number of VPN sites. In some specific scenarios, a trade-off introducing a limited amount of routing and/or scheduling state in a P router could be considered in order to provide additional capabilities, or value-add for the SP (e.g. multicast inside a VPN).
- The amount of routing (and/or configuration) information on PE may depend only on the VPNs whose site(s) are connected to that PE.
- The solution should support filtering of VPN routing information in the PE-to-PE and CE-to-PE configurations.

7.7 Auto-discovery

The solution should support an auto-discovery mechanism that dynamically conveys VPN information between PEs. This mechanism can be used for different purposes, primarily for service scalability purposes (one example based on BGP is provided via references in Appendix II).

7.8 Support of various types of customer IP traffic

- Unicast;
- Multicast;
- The solution should be able (easily extendable) to enable a service provider, having an IPv4 or an IPv6 backbone, to provide both IPv4 and IPv6 VPNs to its customers.

7.9 Support of various VPN topologies

– The solution should support a wide range of inter-site connectivity ranging from hub-and-spoke to partial mesh and full mesh.

7.10 Support of various customer access scenarios

- Permanent and temporary access:
  - multi-homing;
  - backdoor links;
  - dial-in.
- Support of customer access right outsourcing feature (the management system could rely on centralized information to get all needed parameters for optimal adaptation of templates to specific needs. This could reduce provisioning delay in case of current VPN configuration requested by the customer (add, modify, delete), which can be a very heavy task in terms of access tables update).

7.11 CE access to PE

The solution should support various access technologies: PSTN, ISDN, xDSL, cable modem, Leased Lines, ATM, Frame Relay, Wireless local loop, mobile radio access, etc. (a wide range of bandwidth should be supported, according to the specific technology in use).

7.12 Addressing requirements and support of various IP numbering schemes

- The solution must allow VPN address overlapping: IP addresses have to be unique only within a given VPN, but not across VPNs.
- The solution should minimize the usage of IP addresses.

- The solution should not preclude NAT.
- Support of customer IP numbering schemes (private, globally unique, no scheme), (on-demand) support of a dynamic IP address allocation mechanism, support of an IP numbering outsourcing feature. (Support of customer IP numbering outsourcing feature: the management system could rely on centralized information to get all needed parameters for optimal IP numbering allocation. Such a system could increase the network flexibility in case of growth. This could reduce provisioning delay in case of current VPN configuration requested by the customer (add, modify, delete), which can be a very heavy task in terms of routing tables update. It could even allow cost-effective IP numbering resource optimization.)
- A unique identifier for the VPN (as well as further identifiers, such as for VPN tunnels) might be appropriate in specific scenarios.

7.13 Support of various service deployment scenarios

- Multiple VPNs per customer site.
- VPN service coupled with Internet access per customer site.
- The solution must support connectivity among sites belonging to the same or different organizations (Intranet/Extranet).
- Inter-AS VPN.
- Inter-Provider VPN (the solution must allow VPN to span multiple Service Providers).
- Carrier or carriers (one scenario being hierarchical VPNs).

7.14 Support of alliances of VPNs

NOTE – The "VPN alliance" terminology may be reviewed further.

Network management, signalling and routing protocols shall support/enable:

- the (easy) initial formation of a VPN alliance;
- the (easy) joining of a new alliance member VPN;
- the (easy) quitting of an alliance member VPN;
- the (easy termination of the entire VPN alliance.

Any VPN may become member of a VPN alliance.

While the alliance exists, there may eventually be different degrees of confidentiality with respect to intra-alliance and inter-alliance member communication.

Solutions shall take into account items such as:

- failing connectivity that causes partitions of the VPN alliance;
- use of different VPN approaches internally by the alliance member VPNs;
- use of different approaches for interconnecting the alliance member VPNs;
- use of different routing and signalling protocols internally by the alliance member VPNs;
- using private addressing within alliance member VPNs.

It is expected that the possible usage of a VPN unique identifier for one particular alliance member VPN might play a role for identifying routes/tunnels, at least between different VPNs (that member may be called the VPN alliance leader).

7.15 The solution should allow outsourcing of IP services (e.g. DNS, DHCP)

- The solution should allow the packaging of additional IP services provided by the VPN Service Provider itself, or by a third party service provider, for services such as DNS, FTP, HTTP, NNTP, SMTP, LDAP, VoIP, Videoconferencing, Application sharing, Streaming, E-commerce, and other services like backup.
- The solution should allow the outsourcing of IP services. (The management system could rely on centralized information to get all needed parameters for optimal adaptation of IP services to specific needs. This could reduce provisioning delay in case of new version or VPN configuration requested by the customer (add, modify, delete). It could even allow cost-effective resource optimization by offering services to a large range of customers.)

7.16 Reliability and fault tolerance

It is required to provide high reliability on the network to construct a VPN on the public network which satisfies the same quality as on leased lines.

Survivability techniques, such as protection switching or restoration, are necessary for fast recovery from failure to enhance the reliability of the VPN.

Requirements for protection switching are as follows:

- Fault management, such as fault detection (see 7.2.2.1).
- Both routing and resources are pre-calculated and allocated to a dedicated protection entity prior to failure to offer a strong guarranty of being able to re-build the required network resources post-failure.
- Fast recovery time.
- More general framework for protection switching for MPLS networks is provided in [12].

7.17 Efficiency (customer and network resource utilization)

- Service Provider network Traffic Engineering.
- Per VPN Traffic Engineering.

Traffic Engineering is a key technology for carrier IP networks to control and optimize the networks in general. Traffic Engineering provides optimization of network resources in order to satisfy performance objectives of application services, these are performed taking into account the specific network characteristics which may impact service level objectives.

Particularly, this applies to the provider provisioned IP VPN application service. Indeed, Traffic Engineering could contribute to provide resource and admission control for VPNs. In case of such usage, Traffic Engineering might check whether the requested service for new VPNs can be provided without deteriorating the previously installed VPNs with respect to QoS performance.

Traffic Engineering also plays an important role in modifying and adjusting resources for existing and new VPNs, according to the demands of customers and the needs of the service providers.

7.18 No dependency on the physical or link layer of the Service Provider backbone

MPLS is a technology which can be applicable to various physical layers or data link layers, such as SDH (Packet over SONET using PPP-framing), ATM, Frame Relay, Ethernet, etc. It is desirable that the functions provided on MPLS-based VPNs, such as QoS Control, OAM functionality are available irrespective of any physical layer or data link layer.

7.19 (Economically and technically) smooth migration of customers from pre-existing VPN service offerings

- The solution should allow migration of customers without heavy disruption of service.
- The solution should enable various customer migration scenarios e.g. "Partial migration" scenario: migration of some sites of a given VPN to a network-based IP VPN ensuring service continuity with the other legacy-VPN sites of this VPN.

7.20 Support of interworking functions between MPLS-based VPN technology and other VPN technologies

The requirement of the data plane for the interworking nodes is:

- Mapping of all the relevant information from one underlying VPN transport technology to the other underlying VPN transport technology.

  (A way for the information mapping is using encapsulation: there are various network-based VPN technologies and, in each technology, packets are encapsulated by the header which is specific to the technology. An identifier in the encapsulation header is used to separate the connection of the VPN user from connections of other VPN users in the network, and thus the end-to-end data integrity is maintained. The encapsulation header also has a field which presents the QoS class, and each node on the connection carries out the QoS control by seeing this field.)

  Other requirements for the data plane are for further study.

In some cases (e.g. VPNs based on different technologies), requirements shown below may be taken into account:

- Interworking of signalling protocol which is used by each VPN technology between MPLS-based VPN and other VPN technologies (this requirement may be also applied to interworking between one MPLS-based VPN and another MPLS-based VPN in which different signalling protocols are used).
- Exchanging the routing information between MPLS-based VPN and other VPN technologies.

7.21 Some numerical assumptions for a network-based IP VPN Service Provider offering

- Very large number (e.g. up to 10 000 000) of VPNs per Service Provider.
- Wide range of number of sites per customer (depending on size or structure of the customer organization): ranging from few sites to 10 000 sites per VPN per customer.
- Wide range of number of routes per VPN: ranging from few to 100 000 routes per VPN (this number may be limited by the choice of the routing protocol between CE and PE).
- More than one VPN per site should be possible.
- High values (to be estimated) of the frequency of configuration set-up and change should be supported (ex. real time provisioning of an on-demand videoconferencing VPN).

7.22 A VPN solution may support the following service requirements

- Support of other service deployment scenarios:
  - VPN over CE-to-CE MPLS.

8 Framework architecture

The basic VPN network model is that the Customer Edge (CE) devices are connected to the Provider Edge (PE) routers. The connection must provide direct IP connectivity (one IP hop) between the CE devices and the PE routers. A CE device may be connected to a PE router via any type of data link (e.g. an ATM VCC, Frame Relay circuit, Ethernet, POS, L2TP session, GRE or IPSEC tunnel etc.).

If a particular site has a single host, that host may be the CE device. If a particular site has a single IP subnet, the CE device may be a switch. In general, the CE device can be expected to be a router, which we call the CE router. The PE routers learn the IP addresses reachable at each customer site and distribute this information amongst themselves. The PE routers also establish and maintain tunnels of some sort between themselves that are used for forwarding VPN data traffic across the SP backbone. For the purpose of this Recommendation the tunnels are LSPs. Routers in the SP backbone that do not maintain any VPN state are termed P routers.

The following distinct areas can be identified, and these are discussed below:

- learning customer-site reachability information;
- distributing VPN reachability information;
- constrained distribution of routing information;
- LSP tunnel establishment and usage.

8.1 Learning customer-site reachability information

Mechanisms are needed to allow a PE router to discover the set of IP addresses reachable via a link to a directly connected CE device, and to allow a CE router to discover the set of IP addresses in other sites of the VPN to which the CE device is attached. These mechanisms include:

- running a routing protocol (e.g. RIP, OSPF or BGP);
- use of static configuration;
- tracking dynamic address assignments if DHCP or PPP is used.

There is a wide range of options with respect to the amount of routing information that a CE router receives from its directly connected PE router. At one end of the spectrum the PE router may just advertise a single route, default, to the CE router. At the other end of the spectrum the PE router may advertise all the routes it received from other sites.

8.2 Distributing VPN reachability information

When a PE router has determined the set of destinations reachable via its directly connected CE device for a VPN, it must then distribute this information towards other PE routers that have customer sites attached for that VPN.

The mechanisms available to do this are:

- run an instance of a routing protocol for that VPN – the virtual router (VR) approach. The VR approach is discussed in more detail in 9.2.
- piggyback the VPN reachability information on a backbone BGP. An approach using BGP is described in 9.1.

  NOTE – In theory one could piggyback this information on an IGP, however, the scalability considerations make this option non-viable.

8.3 Constrained distribution of routing information

To meet the specified scalability goals, a PE router should be able to maintain just the routes for the VPNs whose sites are directly connected to that PE router. That, in turn, requires the ability to constrain the distribution of VPN routing information.

When a PE router learns reachability information for a locally attached VPN customer site, this information must be distributed (subject to route filtering and/or route aggregation) to other PE routers that also have customer sites attached to the VPN. One element of a VPN solution is how, on a per VPN basis, each PE router determines a set of other routers to which it must distribute this reachability information.

The mechanism used by BGP/MPLS VPN (see 9.1) is route filtering based on the BGP community attribute. More details can be obtained from [5].

Possible mechanisms used by the Virtual Router approach to determine the set of other routers that are treated as routing peers are:

- use of a directory which PE routers query;
- explicit configuration via configuration management;
- multicast approach;
- piggybacking the information in a routing protocol used by the provider backbone (e.g. BGP).

Another consideration is inter-site connectivity. It could range from a full mesh to a hub-and-spoke, or anything in between (e.g. partial mesh).

Yet another consideration is that a link between a PE router and a CE device could be either established "on-demand", or could be relatively permanent. An example of an "on-demand" link would be a PPP session, where RADIUS could be used to associate the CE device with a particular VPN.

In the Virtual Router approach, for a given VPN, determining the set of PE routers that have CE devices in that VPN is known as determining VPN membership. Also in this approach, one needs to construct a per VPN topology. The mechanism for constructing such a topology may be distinct from the mechanism used to actually distribute the reachability information between PE routers. For example, any of the mechanisms listed above can be used for this purpose.

8.4 LSP tunnelling establishment and usage

An important aspect of the LSP tunnelling is whether an LSP is used to provide transport for a single VPN, or whether it is used to carry traffic for multiple VPNs. This is usually a trade-off between the extra resources needed to establish and maintain VPN-specific tunnels, against the fine-grained QoS control and any other advantages which may be obtained with dedicated LSPs.

Another aspect of the LSP tunnelling is that the LSP tunnels form a network by themselves, i.e. LSP tunnels may be built to offer various topologies (from hub and spoke, to partial mesh and full mesh). Topology choices may depend on the different customer and SP requirements, such as supporting alternative ingress to egress paths, minimizing the number of tunnels to be managed and maintained. Different algorithms are available for determining tunnel topologies. Additional references can be found in Appendix II.

9 Approaches for support of network-based IP VPN services

9.1 BGP/MPLS VPN approach

The approach described in this clause is described in [5].

This approach includes:

- Non-disruptive service configuration in the event of addition/deletion of new sites or extranet partners.
- Optimal use of LDP for setting up label switched paths with minimal configuration.

- Providing Internet access to customers when they have a single data link layer between them and the PE router, and the data link layer cannot support multiple logical IP addresses.
- Support for backdoor links between sites in specific configurations.
- Use of hub and spoke topology to build a management network.
- The interaction in the PE between the Service Provider BGP and the instances of IGP (used to exchange routing information between the CE and the PE).

9.2 Virtual Router approach

This clause describes a network-based VPN solution based on the Virtual Router concept, which offers separate routing, forwarding, and Quality of Service on a per VPN basis.

Several solutions have been put forward to achieve different levels of network privacy when building VPNs across a shared public backbone. Most of these solutions require separate per VPN or per VPN site forwarding capabilities and make use of IP or LSP tunnels across the backbone. This clause describes a network-based VPN architecture based on the virtual router concept, which offers separate routing, forwarding, and Quality of Service on a per VPN basis. This architecture complies with the IP VPN framework described in [3].

Virtual Routers use the same mechanisms from a routing and data forwarding standpoint as physical routers and are easy to deploy, operate, and troubleshoot. VPN membership discovery is aided by the use of one of a number of mechanisms suggested in this clause. This approach attempts to draw the line between the SP and the VPN customer: the SP owns and manages layer 1 and layer 2 services while layer 3 services belong to the VPN and can be, at the discretion of the SP, manageable by the VPN customer. Data security issues are addressed by the use of either private LSPs, or the use of label stacks over shared LSPs, to keep the data belonging to specific VPNs confined to their domains.

Any routing protocol can be used in the Virtual Router. This flexibility applies to the CE, to PE segments as well as in the PE to PE segments. Private data and routing information is exchanged between VPN sites through IP-based or MPLS-based tunnels across the backbone.

9.2.1 Virtual Router

A Virtual Router (VR) is an emulation of a physical router at the software and hardware levels. Virtual Routers have independent IP routing and forwarding tables and they are isolated from each other. This means that a VPN's IP addressing space can overlap with another VPN's address space. The IP addresses need only be unique within a VPN domain.

A Virtual Router has two main functions:

- Constructing routing tables describing the paths between VPN sites using any routing protocols (e.g. OSPF, RIP, or BGP).
- Forwarding or switching packets to the next hops within the VPN domain.

From the user point of view, a Virtual Router provides the same functionality as a physical router. Many virtual routers can coexist on the same PE router. From the CEs' point of view, the PE router performs the functions of many routers, forwarding packets to the correct destination, while isolating each VPN traffic in the same manner that individual routers do. Separate router capabilities provide each VPN CE link with the appearance of a dedicated router that guarantees isolation from other VPN traffic while running on shared switching and transmission resources.

Virtual private networks are created by interconnecting VRs across the backbone and customer edge devices. The network administrator assigns a Virtual Router at every PE where the sites attach to the CE-based network. Virtual Routers belonging to the same IP VPN domain must have the same Virtual Private Network identifier (VPN-ID). The VPN-IDs provide VPN membership between VRs. To the CE access device, the Virtual Router appears as a neighbour router in the CE-based network, to which it sends all traffic for non-local VPN destinations. Each CE access device must learn the set of destinations reachable through its connection to the virtual router on the PE router; this may be as simple as a default route. Virtual Routers participating in a single VPN domain are responsible for learning and disseminating reachability information among themselves.

9.2.2 VR-based VPN architecture building blocks

Each Virtual Router is configured to support one VPN at a given time (although the VR might be configured to support many).

It is recognized that any network-based VPN (using piggybacking reachability on the routing protocol or not) requires some form of tunnelling (e.g. MPLS).

VPN sites are tunnelled through the use of MPLS tunnels. In this architecture, MPLS is used as a transport mechanism, even if other types of tunnelling are not excluded with this architecture. Furthermore, depending on the VPN deployment scenario, label stacking mechanism can be used. The tunnels can be statically configured or dynamically established (using existing mechanisms). Traffic sent through the tunnel is opaque to the underlying backbone technology used.

A network-based IP VPN (over MPLS or not) consists of providing site-to-site private connectivity across a SP core-networking infrastructure. A virtual private network is composed of multiple VPN sites attached to private CE-based network. The CE device (e.g. a router) is connected to a PE.

The PE provides to the CE-based network routing and forwarding capabilities across the backbone. The underlying backbone data link technology can be ATM, FR virtual circuits, or PPP.

The private CE-based network, where the VPN sites are attached to access the PE router by connecting to a Virtual Router over an access link, can be ATM, FR virtual circuits, or a PPP connection. Routing tables associated with each Virtual Router define the site-to-site connectivity for that VPN.

9.2.3 VR-based VPNs deployment scenarios

Virtual Routers can be deployed in different configuration schemes. The following are three basic examples of deploying VR-based VPNs.

Example 1: Direct VR connectivity using layer 2 connections, see Figure 2.

Virtual Routers can be deployed directly over layer 2 connections (e.g. ATM).

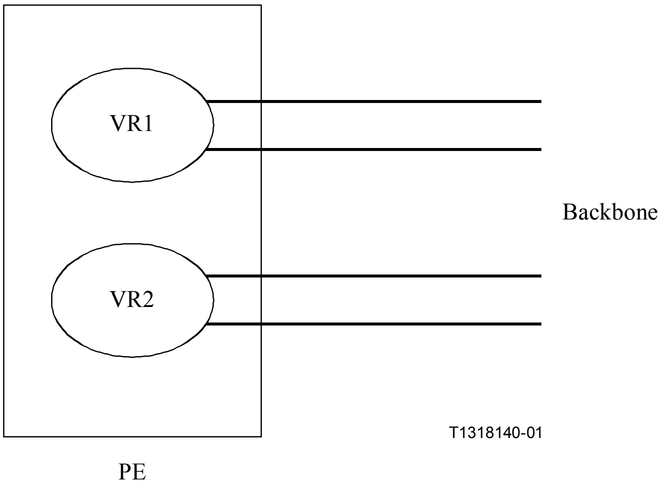

Figure 2/Y.1311.1 – Example 1: Direct VR connectivity using layer 2 connections

Example 2: Using one Virtual Router on the backbone, see Figure 3.

A Virtual Router can be used to connect each PE to a shared backbone.

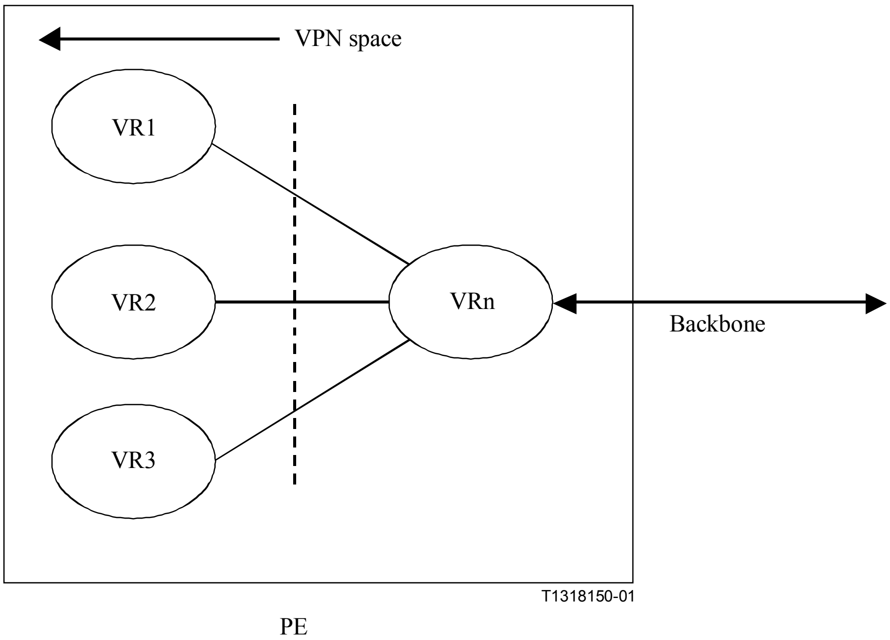

Figure 3/Y.1311.1 – Example 2: Using one Virtual Router on the backbone

Example 3: Using multiple Virtual Routers on the backbone, see Figure 4.

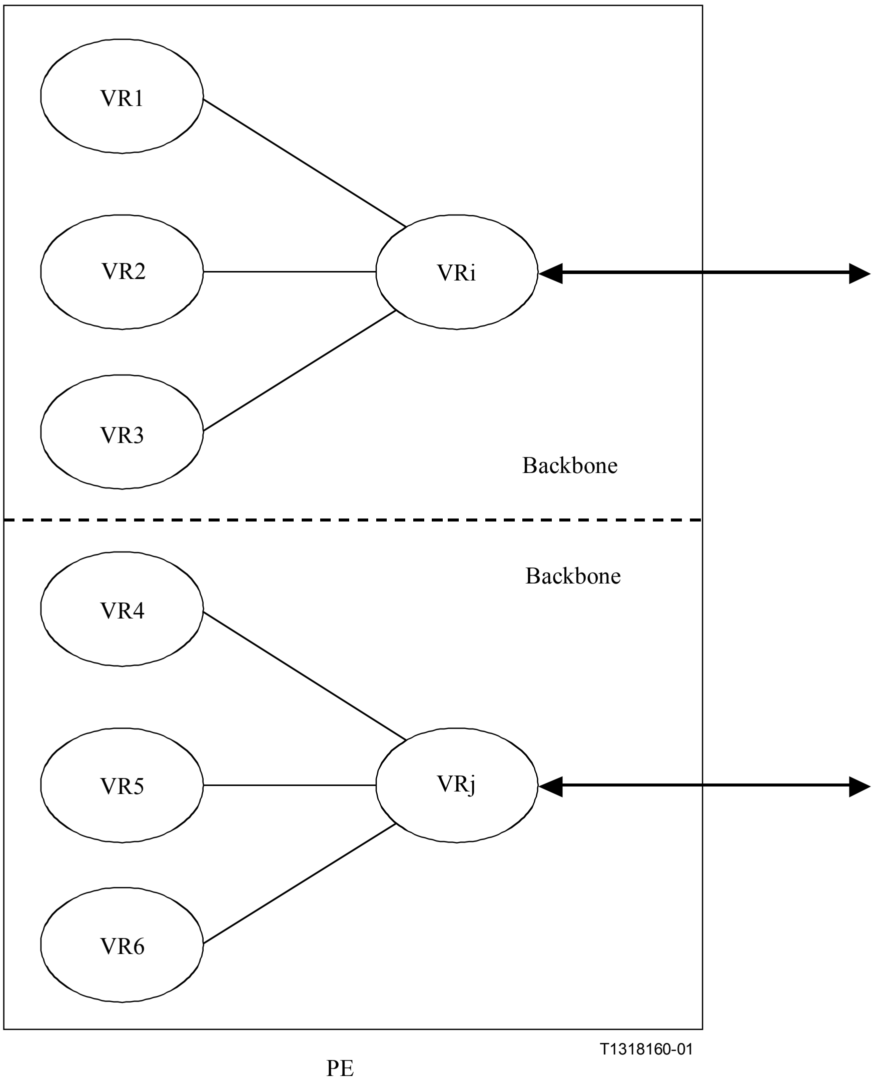

Figure 4/Y.1311.1 – Example 3: Using multiple Virtual Routers on the backbone

9.2.4 VPN reachability determination

By definition, virtual routers run different instances of routing protocols on a per VPN basis. Using tunnels (e.g. MPLS LSPs) reachability information is carried across the tunnels. The Virtual Router holds the routes only for the specific VPNs configured for that VR. This architecture does not use piggybacking VPN reachability information in the routing protocol running on the backbone (e.g. BGP).

Clause 9.2.4.1 below describes one method to distribute reachability information among VRs.

9.2.4.1 Inter VR broadcast Link

Virtual Routers need to send messages to all other VRs in other PEs in a particular VPN (for example, VRs need to send broadcast datagrams as mandated in routing protocols (OSPF broadcast mode, RIP V2 etc.)).

In the traditional routed networks, when broadcast media such as Ethernet is available, and when routing protocols such as OSPF broadcast mode or RIP V2 are configured over these media, link resources are efficiently used and convergence times are minimized.

In the case of VR based VPNs, a broadcast facility for a VR to send messages efficiently to all other VRs in the VPN could then be useful, particularly in case of large networks (e.g. high number of VPNs and PEs per VPN).

One way to provide this broadcast facility is by the use of Multicast. More detailed information can be found via [6].

9.2.5 VPN membership and topology determination

VR-based VPNs can be deployed in different configurations. The Virtual Router approach explicitly separates the mechanisms used for distributing reachability information from mechanisms used for achieving membership and topology determination. The VR-based architecture doesn't exclude the possibility that, on a single PE, multiple types of VR-based VPNs can coexist using different membership and topology discovery mechanisms.

Among these mechanisms we can list:

- Directory server approach which PEs query to determine their neighbours.
- Explicit configuration via a management platform.
- Multicast approach (more detailed information can be obtained via [6]).
- Piggybacking VPN membership and topology using available routing protocols [3] (e.g. BGP).

9.2.6 Operations and management

The key element in this clause is the fact that all existing operational and management tools and mechanisms can be used in the context of a VR-based solution. In general, the SP owns and manages layer 1 and layer 2 entities. To be specific, the SP controls physical switches or routers, physical links, logical layer 2 connections (such as DLCI in Frame Relay, VPI/VCI in ATM) and LSPs (and their assignment to specific VPNs). In the context of VPNs, it is the SP's responsibility to contract and assign layer 2 entities to specific VPNs. VPN Layer 3 entities can be managed either directly by the SP or, at the discretion of the SP, by the VPN customer. Examples of these entities include IP interfaces, choice of dynamic routing protocols or static routes, and routing interfaces. Note that although layer 3 configuration logically falls under the VPN user's area of responsibility, it is not necessary for the VPN user to execute it. It is quite viable for the VPN user to outsource the IP administration of the Virtual Routers to the SP.

9.2.6.1 VPN monitoring using VR-based solution

When a VPN user logs into a PE (directly or indirectly) to configure or monitor the VPN, the VR-based architecture allows the VPN user to log into the VR related to his specific VPN. The VPN user has only layer 3 configuration and monitoring privileges for the VR. Specifically, the VPN user has no configuration privileges for the physical network. This provides the guarantee to the SP that a VPN administrator will not be able to inadvertently, or otherwise, adversely affect the SP network.

9.2.6.2 VPN service availability with VR-based solution

In the VR-based architecture, it is possible for the SP to control and decide what VPN services get re-established first in case of PE service disruption (e.g. migration, upgrades, failures, etc.). The ability to not rely on piggybacking VPN reachability on the backbone routing protocol allows the VR-based solution to address per VPN availability requirements for applications running on top of the VPN network. This particular point is important when a large number of VPNs is supported on the PE.

9.2.6.3 VPN troubleshooting

In the VR context, SP (or the VPN customer) can use all existing troubleshooting tools with no modifications on a per VPN basis (e.g. ping).

9.2.7 Security considerations

Different levels of data, routing and configuration security may be implemented using VR-based architecture.

9.2.7.1 Routing and data security

The use of existing routing protocols such as OSPF and BGP means that all the encryption and security methods (such as MD5 authentication of neighbours) are fully available in VRs. Furthermore, any private routing, forwarding and addressing manipulation are done within the virtual router context. Direct layer 2 connections (ATM, FR), or tunnelling mechanisms used (e.g. MPLS LSPs) provide different levels of data security.

9.2.7.2 Configuration security

Virtual Routers appear as physical routers to the VPN user. Existing security mechanisms as password, RADIUS, etc. can be available to the VPN user.

9.2.8 VPN Quality of Service

The architecture adapts to different Quality of Service mechanisms to ensure site-to-site Quality of Service preservation on a per VPN basis. Packets received from a VPN site can receive Quality of Service treatment at the Virtual Router level, which directly impacts what egress backbone link to use. In this case, the Virtual Router may classify and police the packets on a per VPN basis.

This model allows separate Quality of Service engineering of the VPNs and the backbone.

9.2.9 Scalability

In this architecture, only the PEs are handling VPN type information.

The internal backbone nodes (e.g. routers) are not VPN aware.

Furthermore, for a network-based VPN solution, it is desirable to simplify the deployment and configuration of different VPNs with several sites sharing the same geographical location. Virtual Routers allow multiple private CE-based networks to connect to a single SP device.

One advantage of the ability to contain the VPN address space, and the VPN routing and forwarding capabilities within the Virtual Router entity, is the possibility to distribute PE system resources on a per VPN basis. An example of such distribution is to apply different scheduling mechanisms for processing each VPN activity within the PE router. This distribution contributes in establishing a wide range of priority schemes among VPNs.

9.2.10 Hierarchical relationship between VR-based VPNs

This clause describes one technique for building a hierarchical relationship between VR VPNs. An application of this technique enables the aggregation of many regional or local Service Provider VPN networks across a Hierarchical VPN tunnelling architecture. The approach presented here does not require any modifications of any existing routing protocols.

A simplified example that shows a hierarchical relationship between Virtual Routed VPNs is shown in Figure 5.

NOTE – Hierarchies can be extended to more than two levels.

Hierarchical levels are designated numerically with the highest level designated as 0. Lower hierarchical levels are designated as Level 1, 2, etc. Higher level VPNs transport lower level VPNs. So:

– Level 0 represents the highest hierarchical level. A Level 0 VPN transports lower level VPNs but is not itself transported by any other VPN;

– Level 1 represents a VPN that is transported by a Level 0 VPN but is not itself transported across any lower or equal level VPN.

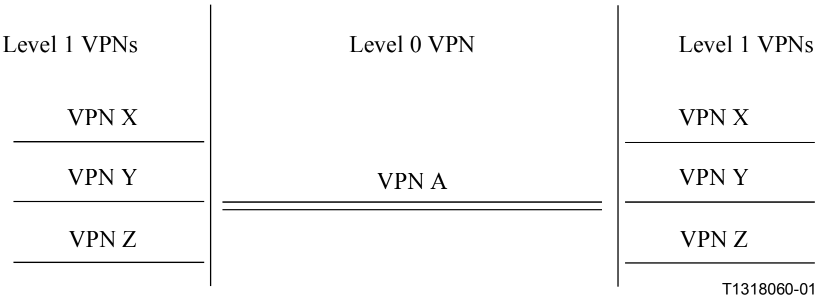

Figure 5/Y.1311.1 – Hierarchical VPN Levels

By assigning the VPNs depicted in Figure 5 to different hierarchical levels, a hierarchical relationship between the VPNs is created. For example, the highest hierarchical level is designated as "Level 0". In this example, VPN A is a level 0 VPN. Similarly, VPNs' X, Y and Z are part of the next lowest hierarchical level, designated "Level 1". Data within a Level 1 VPN is transported transparently across the Level 0 VPN.

A possible realization of a Hierarchical VPN (similar to that depicted in Figure 5) can now be described using the VR model. This realization does not assume a single Service Provider only is involved. Specifically, in the examples which follow, SP1 and SP2 do not have to be the same Service Provider. MPLS Label stacking techniques are used to create the hierarchical levels and explain how the data is transported.

Figure 6 shows an example of a Hierarchical VPN involving two Service Providers. This example assumes that SP1 provides an international backbone network that is utilized by SP2 to connect its geographically isolated regional (or local) networks. In this example, SP2 is providing two customer VPNs, X and Y. A two-level Hierarchical VPN is created to allow VPN X and VPN Y (i.e. level 1 VPNs in this hierarchy) to be transported (at level 0) across VPN A.

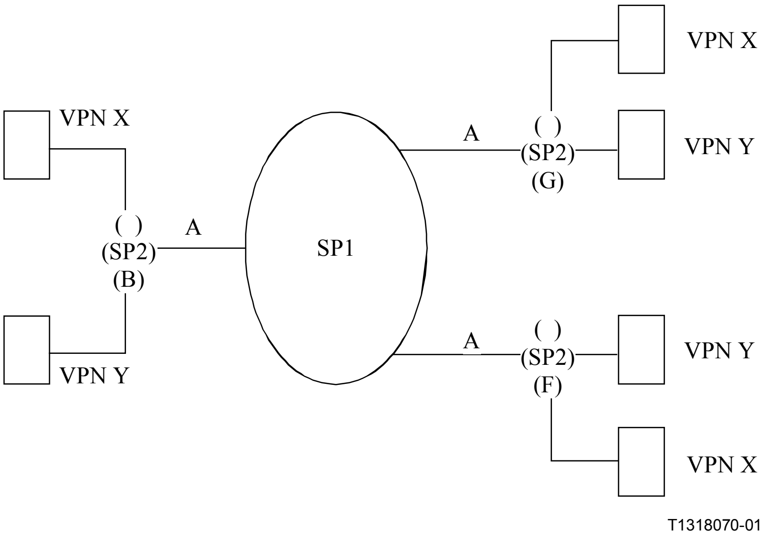

Figure 6/Y.1311.1 – Hierarchical VPN

Figure 7 expands the diagram to show the relationship between SP2 and SP1. From this figure we can see that SP2 provides both the two end customer VPNs, and SP2 must also know about the backbone (VPN A) that it uses for transporting the hierarchy. On the other hand, SP1 needs to be concerned with just the Level 0 VPN A.

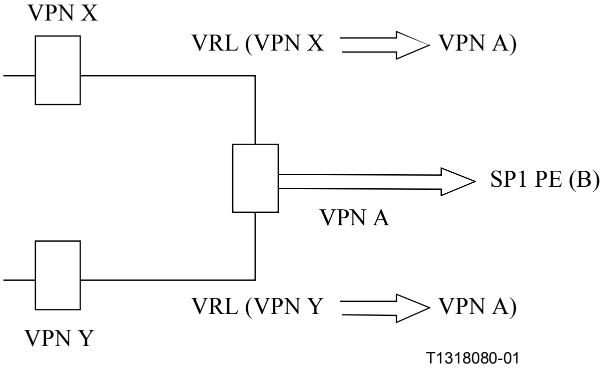

Figure 7/Y.1311.1 – Hierarchical relationship of Virtual Router Links

Figure 7 also shows a relationship between a level 1 VPN (e.g. VPN X) and a level 0 VPN (e.g. VPN A). A Virtual Router Link (VRL) is used between the Level 1 and Level 0 VPNs. The VRL is explained in more detail in the next clause.

In Figure 7, the hierarchical relationship is shown by the directional arrow indication (i.e. VPN X => VPN A). The lower level VPN X has an arrow pointing to the higher level VPN A, as indicated by VPN X => VPN A.

9.2.10.1 Virtual Router Link

A VR can be connected to other VRs by a Virtual Router Link (VRL).

Each end of VRL is logically bound to a VR. From the perspective of the VR, the VRL looks like one of its many links, some of which could be physical links.

The user can define a set of rules on this VRL to control the relationship between two VPNs. This relationship could be hierarchical or peering.

In the case of hierarchical VPNs, VRLs are configured between VRs with one end as the upper end of the hierarchy, and the other as the lower end.

NOTE – Investigation into whether VRLs can be extended to cover point-to-point connections between VRs for control information exchange is for further study.

9.2.10.2 Label distribution

VPNs can use any label distribution protocol. The only restriction is, within a specific VPN, the same protocol should be used in all its PE devices, so that they can interwork. This is restricted by the nature of the distribution protocol, not by the VPNs.

Referring to Figure 6, SP1 provides the Level 0 VPN service (called VPN A) to SP2(B/G/F).

The label distribution operates independently in each level of the VPN Hierarchy. Labels are distributed for the Level 0 VPN separately from the labels that are distributed for the Level 1 VPN. The following text describes the label distribution for each level of the hierarchical VPN.

Level 0 (VPN A) label distribution

The PEs of SP1 share the VPN A routing information between each other. In other words, the reachability information of SP2 edge routers is exchanged. LSP tunnels are set up in VPN A between the edge routers of SP2. For example, an LSP tunnel from SP2 (edge router B) is created to SP2 (edge router G).

Level 1 (VPN X) label distribution

The PEs of SP2 share the VPN X routing information with each other. In other words, the reachability information of the CE routers of VPN X is exchanged. LSP tunnels are set up in VPN X between the CE routers in SP2.

Usage of Penultimate Hop Popping (PHP) requires penultimate and top-most labels to be allocated from the same label space (e.g. in this case, the allocation is from VPN A's label space). This implies in the case of Hierarchical VPNs, that an additional label (i.e. the penultimate label) will be necessary between the IGP label (i.e. top-most label) for the PE and VPN destination label. This is shown in 9.2.10.3 on Forwarding.

In this example, it is indicated that A2 is the label for SP2-CE(G) in SP2-CE(B) and it is shown in 9.2.10.3 how A2 is used. (see Figure 8). This label is chosen from the VPN A Label space.

Architecturally, Level 1 VPN X and Y are connected to Level 0 VPN A by a Virtual Router Link. Note that the edge routers of SP2 must have knowledge of all three VPNs (i.e. VPN X, VPN Y, and VPN A). When the VRL is configured for a hierarchical relationship, then the top level VPN will allocate a label for each VRL, i.e. to each VPNs, from its label space.

9.2.10.3 Forwarding

User data from the lower level VPNs (e.g. Level 1 in Figure 8) are forwarded by the LSP tunnels of the upper level VPN (e.g. Level 0 in Figure 8). The label encoding shown in Figure 8 is explained below.

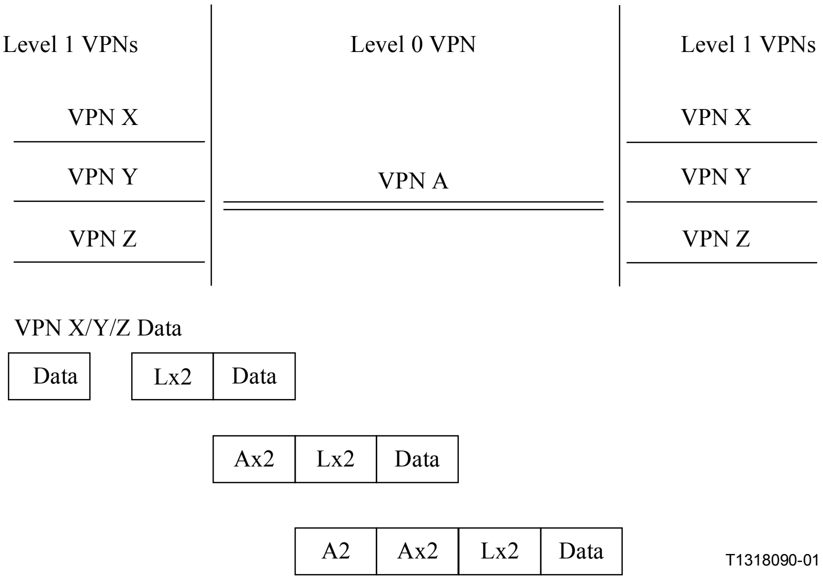

Figure 8/Y.1311.1 – Label encoding

1) Customer data arrives at the VPN X CE router in SP2 (B) and is encapsulated in a MPLS frame.

2) Label Lx2 is pushed on to the Label Stack. Lx2 is the peer VPN X CE label used to forward VPN X data to VPN X CE router in SP2 (G).

3) Next, Label Ax2 is pushed on to the Label Stack. Ax2 is the peer VPN X attachment label with VPN A taken from VPN A's label space. This label is used by VPN A to forward data on the SP2 (G) VRL between VPN A and VPN X.

4) Finally, Label A2 is pushed on to the Label Stack. This is the peer VPN A label used to forward data from the VPN A SP2 (B) PE router to the VPN A SP2 (G) PE router.

In summary, the complete LSP path therefore to move customer data on VPN X from the SP2 (B) CE to the SP2 (G) CE is as follows:

a) Transport data across Level 0 (VPN A) using label A2.

b) Transport data across the VRL from Level 0 to Level 1 in SP2 (G) using label Ax2.

c) Transport data across Level 1 (VPN X) from SP2 (B) to SP2 (G) using label Lx2.

10 QoS approaches

The following proposed approaches have been identified.

10.1 "Point-to-Cloud" SLS

The IETF Differentiated Services architecture defines mechanisms which are DiffServ Traffic Conditioning and DiffServ PHBs. It also defines that various end-to-end Differentiated Services can be constructed by combining in specific ways some subset of these mechanisms along with specific resource allocation policies.

It is expected that resource allocation policies (on a per DiffServ service basis) can be developed by network administrators which would allow, in combination with DiffServ Traffic Conditioning and PHB, support of "point-to-cloud" SLS.

As an example, a network administrator may support a "point-to-cloud" SLS by:

- activating Traffic Conditioning at each service boundary based on the traffic parameters of the corresponding individual SLS;
- activating PHBs and allocating resources on each access link (for each PHB) based on the traffic parameters of the corresponding individual SLS;
- activating PHBs in the network core and allocating resources for each PHB on an aggregate basis (i.e. independently of individual SLSs) for each PHB based on ongoing monitoring and provisioning cycles for each PHB on every link.

DiffServ Traffic Conditioning, as well as DiffServ PHBs, can be supported on MPLS devices. Consequently, with an MPLS VPN infrastructure, Traffic Conditioning functions and PHBs can be activated at any point of the network (e.g. CE, PE, P devices) in a consistent manner regardless of whether this device is running MPLS or regular IP. In turn, this means that end-to-end DiffServ services can be built over a DiffServ-capable MPLS VPN backbone in the same way as they can be built over a non-MPLS DiffServ network. In turn, this means that "point-to-cloud" SLS can be supported over a DiffServ capable MPLS VPN backbone exactly in the same way as they can be offered over (non-MPLS) IP backbones.

10.2 "Point-to-Point" SLS

Some applications expected to be transported over a public MPLS VPN service are anticipated to require "point-to-point" SLS.

10.2.1 "Point-to-Point" SLS via resource allocation policies

Although the end-to-end DiffServ services are still to be defined in detail in the IETF, it is expected that, in some environments, resource allocation policies (on a per-DiffServ service basis) can be developed by network administrators which would allow, in combination with DiffServ Traffic Conditioning and PHB, support of "point-to-point" SLS. As an example, a network administrator may support a "point-to-point" SLS by:

- activating Traffic Conditioning at each service boundary based on the traffic parameters of the corresponding individual SLS;
- activating PHBs and allocating resources on each access link (for each PHB) based on the traffic parameters of the corresponding individual SLS;
- activating PHBs in the network core and allocating resources for each PHB on an aggregate basis (i.e. independently of individual SLSs) for each PHB based on significant over-provisioning combined with ongoing monitoring and provisioning cycles for each PHB on every link.

Again, because the DiffServ mechanisms can be supported over MPLS in a transparent manner, in environments where resource allocation policies can be developed in order to offer "point-to-point" SLS, those can be applied to DiffServ-capable MPLS VPN backbones in exactly the same manner.

10.2.2 "Point-to-Point" SLS via resource allocation policies and additional mechanisms (explicit in-band admission control, constraint-based routing)

It is expected that, in some environments, "point-to-point" SLSs cannot be efficiently supported by relying solely on the DiffServ mechanisms combined with resource allocation policies. For instance, where Integrated Services (IntServ) services are to be supported from a given VPN Site to another given VPN Site with individual "point-to-point" commitments, and where backbone resources are scarce so that overprovisioning cannot be assumed, additional mechanisms, such as explicit in-band admission control as well as constraint based routing, would be required.

Reference [7] provides a framework for supporting end-to-end IntServ services when a DiffServ cloud is used in the core. One approach discussed is to perform admission control on an aggregate basis in the core over the DiffServ resources.

DiffServ mechanisms can be supported on an MPLS backbone in a manner which is compatible with MPLS Traffic Engineering (TE) signalling protocols. In particular, the MPLS Label Switched Paths (LSPs) can be established using MPLS Traffic Engineering (TE) signalling protocols. In this case, bandwidth requirements can be signalled by MPLS Traffic Engineering (TE) signalling protocols so that bandwidth reservation, as well as admission control, can be performed at LSP set-up. Also, those DiffServ LSPs can be constraint-based routed.

MPLS Traffic Engineering can be made aware of DiffServ so that constraint-based routing can be performed separately for different classes requiring that different constraints be met.

Thus, by combining DiffServ support over MPLS with the existing MPLS constraint-based routing mechanisms in accordance with the approach defined in [7], or DiffServ-aware TE approaches, end-to-end IntServ "point-to-point" SLS can be supported over a DiffServ/TE-capable MPLS VPN backbone. This proposed approach can be used even in environments where overprovisioning cannot be assumed.

In case of heterogeneous backbones as in Annex A (not fully-MPLS backbones), additional mechanisms such as aggregation of RSVP for reservations across the non-MPLS backbone can be used to provide end-to-end SLS guarantees.

10.3 "CoS transparency"

Reference [8] states that the codepoints of the DS field may be changed within a DS domain by DS interior or DS boundary nodes. It is assumed that the same principle applies for the fields used in the context of the DiffServ over MPLS approach (e.g. the EXP field within the MPLS Shim Header).

The modification of the these fields is not sufficient in conjunction with the provisioning of IP VPNs, since the specific requirements of IP VPNs have not been taken into account. These specific requirements are:

- VPN customers using applications with internal CoS solutions should have the possibility to utilize the solutions independent of the CoS solution supported by the SP infrastructure.
- VPN customers supporting more CoS than the SP should have the possibility to use these classes within their physical private network sites.
- A carrier's carrier service provided by a Network Provider may enable a SP (client of the mentioned network provider) to offer the IP VPN service to its customers. The unchanged transport of the indicated CoS is an essential requirement for the Network and Service Providers. By means of the CoS transparency feature, the SP can offer his own CoS solution to his customers regardless of the CoS solution supported by the Network Provider.

Although an IP VPN can be considered as a kind of emulation of a physical private network, it is not feasible for the Network Provider to support all the various customers' or Service Providers' CoS solutions. Thus, the support of CoS Transparency ensures that the unchanged transmission of the CoS indicated by a customer or a SP is guaranteed across the Network Provider's MPLS network.

DiffServ Tunnelling Models over MPLS include:

- Uniform Tunnelling Model;
- Pipe Tunnelling Model.

The Pipe Model is such that the DiffServ information of packets transported over the Tunnel is not affected by the DiffServ information used over the Tunnel span.

Operations of the Pipe Model without PHP (Penultimate Hop Popping) are illustrated in Figure 9.

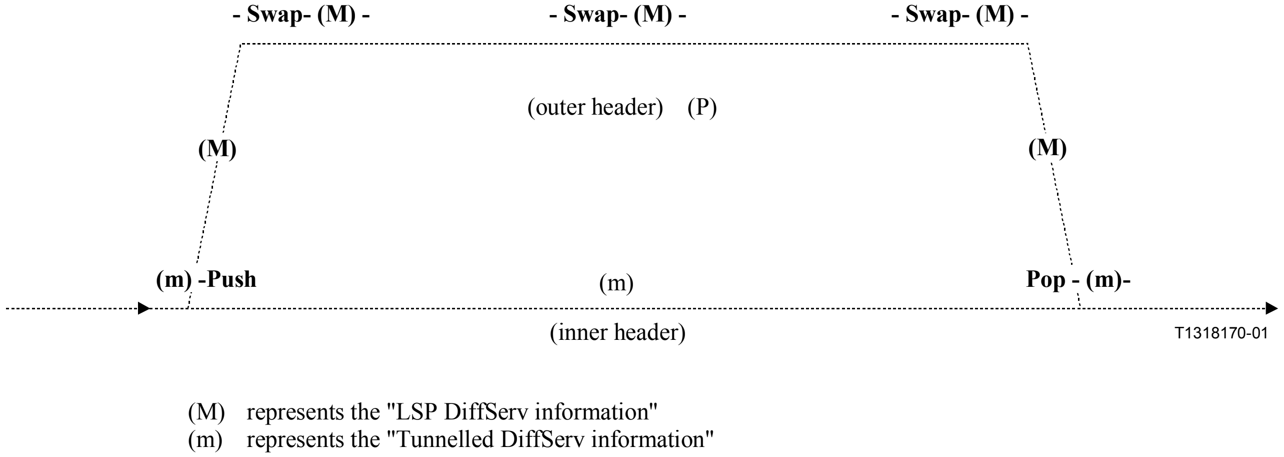

Figure 9/Y.1311.1 – Pipe model without PHP

One application of the "Pipe Tunnelling Model" is support of CoS Transparency over an MPLS VPN backbone.

11 Inter-Autonomous System (Inter-Service Provider) VPN

Network-based IP VPNs can span several ASs or SPs. The most common example is that of an international corporation which has offices in several countries around the globe and would like to outsource its IP services to an SP. Reality is such that it would be very rarely that such a corporation would be able to buy services from one SP who has points of presence near every site that the corporation has. Typically, some SPs span regions/countries and some have international presence. This means that the corporation needs to buy VPN services from different SPs depending on the local or branch office needs. This in turn means that interconnecting these geographically disparate VPN islands is of high value to the Provider with global presence. Of course, global presence may mean international presence to an SP aiming to provide connectivity to national Providers in various parts of the world; it could also mean national presence to a SP aiming to provide connectivity to regional Providers in a given country. The need for interworking is then a requirement.

One way to provide VPN services to a corporation via several ASs (SPs) is by using the hierarchical VPN mechanism described in 9.2.10.

However, no constraints are currently anticipated that will prevent this method from being extended to cover Inter-AS (SP) interconnection scenarios based on other VPN approaches.

It should also be noted that capabilities for Inter-AS (SP) VPN scenarios based on the BGP/MPLS VPN approach are available in [5].

12 Interworking

12.1 Interworking between different solutions

This clause outlines one possible solution of interworking between approaches described in this Recommendation.

The following issues are taken into account:

- Motivation for interworking among VPNs (see 12.1.1).
- Assumptions of MPLS VPNs as elements for interworking (see 12.1.2).
- Functional capabilities for interworking such as realization of security, mapping of the QoS class, dynamic routing information distribution (see 12.1.3).

Scalability limitations of this solution may limit its applicability and therefore further work is needed.

12.1.1 Motivation for interworking among MPLS VPNs

Two cases are identified:

Case 1: VPNs spread over multiple differently implemented MPLS networks owned by different VPN SPs. This follows the normal requirement and expectation that each VPN SP chooses its best VPN implementation out of multiple implementations.

Case 2: VPNs spread over multiple differently implemented MPLS networks owned by a VPN SP. A VPN SP may deploy multiple MPLS networks (e.g. an old MPLS network and a new MPLS network). The VPN interworking removes the requirement that all user sites of one VPN need to be connected to the same MPLS network.

In both cases, the interworking enables VPN SPs to provision VPN services flexibly. It is of benefit to VPN users as well.

12.1.2 Assumptions

The following MPLS network structure in Figure 10 is assumed to be present as a base to provide VPN services.

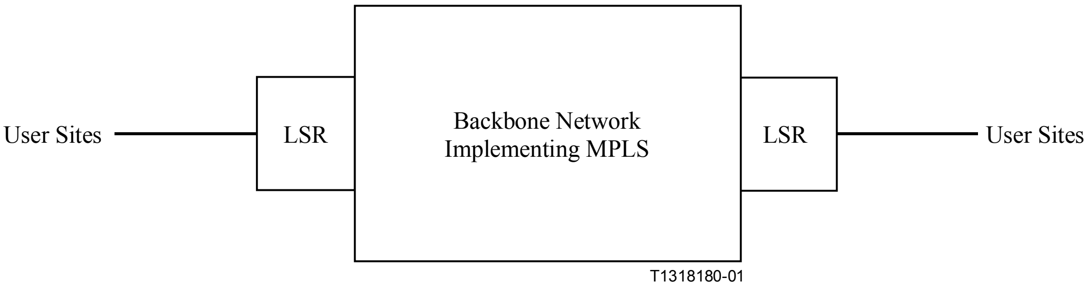

Figure 10/Y.1311.1 – Structure of MPLS network

Figure 11 depicts the interworking model.

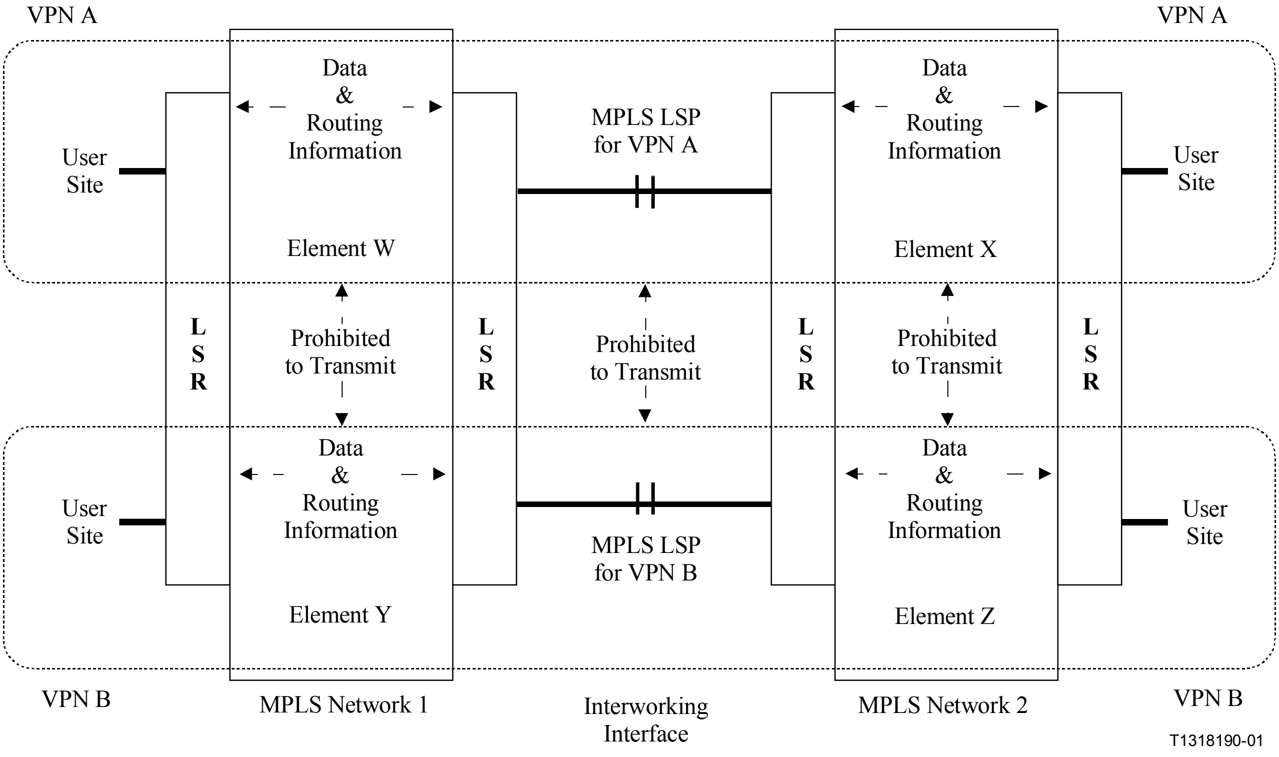

Figure 11/Y.1311.1 – Interworking model

An "element" is each part of a VPN that is separated by an MPLS network. When a VPN spans multiple MPLS networks (domains), the part of the VPN belonging to a single MPLS network is called an "element".

12.1.3 Functional capabilities for interworking among MPLS VPNs

12.1.3.1 Functional capabilities for interworking

There are the following two types of VPN interworking:

- Type (1): Interworking where each MPLS network is terminated and IP header look-up is executed at an egress/ingress LSR.
- Type (2): Interworking without terminating MPLS and without IP header look-up at any egress/ingress LSR.

As each existing MPLS VPN is implemented in a unique manner, it is difficult to realize type (2).

Type (1) is easy to provision since it utilizes the LSR's function of IP header look-up. Therefore, we focus on type (1).

The assumptions are that the connections at the interworking interface are provided by IP or MPLS.

The following three functional capabilities are required to support VPN interworking:

- Realization of security;
- Mapping of the QoS class;
- Dynamic routing information distribution in clauses 12.1.3.2, 12.1.3.3 and 12.1.3.4 respectively.

12.1.3.2 Realization of security

When MPLS VPNs span multiple MPLS networks, every VPN has a designated "connection" (e.g. ATM VC, MPLS LSP, etc.) at the interconnection boundaries of the MPLS networks. It is not permitted to transmit packets between any given connection and any other MPLS VPN (except where specific inter-VPN agreements have been made). This mechanism results in realization of security. The procedures by which such an assignment is established are specific to the solution used by the MPLS network implementation associated with the connection.

The identity of VPN at each end is meaningful only in the context of the specific MPLS network associated with the connection. It is assumed that multiple VPNs do not share one connection.

See Figure 11 above: there is a logical connection between the MPLS network 1 and MPLS network 2 used for constructing a VPN over both MPLS network 1 and MPLS network 2. The connection for the VPN is assigned to element "W", and "W" is meaningful only in the context of MPLS network 1. The other side of the connection is assigned to element "X", and "X" is meaningful only in the context of MPLS network 2.

NOTE – It is recommended that bandwidth of a connection does not interfere with bandwidth of any other connections. Detailed QoS specifications of the connection are for further study.

12.1.3.3 Mapping of the QoS class

Attributes of a QoS class may be assigned to each connection. This enables provisioning of multiple QoS classes within each VPN. Class Identification in the IP Layer is needed only once.

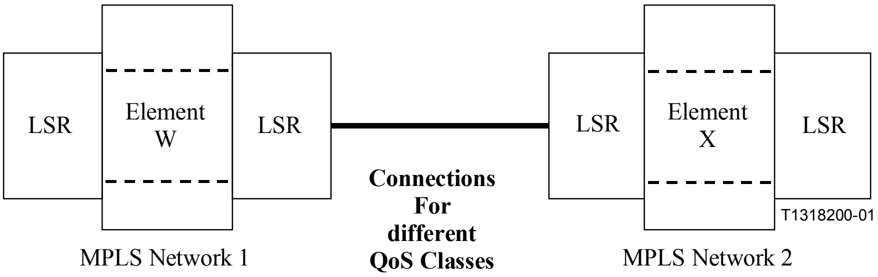

Figure 12/Y.1311.1 – Using multiple connections for multiple QoS classes for each VPN

An alternate method is to use the CoS field, a bit-pattern in a field such as EXP of the Shim header or DSCP (TOS) of the IP header, to identify a QoS class during packet transmission on the connection. The connection is shared by multiple QoS classes. A typical example of this mapping method is DiffServ. This method can reduce the number of connections, while QoS control on the connection is difficult.

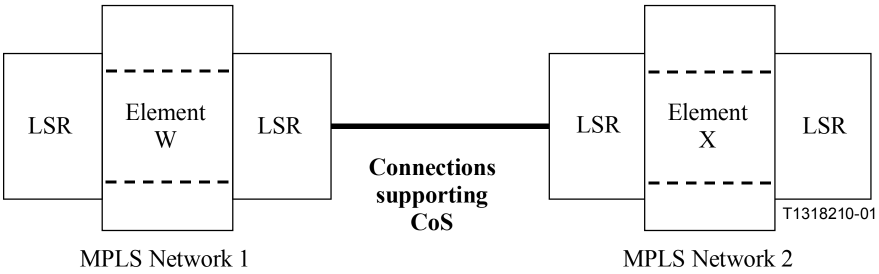

Figure 13/Y.1311.1 – Using CoS on a single connection for supporting multiple QoS classes for each VPN

12.1.3.4 Dynamic routing information distribution

Some mechanisms for routing control per VPN are required in each egress/ingress LSR. The connection between MPLS network 1 and MPLS network 2 of Figure 11 just transmit packets of standard IP routing. Routing information is then forwarded by the functional capability described in 12.1.3.2, as well as data. This enables dynamic routing information distribution within each VPN. Standard routing protocols such as BGP, OSPF, RIP, DVMRP, PIM can be used on the connections for every VPN.

12.1.3.5 Considerations about the scalability of the proposed interworking solution

Figure 14 summarizes the functional capabilities for MPLS VPN interworking via IP over ATM. Note that this solution does not require any new protocols or modification of existing protocols.

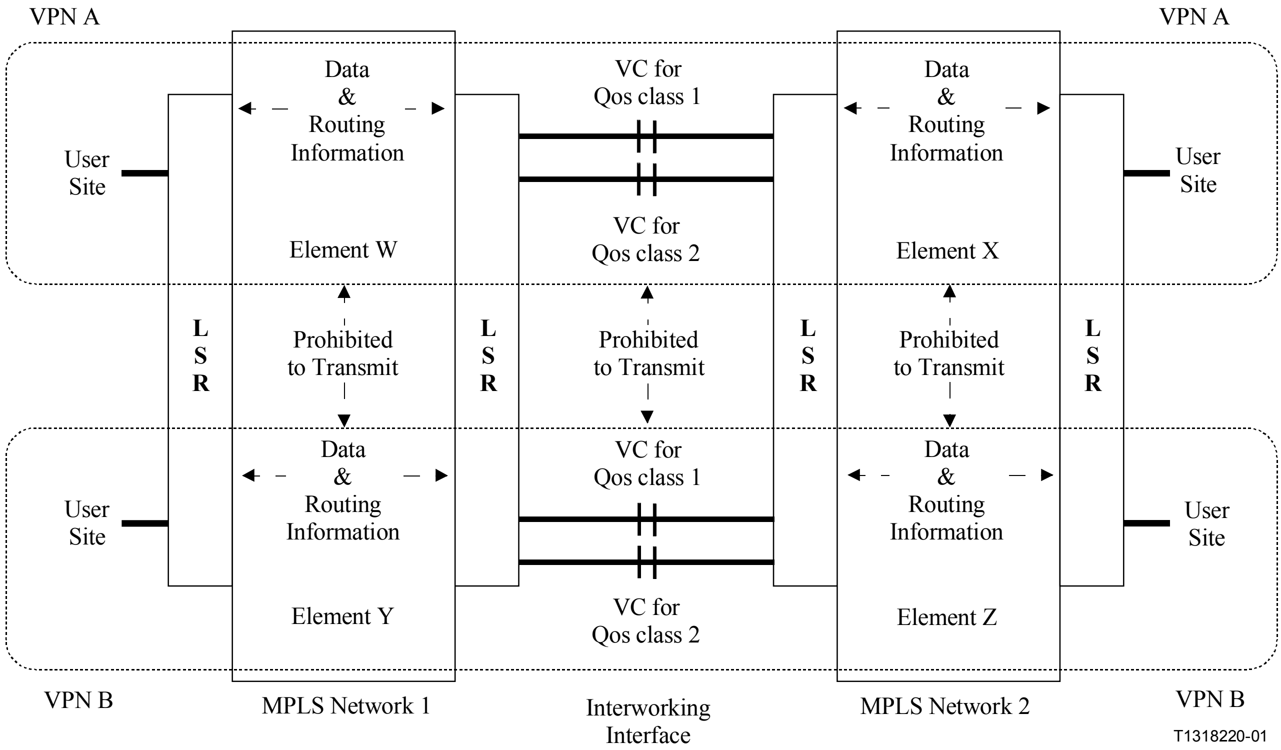

Figure 14/Y.1311.1 – Proposed VPN interworking by using IP over ATM

The solution in clause 12 focuses on static interworking (i.e. user-plane interworking) to deploy quickly. Dynamic interworking (i.e. control-plane or management-plane interworking) should be discussed to reduce manual configuration in the near future, thereby improving scalability.

12.2 Service interworking with other VPN architectures

Service interworking should take the following aspects into consideration:

- data plane interworking;
- control plane interworking;
- management plane interworking.

Appendix I provides informative material on this topic.

ANNEX A

MPLS VPNs over non-MPLS core network infrastructures

This Recommendation addresses the support of IP VPN services over an MPLS architecture which does not require a fully-MPLS network infrastructure.

A generic deployment scenario of not fully-MPLS network infrastructure is presented in Figure A.1.

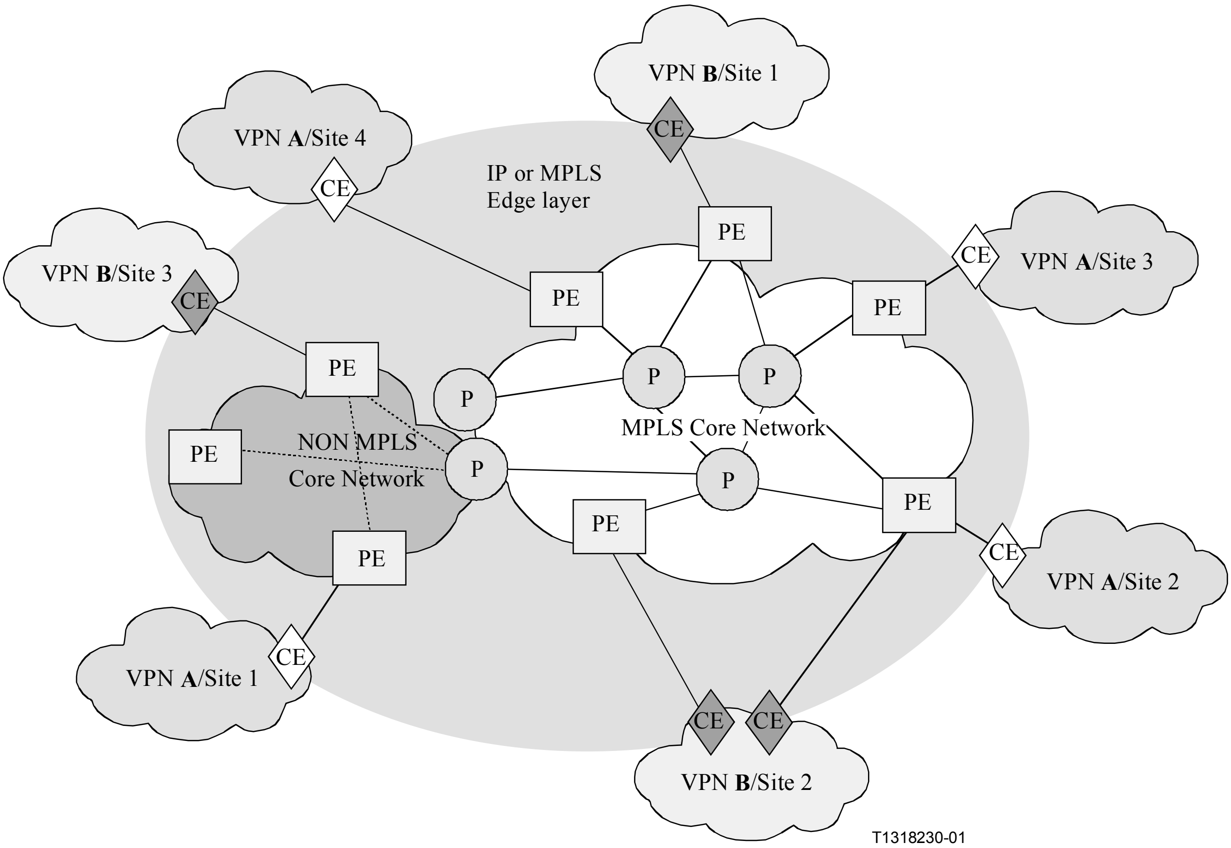

Figure A.1/Y.1311.1 – Not fully-MPLS network infrastructure

An example of a specific deployment scenario in which the non-MPLS portion of the network infrastructure is pure IP, is to use mechanisms such as MPLS-over-GRE or MPLS-over-IP.

NOTE – In the case of not fully-MPLS network infrastructure, specific impacts on ability to meet all the requirements described in this Recommendation will be further studied.

APPENDIX I

Examples of service interworking with other VPN architectures

Interworking should take the following aspects into consideration:

- data plane interworking;
- control plane interworking;
- management plane interworking.

Data plane interworking

In data plane interworking, information in the encapsulation header specific to the VPN architecture of the received packet is mapped to that of transmitted packet to satisfy the service requirement described in clause 7.

Figure I.1 below shows the example of the encapsulation header used by several VPN architectures to identify the VPN users.

VPN architecture	Header	Identifier
MPLS	shim header	Label
VLAN (IEEE802.1Q)	TCI	VLAN ID
IP over ATM	cell header	VPI/VCI
IP over FR	FR header	DLCI
L2TP	L2TP header	Tunnel ID/Session ID

Figure I.1/Y.1311.1 – Example of the headers used by VPNs

Note that the length of the identifier fields for different VPN architectures are not the same, therefore an accurate mapping should be defined.

The information in the encapsulation header and the information in the Layer 3 header (i.e. IP header) have to be mapped to preserve VPN user identification.

For example, mapping the combination of the Identifier in the encapsulation header and the destination IP address in the IP header of the received packet to the Identifier of the transmitted packet may be performed.

Also the QoS class information of a packet can be handed over from end to end. As an example, in case of interworking between MPLS VPN and VLAN (explained later in this appendix), the node may map the user priority in the tag control information to the EXP field in the MPLS shim header (or the appropriate field in a non-shim MPLS header).

Control plane interworking

Routing information specific to each VPN architecture needs to be exchanged between different VPN architectures to realize the mapping of the header information.

Management plane interworking

To enhance interworking, it is desirable that management systems of different VPN architectures are interoperable.

Example of interworking between MPLS VPN architectures and VLAN

The text below in this clause describes the interworking between MPLS VPN and VLAN specified by IEEE802.1Q [9] as an example of the interworking between different VPN architectures.

Figure I.2 shows a network model of the interworking between MPLS VPN and VLAN. VLAN #As are located in physically separated places and mutually connected by the MPLS VPN, and VLAN #Bs are also located in physically separated places and mutually connected by the MPLS VPN in this model.

1) *From VLAN to MPLS*

   The node at the ingress of the MPLS VPN maps the VLAN ID assigned to each VLAN to the MPLS Label to separate the VPN users in the MPLS VPN, and maps the destination IP address prefix to the MPLS Label to route the packet to the appropriate destination.

2) *From MPLS to VLAN*

   The node at the egress of the MPLS VPN maps the MPLS Label to the VLAN ID assigned to each VLAN, and routes the packet to the appropriate destination by seeing the destination IP address.

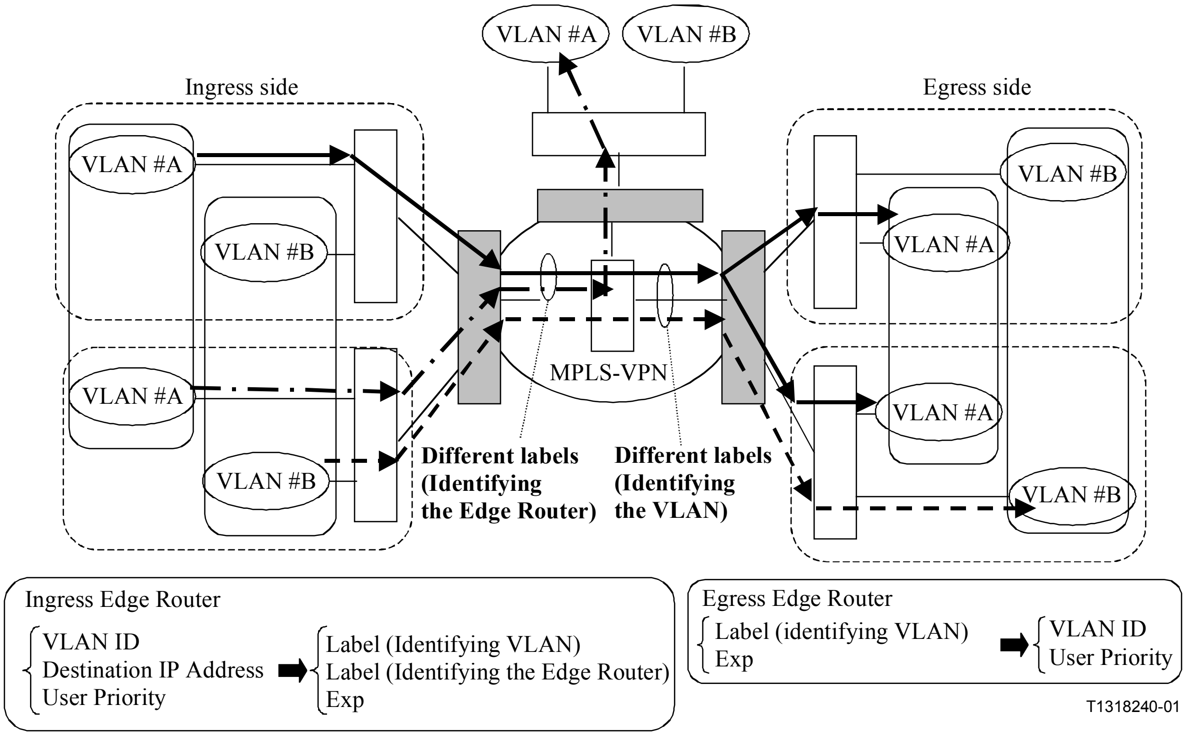

Figure I.2/Y.1311.1 – Network model of interworking between MPLS VPN and VLAN

APPENDIX II

Bibliography

[1] CARUGI (M.) *et al., Service requirements for Provider Provisioned Virtual Private Networks*, work in progress in IETF.

[2] CALLON (R.) *et al., A Framework for Provider Provisioned Virtual Private Networks*, work in progress in IETF.

[3] JACQUENET (C.), *Functional needs for the deployment of an IP VPN service offering: a service provider perspective*, work in progress in IETF.

[4] ROSEN (E.) *et al., BGP/MPLS VPNs* (draft-rosen-rfc2547bis-03.txt), work in progress in IETF.

[5] OULD-BRAHIM (H.) *et al., Network based IP VPN Architecture using Virtual Routers*, work in progress in IETF.

[6] OULD-BRAHIM (H.) *et al., BGP/VPN: VPN Information Discovery for network based VPNs*, work in progress in IETF.

[7] MUTHUKRISHNAN (K.) *et al., A Core MPLS IP VPN architecture*, (draft-muthukrishnan-rfc2917bis-00.txt), work in progress in IETF.

[8] KATHIRVELU (C.) *et al., Hierarchical VPN over MPLS Transport,* work in progress in IETF.

[9] LE FAUCHEUR (F.) *et al., MPLS Support of Differentiated Services*, work in progress in IETF.

[10] SUMIMOTO (J.), SUZUKI (M.), TABATA (O.), ESAKI (Y.), DOUKAI (M.), *MPLS VPN Interworking*, work in progress in IETF.

[11] WORSTER (T.) *et al., MPLS Label Stack Encapsulation in IP*, work in progress in IETF.

[12] GODERIS (D.) *et al., Service Level Specification Semantics and Parameters*, work in progress in IETF.

[13] REKHTER (Y.), TAPPAN (D.), ROSEN (E.), *MPLS Label Stack Encapsulation in GRE*, work in progress in IETF.

[14] LE FAUCHEUR (F.) *et al., Requirements for support of DiffServ-Aware MPLS Traffic Engineering*, work in progress in IETF.

[15] LE FAUCHEUR (F.) *et al., Extensions to IS-IS, OSPF, RSVP and CR-LDP for support of DiffServ-Aware MPLS Traffic engineering*, work in progress in IETF.

[16] BAKER (F.), ITURRALDE (C.), LE FAUCHEUR (F.), DAVIE (B.), *Aggregation of RSVP for IPv4 and IPv6 Reservations*, work in progress in IETF.

[17] AWDUCHE (D.), BERGER (L.), GAN (D.), LI (T.), SWALLOW (G.), SRINIVASAN (V.), *RSVP-TE: Extensions to RSVP for LSP Tunnels*, work in progress in IETF.

[18] JAMOUSSI (B.) *et al., Constraint-Based LSP Setup using LDP*, work in progress in IETF.

[19] HUMMEL (H.), *Tree/Ring/Meshy VPN tunnel systems*, work in progress in IETF.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	**Global information infrastructure and Internet protocol aspects**
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2001