INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Y.1311

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2002)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

Internet protocol aspects – Transport

Network-based VPNs – Generic architecture and service requirements

ITU-T Recommendation Y.1311

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

Network-based VPNs – Generic architecture and service requirements

Summary

This Recommendation specifies the generic architecture and service requirements that are applicable to the provision of Network-Based Virtual Private Networks by Network Service Providers.

Source

ITU-T Recommendation Y.1311 was prepared by ITU-T Study Group 13 (2001-2004) and approved under the WTSA Resolution 1 procedure on 16 March 2002.

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

ITU-T Recommendation Y.1311

Network-based VPNs – Generic architecture and service requirements

1 Scope and field of application

This Recommendation describes a number of generic architectural aspects and specifies a number of generic service requirements involved in the provision of network-based Virtual Private Networks (NB VPNs).

Network-based VPNs have a common set of requirements and are related through the use of a common set of mechanisms. This Recommendation describes NB VPN service definitions, framework and requirements.

The scope of this Recommendation covers the various core implementations of an NB VPN, as well as the services offered to the customer at the access interface.

The scope is also illustrated in Figure 1, which depicts the principles arrangement between services and implementation approaches:

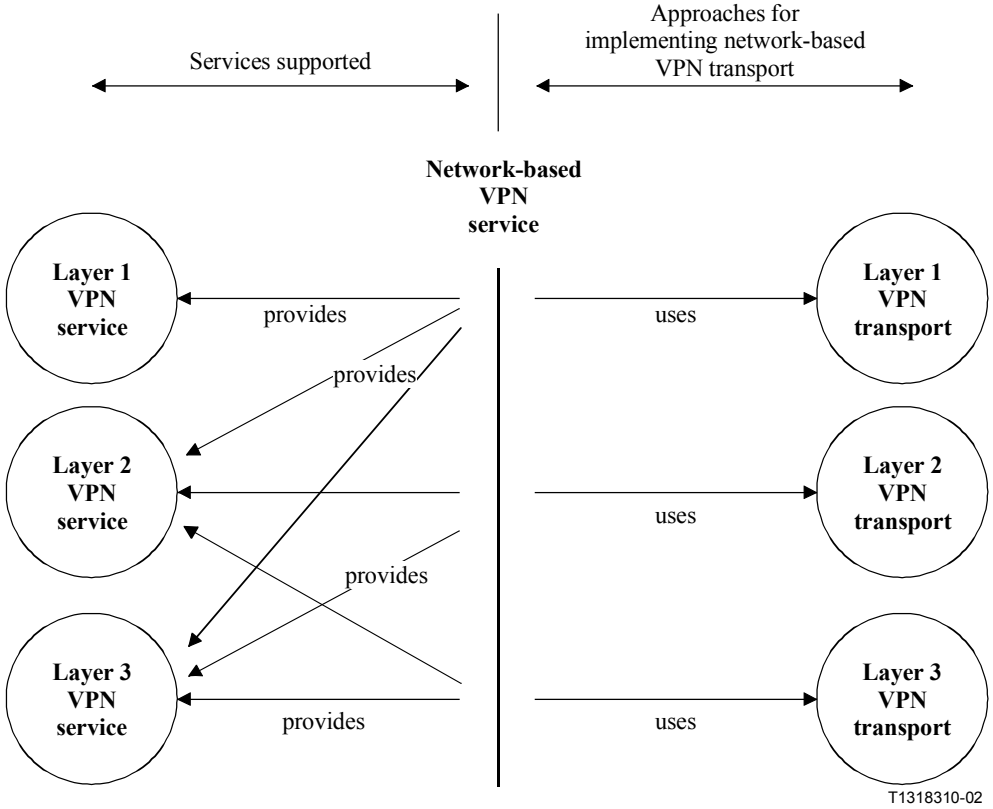


Figure 1/Y.1311 – General Scope

NOTE 1 – The examples shown above are non-exhaustive.

NOTE 2 – Not all combinations of elements shown in the figure are feasible, or are within the scope of this Recommendation.

Further explanation of the concepts shown in Figure 1, are contained in clauses 5 and 6.

2 References

2.1 Normative 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; 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.

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

[2] ITU-T RecommendationY.1311.1 (2001), *Network-based IP VPN over MPLS architecture*.

3 Terms and definitions

This Recommendation defines the following terms.

3.1 Network-based Virtual Private Network (NB VPN)

A network-based virtual private network is that part of a network which provides connectivity amongst a limited and specific subset of the total set of users served by the network provider. A VPN has the appearance of a network that is dedicated specifically to the users within the subset. This dedication is achieved through logical rather than physical means, hence the use of the word virtual. Users within a VPN cannot communicate, via the VPN provider, with users not included in the specific VPN subset and vice versa.

NOTE – The term "network based" is used to distinguish the network provider solutions described in this Recommendation from VPN solutions which are implemented solely through the use of customer equipment based solutions. Whenever the term "VPN" is used in this Recommendation it shall be taken to mean a "network-based VPN".

3.2 NB Layer 1 VPN

A network-based Layer 1 VPN is a NB VPN where the VPN service operates at layer 1 and provides optical or TDM connections between the customer devices belonging to the VPN, i.e. between a port on one customer device and a port on another customer device.

3.2.1 Optical VPN

A network-based optical VPN is a layer 1 VPN that uses optical interconnections between customer devices as the basis for providing the VPN facilities.

3.3 NB Layer 2 VPN

A network-based Layer 2 VPN is a NB VPN where the VPN service operates at layer 2 and provides a data link service between customer devices belonging to the VPN, e.g using IEEE 802, FR or ATM protocols.

3.4 NB Layer 3 VPN

A network-based Layer 3 VPN is a NB VPN where the VPN service operates at layer 3, and provides a layer 3 service between customer devices belonging to the VPN, e.g using IP protocols.

3.4.1 NB IP VPN

A network-based IP VPN is a network-based layer 3 VPN that uses IP addressing, IP forwarding and routing, and the IP protocol for control and data, and IP technology as the basis for providing the VPN facilities.

3.5 Virtual Services Network (VSN)

The Virtual Services Network is an abstract representation of the set of services that can be made available to a customer of an NB VPN. These services include services which enable the control, administration and management of the VPN.

3.6 Virtual Transport Network

The Virtual Transport Network is an abstract representation of the set of forms of implementation of an NB VPN.

4 Abbreviations and Acronyms

This Recommendation uses the following abbreviations.

ATM	Asynchronous Transfer Mode
CE	Customer Edge
FR	Frame Relay
GRE	Generic Routing Encapsulation
IEEE	Institute of Electrical ans Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
MPLS	Multiprotocol Label Switching
NB	Network Based
P	Provider
PE	Provider Edge
PPVPN	Provider Provisioned Virtual Private Network
QoS	Quality of Service
SLA	Service Level Agreement
TDM	Time Division Multiplex
VPN	Virtual Private Network
VSN	Virtual Service Network
VTN	Virtual Transport Network

5 Service definition

5.1 Introduction

This clause provides a generic functional definition of a "Network-based VPN" network service. Implementation issues as well as implementation-specific service aspects are out of scope of this part of Recommendation.

5.1.1 Types of VPN service

The following three types of service are identified.

5.1.1.1 Layer 1 VPN service

In a layer 1 VPN service the customer edge device is connected to the network provider via one or more links, where each link may consist of one or more channels or sub-channels (e.g. wavelength, or wavelength and timeslot respectively, or just timeslot). The customer edge device and the provider edge device are peered to each other only at the physical link layer across the access network.

A link has two end-points:

a) one on the customer edge (CE) device, known as the port;

b) one on the provider edge device , known as the provider edge (PE) port.

The scope of a layer 1 service is related to port-based VPNs only.

5.1.1.2 Layer 2 VPN service

In a layer 2 VPN service, customer edge device receives data link layer (i.e. layer 2) service from the network provider. The customer edge device and the provider edge device are peered to each other at the data link layer across the access network. The network performs forwarding of user data packets based on information in the packets' data link layer headers, such as a for example frame relay DLCI, ATM VCC, or 802.1q VLAN tag.

5.1.1.3 Layer 3 VPN service

In a layer 3 VPN service, customer edge device receives network layer service (typically in the form of IP packets) from the network provider. The customer edge device and the provider edge device are peered to each other at the network layer across the access network. The network performs forwarding of user data packets based on information in the IP layer header, such as an IPv4 or IPv6 destination address. The customer sees the network as a layer 3 device such as an IPv4 or IPv6 router.

5.1.2 NB VPN service view

Figure 2 depicts the service view for three instances of the NB VPN service, illustrating different various applications.

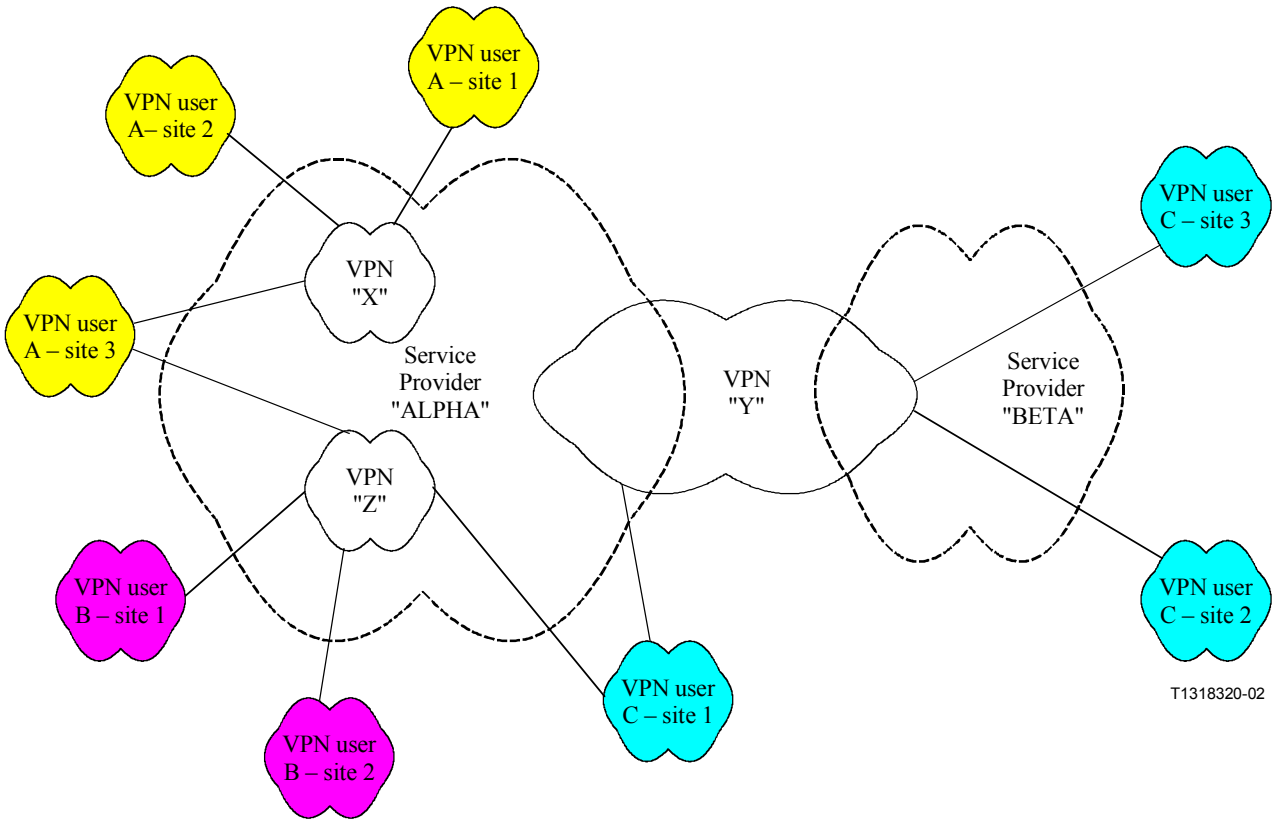


Figure 2/Y.1311 – NB VPN service view

5.1.3 NB VPN service deployment scenarios

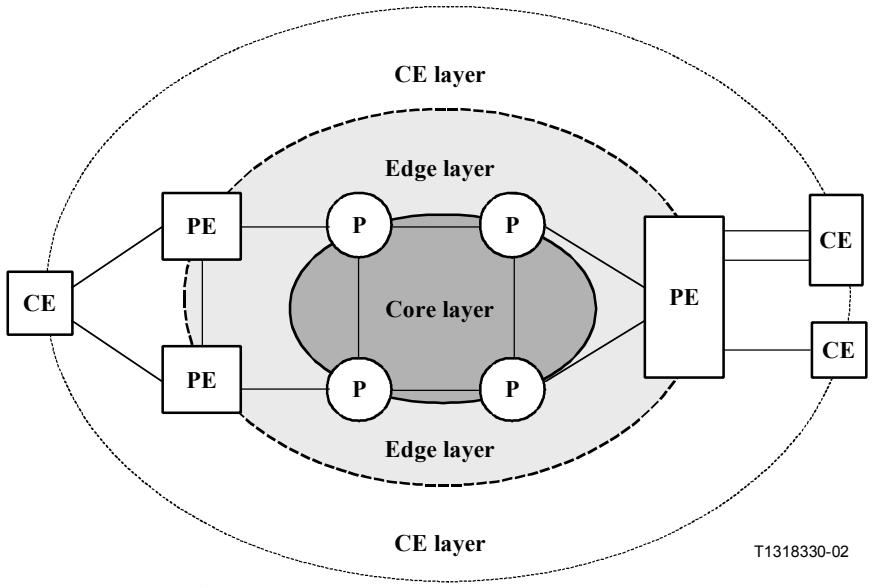
A number of generic service deployment scenarios are envisaged for Network-Based VPNs. Scenarios for layer 3, 2, and 1 VPNs are described in further detail in Appendices I, II and III respectively.

It should be noted that these are some of the more commonly envisaged deployment scenarios, and not necessarily an all-encompassing list of the scenarios to be supported by network-based VPN services. In other words, a service provider may provide an VPN service supporting a subset or a superset of the above scenarios based on customer requirements and constrained by technical or other limitations.

5.2 NB VPN service reference model

5.2.1 Designation of VPN network elements

The generic VPN reference model for a VPN is shown in Figure 3 below.



CE Customer Edge
PE Provider Edge
P Provider

Figure 3/Y.1311 – VPN reference model

For ease of provision of a VPN, by a network provider, it is essential to accommodate addition, deletion, moves and/or changes among sites and members with as little manual intervention as possible. A key enabler of VPN provision is the establishment of the "tunnels" which separate the traffic of a given VPN from that of another VPN, and from traffic of the open network across a common infrastructure. If key VPN network elements can announce their presence to one another through auto-discovery techniques, then the required tunnels can be configured with a minimum of manual intervention. The principle of auto-discovery applies to all types of VPN irrespective of the layer at which the service is offered. For example, the CE-PE peer relationship established for the VPN service may occur at layer 1, 2, or 3.

The tunnels for VPN between PE devices across the core may be constructed at layer 1, or layer 2 or layer 3. Examples of layer 1 tunnels are optical or TDM paths. Examples of layer 2 tunnels are ATM, MPLS, or IEEE 802.2 paths. Examples of layer 3 tunnels are IP paths (based on a variety of IP-based protocol mechanisms).

NOTE – The VPN layer service offered to the CE by the PE may operate at a layer that is different from that used by the tunnelling technique between the PEs. In the case where the required CE-CE layer service is different from the PE-PE layer service, emulation and/or encapsulation techniques will be used by the PEs to resolve the difference.

The PE is the device within the provider network that offers the VPN service to the customer. The CE is the device which provides the interface to the customer domain. Each CE may be the ingress/egress device for a subtending set of addressable/reachable VPN customer end-points within a given geographic area within the customer domain. Such a geographic area is sometimes referred to as a site. Connectivity between CEs and PEs may be provided in a number of different ways. For example, a given CE may be connected to one or more PEs, and a given PE may be connected to one or more CEs that may or may not belong to the same site or same VPN.

The P device is the routing or switching device within core infrastructure that interconnects PEs. P devices have little (if any) knowledge about the existence of VPNs.

5.2.2 Auto-discovery among network elements

The degree of auto-discovery among networks elements will vary according to technical implementation and administrative decisions. In theory, the principle of auto-discovery can be applied to the following three cases.

5.2.2.1 PE-PE discovery

Whereby PEs of a given VPN learn of each others existence, and establish appropriate configuration management information.

5.2.2.2 CE-PE discovery

Whereby PEs of a given VPN learn of CEs of a given VPN, and establish appropriate configuration management information.

5.2.2.3 CE-CE discovery

Whereby CEs of a given VPN learn of each others existence and subtending addresses served, and establish appropriate configuration management information.

6 Abstract framework of NB VPN

6.1 Operational environment

It is vital that network operators:

a) be able to quickly respond to a variety of customer service requirements;

b) be able to exploit a variety of technologies within the network as means of realization of the required services.

These two requirements can be met by decoupling the internal means of service delivery from the service delivered at the service delivery point. Such an arrangement provides network operators with:

c) an agile evolutionary path;

d) a flexibility point to facilitate the mixing and matching between access and core technologies;

e) a means of accommodating legacy systems;

f) identifiable points at which interworking may occur.

Since either the service itself or the technology may not be homogenous from end-to-end, we may consider both the service and the technology as comprising a virtual service and a virtual transport network. Additionally, the VPN has the appearance and characteristics of a network dedicated to a given customer. The service and transport technology perceived by the end user(s) may not be the same throughout all constituent network components from end-to-end. Instead, they may be simulated or emulated by other means and which can therefore be regarded as virtual.

Generically, these concepts can be illustrated by a high level of abstraction as shown in Figure 4 below. This model allows the definition of the generic service requirements in a technology-independent manner.

In most cases, for a given VPN the same service would be provided end-to-end, at each CE., e.g. IP to IP or FR to FR. However, interworking arrangements could facilitate having different services at each end, within some constraints (such as ATM to FR for example).

6.2 VSN/VTN overview

6.2.1 General model

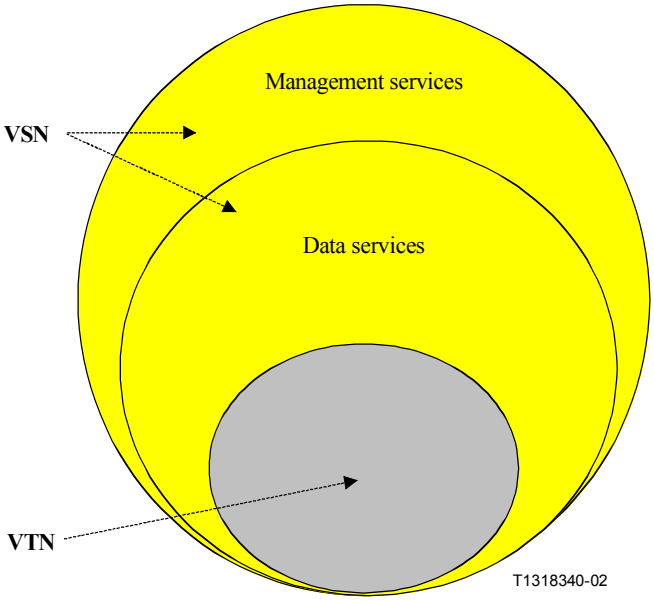


Figure 4/Y.1311 – VSN/VTN Model

6.2.2 VSN and VTN components

The VPN is considered to be comprised of the VSN and the VTN components.

The VSN comprises a number of service delivery platforms, which deliver services to the carrier's customer. The service delivery environment includes the network and policy management elements that facilitate personalization and customization capabilities for both customers and applications.

The VSN component will offer one or more of the following carrier managed services:

- Managed Layer 1 Services.
- Managed Layer 2 Services.
- Managed Layer 3 Services (Internet Access, Intranet Services, Extranet Services).
- Managed Remote Access Services.
- Managed Security Services.

The VTN is the transport infrastructure itself, viewed as the virtualization of the carrier backbone.

The provision and nature of a VPN requires the separation and isolation of said VPN traffic from the traffic of other VPNs and from the public traffic. These requirements necessitate some form of tunnelling mechanism, where the data payload formats and/or addressing used within a given VPN is unrelated to those used to convey the tunnelled data across the backbone.

The VTN component will offer one or more of the following carrier managed transports:

- Backbone Virtualization:
  - Transport for VSN at Layer 1 , 2, or 3.
- Access Virtualization:
  - Subscriber Access into VSN at layer 1, 2, or 3.

VTN approaches for particular VPN types are described in other Recommendations on NB VPNs in the Y.1311 series.

6.3 VPN management

An important aspect of a VPN is its management. In addition to the transport connectivity provided by the VPN itself, the service provider will need to provide network-based services to the user, in order to facilitate administration, control and general management of the VPN. Management services may include among others:

a) configuration management of the VPN;

b) performance management of the VPN;

c) fault management of the VPN;

d) accounting management of the VPN;

e) security management of the VPN.

Management services may be distributed within the provider's network, and thus belong to virtual services network (VSN), as shown in Figure 5.

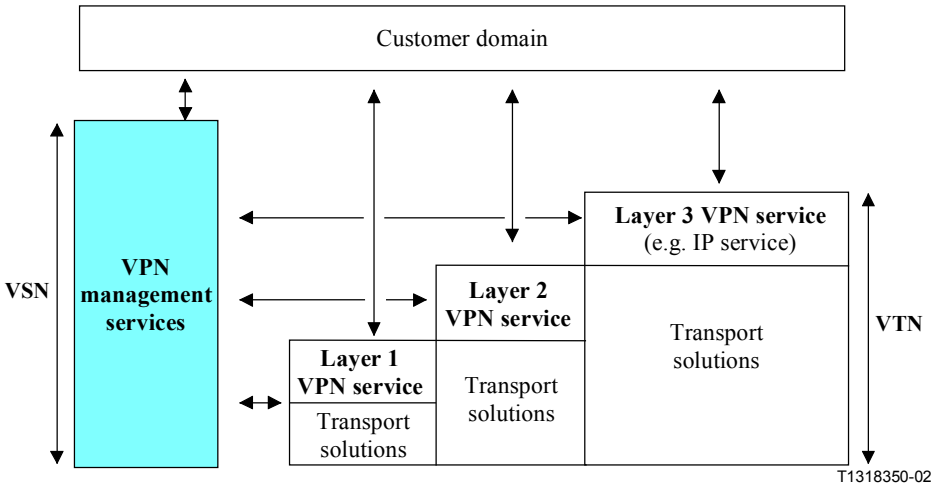


Figure 5/Y.1311 – VSN/VTN model – management services

7 Service requirements

As described in clause 6, an NB VPN can be modelled as being composed of a Virtual Services Network and a Virtual Transport Network. Both these components can be regarded as having identifiable service requirements, representing the user aspects and the network operator aspects respectively.

7.1 Service requirements for virtual services network

The following subclauses outline the VSN service requirements.

7.1.1 General VSN service requirements

- means for user to define VPN membership;
- accommodation of user-defined VPN address schemes;
- transparency to user data;
- means for single customer site to belong concurrently to more than one VPN;
- provision for arbitrary user defined VPN topologies (ranging, for example, from hub-and-spoke, partial mesh to full mesh);
- provision for multi-protocol support;
- provision of multi-homed user sites;

- support for fixed and mobile users;
- provision of standards-based interfaces (independent of user's supplier of device);
- support for wide range of routing protocols between CE and PE routers;
- means to support a variety of user's traffic (QoS) requirements as defined by the user;
- means of supporting different modes of communication such as any-to-any (1:1), multicast (1:N, M:N), and broadcast (1:All);
- means to offer, support and maintain agreed levels of service (e.g. via Service Level Agreements);
- means to meet user's security requirements;
- provision of VPN members with secure dynamic access to VPN (e.g. via dial-up);
- provision of appropriate VPN management services (e.g. configuration, fault, performance, security, etc.);
- accommodation for growth of given VPN or number of VPNs.

7.1.2 Configuration management

- use of user-defined service templates to capture VPN site and route characteristics;
- consistency and coherence verification of user configuration information;
- ability to easily change topology;
- ability to easily add, remove or change devices, sites, routes, traffic, etc.;
- ability to accommodate growth requirements for devices, sites, routes, traffic, etc.

7.1.3 Fault management

- information to customer in event of service disruption and restoration;
- dynamic "hidden" recovery (non-disruptive) as far as possible;
- provision of relevant incident reports and summaries.

7.1.4 Performance management

- maintenance of performance consistent with Service Level Agreements (SLAs);
- provision of performance information, statistics, etc.;
- ability to demonstrate performance to customer;
- prediction of trends, likely problems and/or recommendations in relation to current SLAs, traffic patterns, QoS, etc.

7.1.5 Accounting

- provision to customer/users of itemized bills;
- customized breakdown of billing information;
- correlation to QoS and/or Service Level Agreements;
- correlation to performance and fault management information.

7.1.6 Security

- access control;
- authentication;
- data privacy.

7.1.7 Service Level Agreements and QoS

- Service Level Agreements, per VPN and/or per VPN site, and/or per VPN route should include:
  - Service Level Objectives comprising some or all of:
    - Data 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 Rec. Y.1241.

7.2 Service requirements for virtual transport network

The following subclauses outline the VTN service requirements.

7.2.1 General service provision

- means of assigning globally unique VPN identifier to each VPN;
- means of VPN membership determination;
- ability to accommodate overlapping address space(s) amongst VPNs;
- ability to learn stub link reachability information from user site and disseminate to appropriate peer edge routers;
- means of distribution of intra-VPN reachability information;
- means to construct tunnels to other devices required to support a given VPN;
- accommodate VPNs spanning multiple provider networks;
- use of standards-based interfaces for intra-VPN interoperability;
- use of scalyable solutions to permit growth of given VPN or number of VPNs;

- means to detect loop traffic in a given VPN;
- means to prevent loop traffic in a given VPN;
- means to mitigate loop traffic in a given VPN.

7.2.2 Configuration management

- automatic derivation of configuration information from user information;
- automated configuration of network facilities;
- use of auto-discovery mechanisms for user's external reachability;
- use of auto-discovery mechanisms for intra-VPN reachability;
- comparison with SLAs.

7.2.3 Fault management

- automatic detection of faults (via alarms, incident reports, events, threshold violations of QoS and SLAs, etc.);
- automatic fault localization (via analysis of alarms, reports, diagnoses, etc.);
- provision of fault information to customer;
- incident recording, logs (creation and tracking of trouble tickets);
- automated corrective action (for re-establishment of required traffic, routing, resources, etc.);
- comparison with SLAs.

7.2.4 Performance management

- automatic monitoring of VPN behaviour, including:
  - real-time performance measurements;
  - real-time monitoring of resources and VPN elements status.
- activation of monitoring mechanisms and metrics appropriate to SLA and QoS requirements;
- analysis of information (e.g. bandwidth, response time, availability, packet loss, etc.);
- evaluation of performance in relation to Service Level Agreements (SLAs);
- production of statistics and trends based on collected information;
- analyse of performance information for use in customer reports.

7.2.5 Accounting

- measurement of utilization of various applicable resources;
- quota/SLA utilizations (accumulated consumption, authorizations, etc.);
- long-term storage of accounting information (file creation/administration);
- parameterized processing of accounting information to produce customer defined billing itemization;
- means to correlate accounting information with fault and performance management information;
- comparison with SLAs.

7.2.6 Security

- mechanisms for controlling access to the VPN;
- mechanisms for authentication of users accessing VPN;
- mechanisms for ensuring the privacy of data being transported by the VPN;

- comparison with SLAs.

Appendix I

Service deployment scenarios for NB IP VPN

Introduction

This appendix outlines some important generic service deployment scenarios (irrespective of the underlying transport mechanism used in the service provider network). The following generic ones are envisioned for network-based IP VPN services:

– Intranet (connectivity between sites in the same organization).

– Extranet (connectivity between sites across multiple organizations).

– VPNs across multiple Autonomous Systems or Service Providers.

– Simultaneous VPN and Internet access.

– Hierarchical VPNs (VPNs within VPNs).

– Multiple Remote Access Scenarios (Dial, DSL, fixed wireless, cable).

I.1 Intranet (connectivity between sites in the same organization)

This is the simplest and most common scenario. In this scenario, a VPN is formed between different sites belonging to the same organization. For example, this scenario could be envisioned as one where different branch offices are interconnected and/or also connect to the headquarters. This is the minimum/mandatory scenario that needs to be supported by any VPN architecture. This scenario is described in detail in various clauses of this Recommendation. In Figure I.1, customer sites connect to the service provider edge (PE) device via a customer edge device (CE). This connection can be of various types (e.g. static route, via a routing protocol, an ATM VC, or any dedicated access mechanism like DSL, cable modem or fixed wireless). Tunnels are constructed across the service provider core network. The tunnelling mechanism is specific to the VPN architecture used to construct the VPN (as described in this Recommendation and in ITU-T Rec. Y.1311.1). The tunnels can be either separate on a per-VPN basis as shown in Figure I.1, or they can be common between multiple VPNs, with some kind of a multiplexing functionality to separate traffic between different VPNs. It is also possible (not shown in Figure I.1) that a single customer site may belong to multiple VPNs.

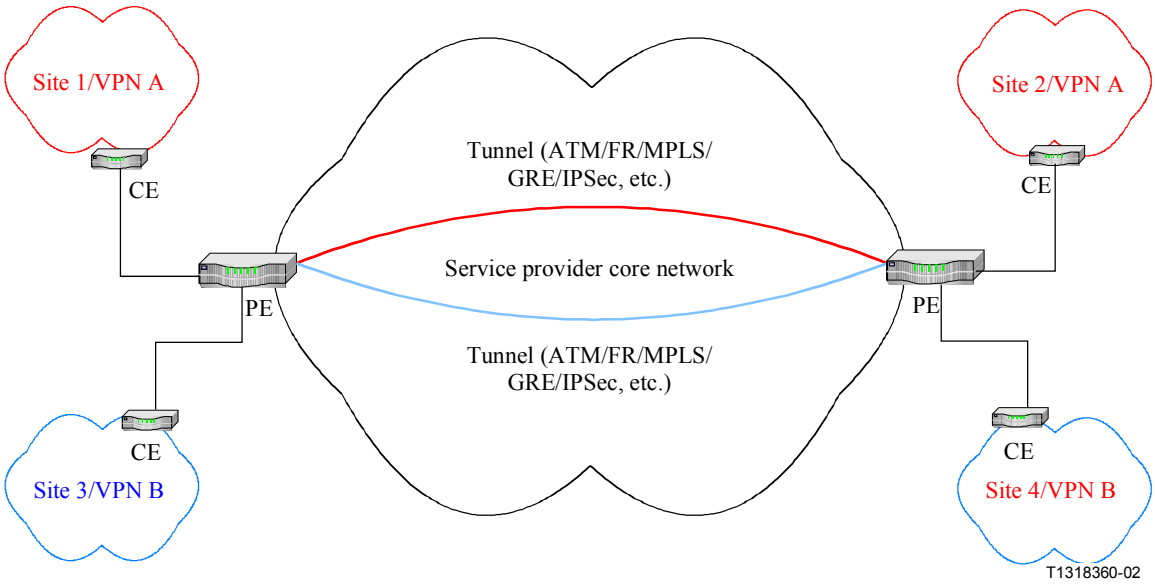


Figure I.1/Y.1311 – Example Intranet scenario

I.2 Extranet (connectivity between sites across multiple organizations)

In an extranet scenario, two or more organizations have access to a limited number of each other's sites. Examples of an extranet scenario include multiple companies cooperating in joint software development, a service provider having access to information from the vendors' corporate sites, different companies and universities participating in a consortium, etc. An extranet can exist across a single service provider backbone or across multiple backbones or autonomous systems. The case of multiple backbones or autonomous systems is examined in scenario 3. The main difference between an extranet and an intranet is the existence of some kind of an access control mechanism at the interconnection between different organizations. This access control can be implemented by a firewall, access lists on routers or similar mechanisms to apply policy-based access control to transit traffic. The access control mechanism may be achieved using separate devices or may be integrated into the PE device. This scenario is illustrated in Figure I.2. In this example, two VPNs are formed connecting Company X and Company Y. The access control mechanism used between the two companies is a firewall (although any other suitable access control mechanism may be used). Additional authentication mechanisms like exchanging a certificate authority may also be used as desired. Again, it is possible that a site belongs to multiple VPNs, which may include one intranet and another extranet. These sub-scenarios also need to be dealt with appropriately while developing a VPN architecture.

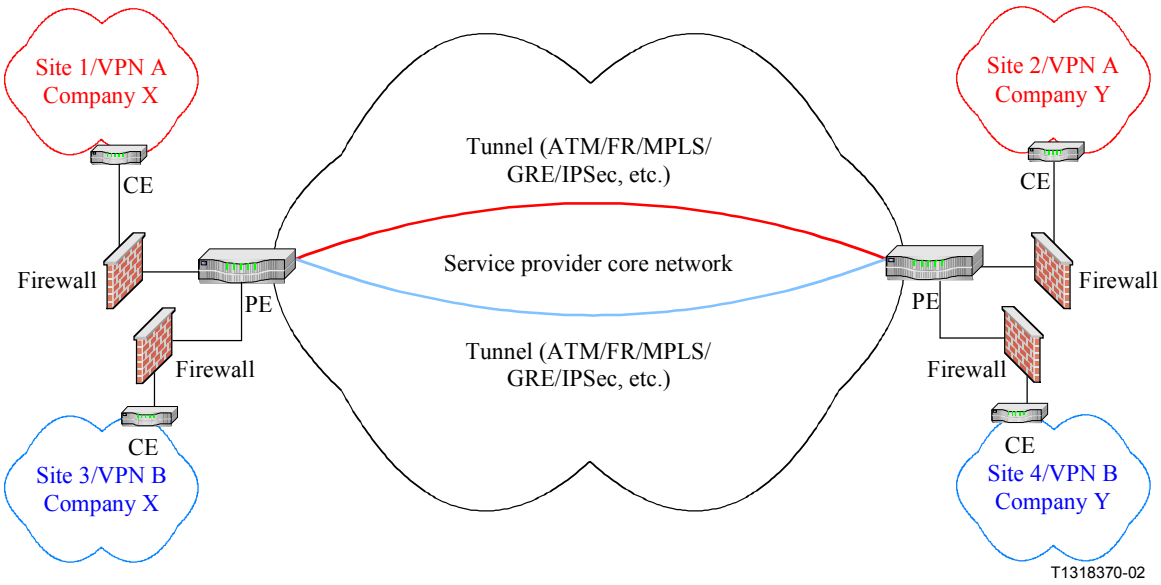


Figure I.2/Y.1311 – Example Extranet scenario

I.3 VPNs across multiple autonomous systems or service providers

In this scenario, a single VPN may extend across two or more service provider networks or Autonomous Systems (ASs). This discussion will describe the scenario where multiple ASs are involved, since it is a more general case. The main connectivity issues in such a case are the communication and security between the PE devices belonging to different ASs. Communication between PEs across ASs may be achieved in a variety of ways, depending on the architectural approach used to construct the network-based IP VPN. The security issue between PEs belonging to different ASs may be resolved using PE-PE tunnels (e.g. IPSec tunnels may be used to provide encryption across ASs). VPN route distribution across ASs should be performed in such a way that it appears as if there is a single tunnel from the ingress PE in one AS to the egress PE in another AS. Specific solutions for this scenario are addressed in this Recommendation and in ITU-T Rec. Y.1311.1. This scenario is illustrated in Figure I.3. The dashed lines shown in Figure I.3/Y.1311 illustrate how an ingress-PE-to-egress-PE tunnel "appears" when inter-AS communication is achieved properly. It should further be noted that one of the pre-conditions for such a VPN to be constructed is the existence of a trust agreement between the service providers involved. Another consideration to be made in this model is the overall scalability of the system, especially if a protocol like EBGP is used for inter-AS communication. A scalable alternative is the use of BGP route reflectors to reduce the number of EBGP sessions between PE devices.

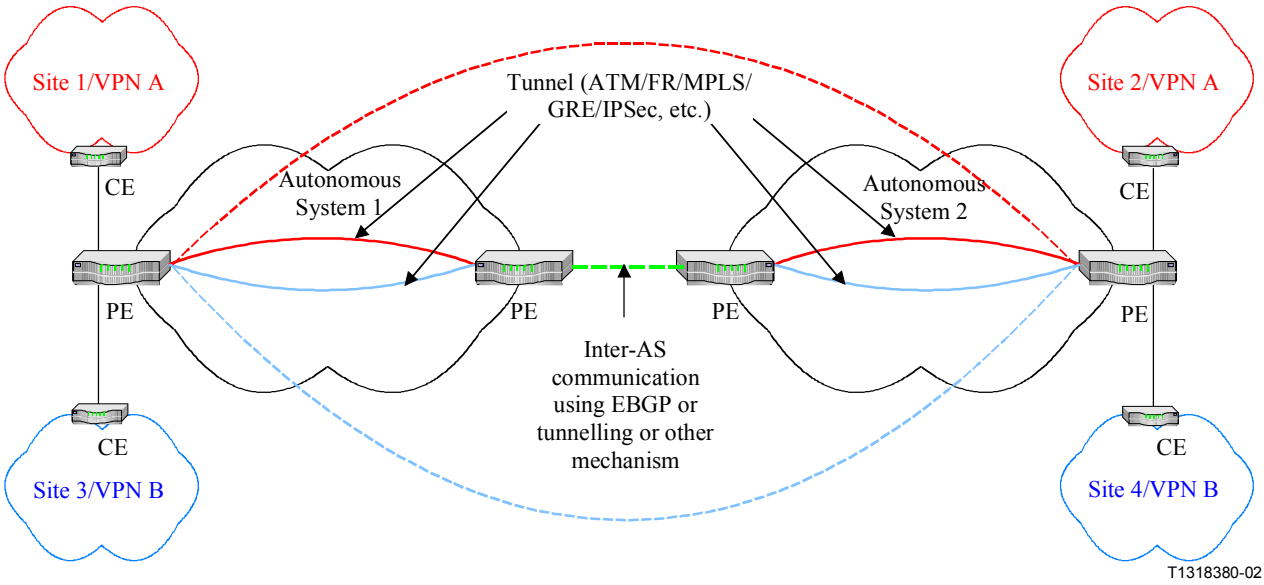


Figure I.3/Y.1311 – VPNs across multiple autonomous systems

I.4 Simultaneous VPN and Internet access

An important scenario for a VPN service is to provide simultaneous access to the global Internet from any site that belongs to any VPN. This can be achieved in a number of ways, again, depending on the VPN mechanism used. If the PE device is composed of virtual routers, then it is possible to access the Internet by means of a dedicated "global" virtual router within the PE device. A network address translation (NAT) or similar mechanism may then be required either at the CE or within the PE device in order to be able to distinguish private VPN addresses from global Internet addresses. If the PE device does not employ virtual routers, non-VPN (Internet) traffic may be directed by means of a default route to an Internet Gateway (Figure I.4). This default route is distributed to all sites within a VPN to provide Internet access to all the sites. Traffic from the Internet to particular sites within VPNs has to be handled properly by ISPs, by distributing to the Internet routes leading to sites within VPNs. The internal structure of the VPN would be invisible to the Internet. A firewall function may be required to restrict access to the VPN from the Internet. An illustration for simultaneous VPN and Internet access is shown in Figure I.4. Specific mechanisms for simultaneous Internet and VPN access are not shown in the figure.

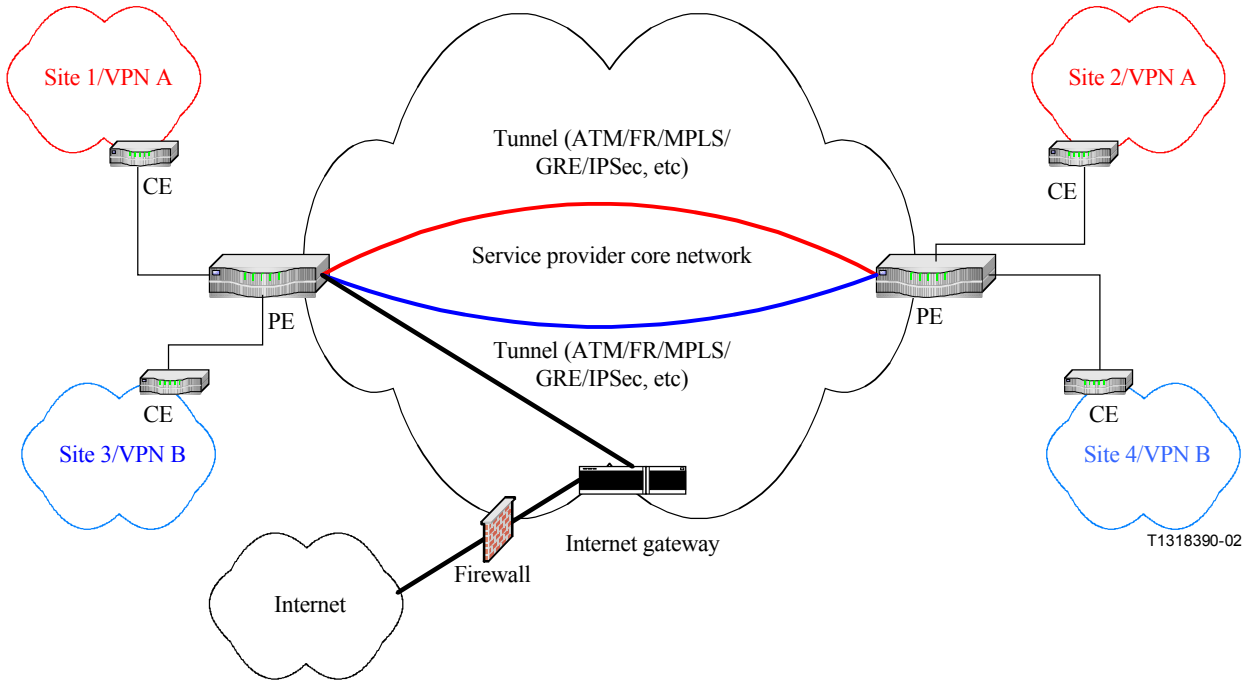


Figure I.4/Y.1311 – Simultaneous VPN and Internet access

I.5 Hierarchical VPNs (VPNs within VPNs)

In this scenario, a service provider offering VPN services may actually be a customer of a larger service provider. Such a service provider network may be envisioned as a large VPN with multiple smaller VPNs within it. For the sake of simplicity, such a service provider network may be called a Level-1 VPN. Similarly, the VPNs within this service provider network may be called a Level-2 VPN. This scenario is illustrated in Figure I.5. The CE and PE devices at Level 1 and 2 are labelled appropriately. From Figure I.5, it is clear that the PE device of the Level-2 VPN (PE2) is the CE device for the Level-1 VPN (CE1). It can also be observed that, in order to provide a network-based IP VPN service at Level-2, the Level-1 VPN would essentially be a CPE-based VPN, because of the establishment of an end-to-end tunnel between the CE1 (i.e. same as PE2) devices. The logical tunnels of the Level-2 VPN are shown as dotted lines, while the solid lines represent the actual CE1-to-CE1 (i.e. PE2-to-PE2) tunnels across the large service provider network. Thus, the CE devices of the Level-1 VPN need to be involved in the VPN establishment mechanism. The large service provider would essentially be a carrier's carrier.

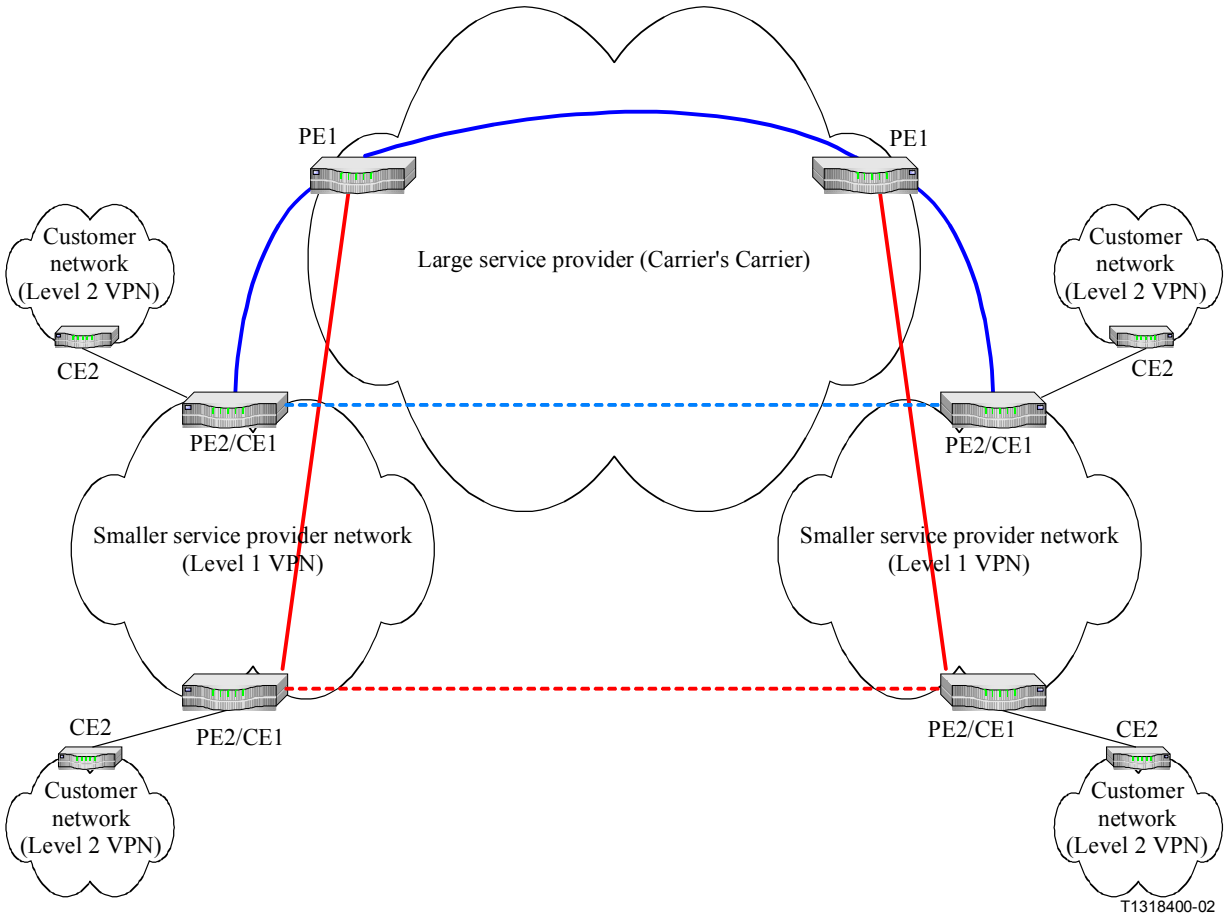
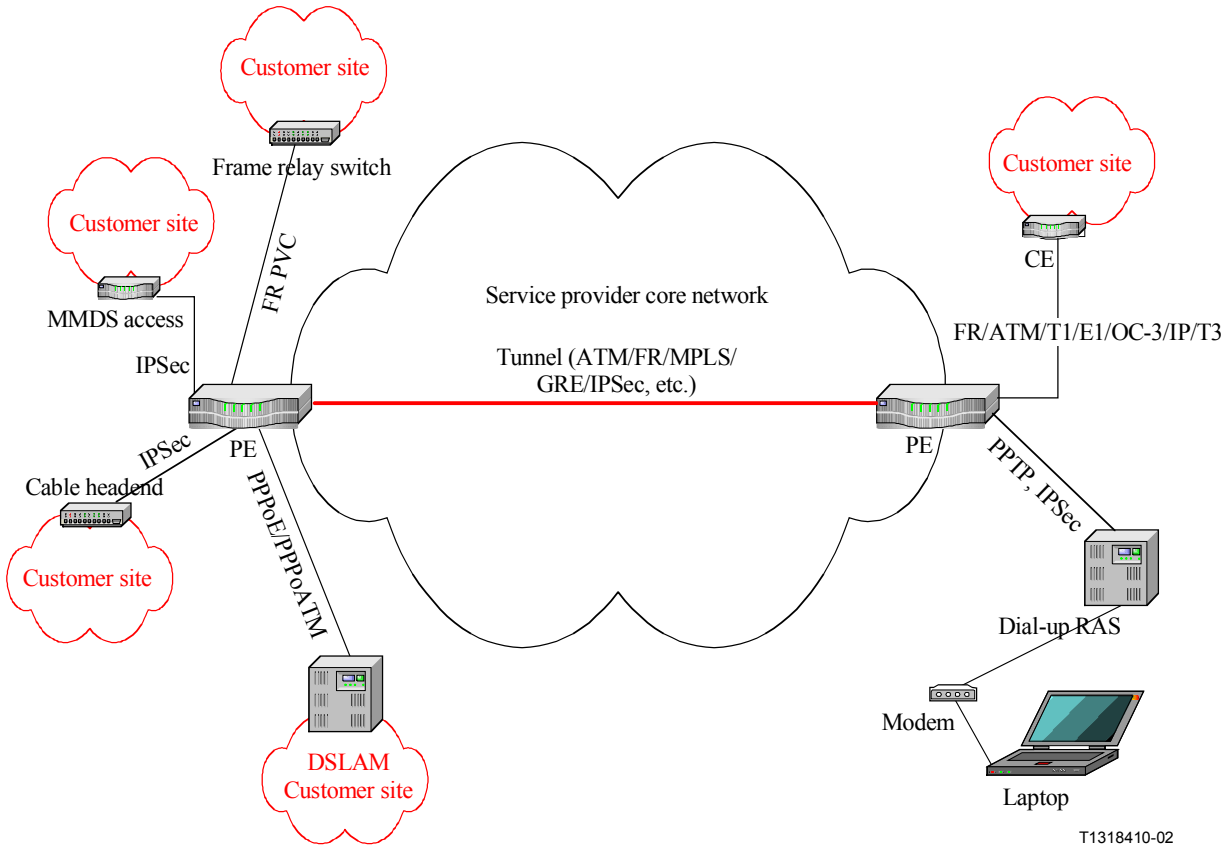


Figure I.5/Y.1311 – Hierarchical VPNs

I.6 Multiple Access Scenarios (Dial, DSL, fixed wireless, cable)

In addition to all the above scenarios, the network-based IP VPN should also support multiple access scenarios. Both dedicated access (for example, by a static route, an ATM PVC, using routing protocols, xDSL, cable modem, fixed wireless, etc.) and dial access should be supported. Appropriate devices for terminating different kinds of access mechanisms may be used, or the required functionality may be integrated into the PE devices. An illustration of a network-based IP VPN with support for various access mechanisms is shown in Figure I.6.



DSLAM Digital Subscriber Line Access Multiplexer

Figure I.6/Y.1311 – Multiple access scenarios

Appendix II

Service deployment scenarios for NB Layer 2 VPN

For further study.

Appendix III

Service deployment scenarios for NB Layer 1 VPN

For further study.

Appendix IV

Examples of practical realizations of VTN approaches for NB IP VPN

Network-based VPNs (including NB IP VPN) may be achieved over different base architectures as already indicated in Figure 1.

A practical realization of the framework network architecture illustrating the concepts in more depth is given in Figure IV.1 below. There are a number of types of network architecture transport

on which to accommodate VPNs. An MPLS based architecture may be used to support MPLS tunnels and an ATM or Frame Relay architecture may be used to support virtual ATM or Frame Relay connections. IP VPN services may be overlaid on either of these network architectures. In addition, non IP services can also be overlaid on either of these network architectures.

One example approach to the implementation of generic Network-Based IP VPN is included in Figure IV.1. The node includes a Virtual Router (VR) architecture, which in turn provides access to an MPLS tunnel for implementation of IP VPNs using BGP or to an IPSec tunnel. BGP may also be implemented over MPLS tunnels without using a VR.

The node containing the VR architecture may be accessed from the customer side, via an access network, by ATM, Frame Relay, X.25, SDH or possibly other access arrangements.

The figure shows other approaches to realization.

IP services are supported on the network node through functions of storage, retrieval and transaction processing. Examples of IP services shown in the figure include address translation, authentication, admission control.

The VSN/VTN model described in clauses 6.2 and 6.3 can be overlaid on the practical realization, to show the relationship to the VSN/VTN concepts as shown in Figure IV.1.

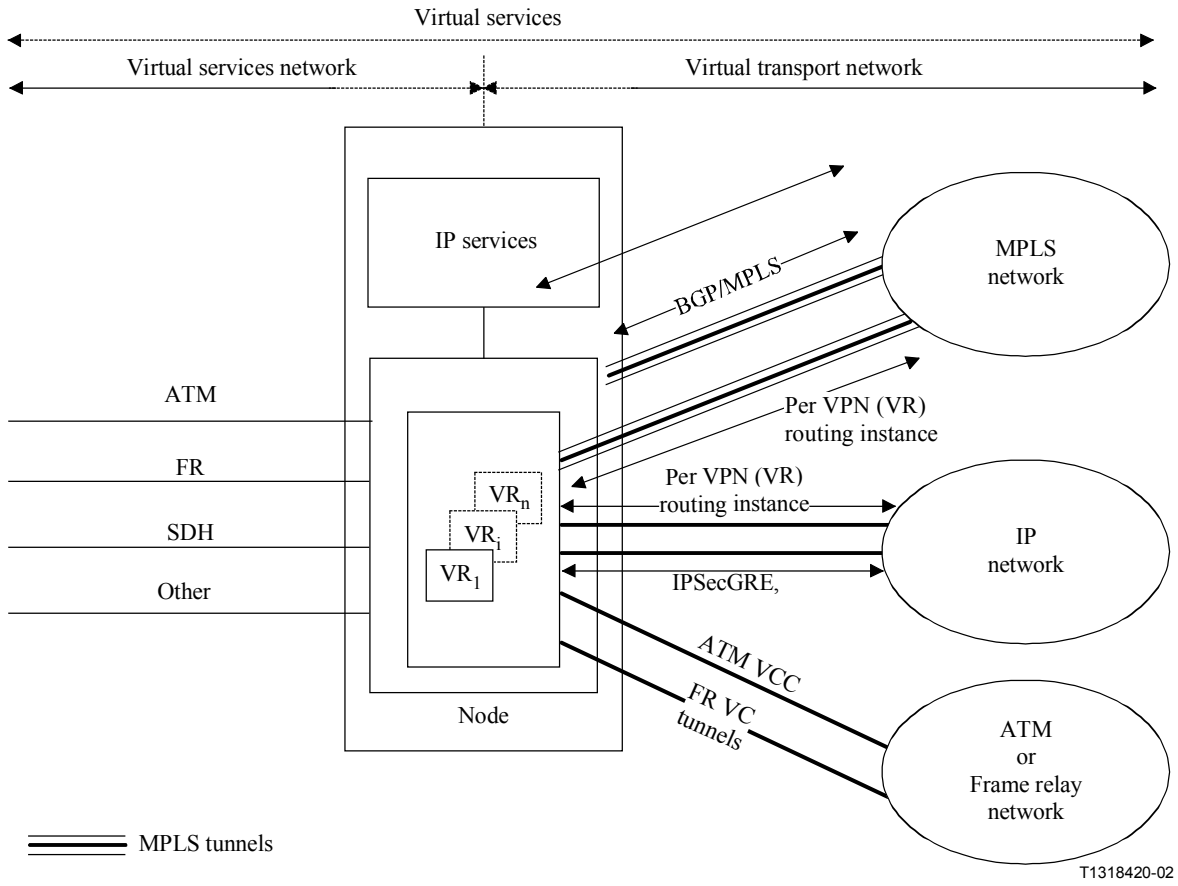


Figure IV.1/Y.1311 – Examples of practical realization of VTN approaches

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, 2002