

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1314

(10/2005)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS
AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Transport

Virtual private network functional decomposition

ITU-T Recommendation Y.1314



International
Telecommunication
Union

Document Sharing Hub

ITU-T Y-SERIES RECOMMENDATIONS
GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-
GENERATION NETWORKS

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

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

ITU-T Recommendation Y.1314

Virtual private network functional decomposition

Summary

This Recommendation describes the set of functions required to establish, operate and maintain client/server and peer level Virtual Private Networks (VPNs). The network functionality is described from a network level viewpoint, taking into account the VPN network layered structure, client characteristic information, client/server associations, networking topology and layer network functionality.

The functional models are described using the modelling methodology described in ITU-T Recs G.805 and G.809. The modelling methodology employed is network technology-independent and therefore the functional models and associated functions described apply to all VPN layer network technologies.

Source

ITU-T Recommendation Y.1314 was approved on 14 October 2005 by ITU-T Study Group 13 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

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.

© ITU 2006

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	1
4	Abbreviations and Acronyms	3
5	Client/server VPNs	6
5.1	Client/server combinations	7
5.2	VPN client layer transparency	9
6	Peer level VPNs.....	9
6.1	Packet/route filtering	10
6.2	Encryption	10
6.3	Ethernet VLANs.....	11
7	Functional architecture of VPNs	12
7.1	Connection-orientated VPN layer networks.....	13
7.2	Connectionless VPN layer networks	14
7.3	VPN client/server relationships	14
7.4	Multiple VPN client layers.....	19
7.5	Multiple VPN server layers	21
7.6	VPN modelling using partitioning.....	23
7.7	VPN peer layer	24
8	VPN topology support	26
8.1	Full mesh VPN topologies.....	27
8.2	Partial mesh VPN topologies.....	27
8.3	Hub and spoke VPN topologies	28
9	VPN QoS considerations	28
9.1	Circuit-switched layer networks.....	29
9.2	Packet-switched layer networks	29
10	Functions required for client/server VPN establishment.....	31
10.1	VPN server layer establishment	31
10.2	VPN client layer authentication/configuration.....	36
10.3	VPN client layer routing and signalling	38
11	Functions required for peer level VPN establishment.....	41
11.1	VPN membership discovery.....	41
11.2	CE/user authentication, authorization, and accounting (AAA).....	42
11.3	VPN peer layer routing.....	42
11.4	VPN peer layer network element configuration.....	42
12	VPN OAM functions	43
12.1	Fault management	43

	Page
12.2 Performance management	45
12.3 OAM activation/deactivation	45
12.4 Defects relevant to each network mode.....	46
13 Functional convergence and service scenarios	47
13.1 Client/server VPN services scenarios.....	48
13.2 Peer level VPN scenarios	48
14 VPN security considerations.....	48
Appendix I – Location of VPN client layer TCPs/TFPs.....	49
Appendix II – Client/server VPNs with multiple VPN server layers	52
Appendix III – Examples of client/server and peer level VPN service scenarios	54
BIBLIOGRAPHY	57

ITU-T Recommendation Y.1314

Virtual private network functional decomposition

1 Scope

This Recommendation describes the set of functions required to establish, operate and maintain client/server and peer level Virtual Private Networks (VPNs). The network functionality is described from a network level viewpoint, taking into account the VPN network layered structure, client characteristic information, client/server associations, networking topology and layer network functionality. The functional models are described using the network technology-independent modelling methodology described in ITU-T Recs G.805 and G.809.

2 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 were 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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.
- ITU-T Recommendation G.809 (2003), *Functional architecture of connectionless layer networks*.
- ITU-T Recommendation G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.
- ITU-T Recommendation Y.1311 (2002), *Network-Based VPNs – Generic architecture and service requirements*.

3 Definitions

This Recommendation uses the following terms defined in ITU-T Rec. G.805:

- 3.1 access point
- 3.2 access group
- 3.3 adapted information
- 3.4 characteristic information
- 3.5 client/server relationship
- 3.6 connection
- 3.7 connection point
- 3.8 layer network
- 3.9 link
- 3.10 link connection
- 3.11 matrix
- 3.12 network

- 3.13 network connection
- 3.14 port
- 3.15 reference point
- 3.16 subnetwork
- 3.17 subnetwork connection
- 3.18 termination connection point
- 3.19 trail
- 3.20 trail termination
- 3.21 transport
- 3.22 transport entity
- 3.23 transport processing function
- 3.24 unidirectional connection
- 3.25 unidirectional trail

This Recommendation uses the following terms defined in ITU-T Rec. G.809:

- 3.26 access point
- 3.27 access group
- 3.28 adapted information
- 3.29 characteristic information
- 3.30 client/server relationship
- 3.31 connectionless trail
- 3.32 flow
- 3.33 flow domain
- 3.34 flow domain flow
- 3.35 flow point
- 3.36 flow point pool
- 3.37 flow termination
- 3.38 flow termination sink
- 3.39 flow termination source
- 3.40 layer network
- 3.41 link flow
- 3.42 network
- 3.43 network flow
- 3.44 port
- 3.45 reference point
- 3.46 traffic unit
- 3.47 transport
- 3.48 transport entity

3.49 transport processing function

3.50 termination flow point

This Recommendation uses the following term defined in ITU-T Rec. G.8010/Y.1306:

3.51 flow domain fragment

This Recommendation uses the following terms defined in ITU-T Rec. Y.1311:

3.52 Layer 1 VPN

3.53 Layer 2 VPN

3.54 Layer 3 VPN

This Recommendation defines the following terms:

3.55 VPN client layer network: A topological component in a client/server VPN that represents the set of access points of the same type associated for the purpose of transferring VPN client layer characteristic information.

3.56 VPN server layer network: A topological component in a client/server VPN that represents the set of access points of the same type associated for the purpose of transferring adapted VPN client layer information.

3.57 VPN peer layer network: A topological component that represents the set of access points of the same type associated for the purpose of transferring VPN peer layer characteristic information.

4 Abbreviations and Acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
AAL	ATM Adaptation Layer
AG	Access Group
AI	Adapted Information
AIS	Alarm Indication Signal
AP	Access Point
ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
CAC	Connection Admission Control
CBR	Constant Bit Rate
CC	Connectivity Check
CE	Customer Edge
CI	Characteristic Information
CL-PS	Connectionless Packet-Switched
CO-CS	Connection-Orientated Circuit-Switched
CO-PS	Connection-Orientated Packet-Switched

CP	Connection point
CV	Connectivity Verification
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Connection Identifier
DSCP	Differentiated Services Code Point
DWDM	Dense Wave Division Multiplexing
EBGP	External Border Gateway Protocol
E-LMI	External LMI
ES	End System
FDF	Flow Domain Flow
FDFr	Flow Domain Fragment
FDI	Forward Defect Indication
FP	Flow Point
FPP	Flow Point Pool
FR	Frame Relay
FT	Flow Termination
FTP	Flow Termination Point
GRE	Generic Routing Encapsulation
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISIS	Intermediate System to Intermediate System
L2TP	Layer 2 Tunnelling Protocol
LDP	Label Distribution Protocol
LF	Link Flow
LMI	Local Management Interface
LOC	Loss Of Continuity
LOS	Loss Of Signal
LSP	Label Switched Path
MAC	Media Access Control
MP2P	Multipoint-to-Point
MP-BGP	Multi-Protocol BGP
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NE	Network Entity
NF	Network Flow

NMS	Network Management System
NSAP	Network Service Access Point
OAM	Operations, Administration and Maintenance
OOB	Out Of Band
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	Operational Support System
P	Provider (Node)
P2P	Point-to-Point
P2MP	Point-to-Multipoint
PCR	Peak Cell Rate
PE	Provider Edge
PM	Performance Monitoring
PNNI	Private Network-to-Network Interface
PHP	Penultimate Hop Popping
PM	Performance Monitoring
PW	Pseudo Wire
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RPR	Resilient Packet Ring
RMON	Remote MONitoring
RSVP-TE	Resource ReserVation Protocol (with) Traffic Engineering (extensions)
SCR	Sustained Cell Rate
SDH	Synchronous Digital Hierarchy
SES	Severely Errored Second
SLA	Service Level Agreement
SNC	SubNetwork Connection
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
SPVC	Switched Permanent Virtual Circuit
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
SVC	Switched Virtual Circuit
TCP	Termination Connection Point
TDM	Time Division Multiplexing
TFP	Termination Flow Point

TTL	Time-To-Live
TTSI	Trail Termination Source Identifier
UNI	User-to-Network Interface
VC	Virtual Circuit/Channel
VCCV	Virtual Circuit Connectivity Verification
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WDM	Wavelength Division Multiplexing

5 Client/server VPNs

Client/server VPNs have a two-layer hierarchy in which a VPN server layer network is used to support one or more VPN client layer networks.

ITU-T Rec. Y.1311 describes client/server VPNs in terms of VPN service types and VPN transport types, where the term VPN service type refers to the VPN client layer and the term VPN transport type refers to the VPN server layer. The different VPN service (client) and transport (server) types are classified in ITU-T Rec. Y.1311 as described below in Table 5-1.

Table 5-1/Y.1314 – Y.1311 service types

Service Type	Description
Layer 1	Provides a physical layer service between customer sites belonging to the same VPN. Connections can be based on physical ports, optical wavelengths, SDH/SONET VCs, frequency channels, or timeslots.
Layer 2	Provides a data link layer service between customer nodes belonging to the VPN. Forwarding of user data packets is based on information in the packets' data link layer headers (e.g., DLCI, ATM VCI/VPI, or MAC addresses).
Layer 3	Provides a network layer service between customer nodes belonging to the VPN. Forwarding of user data packets based on information in the Layer 3 header (e.g., IPv4 or IPv6 destination address).

One drawback to the method of classification used in ITU-T Rec. Y.1311 is that MPLS does not fit into any of these categories and must therefore be treated as a unique layer network technology. Another drawback is that, from a functional viewpoint, network technologies within the same layer can have very different characteristics and requirements. For example, Ethernet and ATM are both Layer 2 technologies; however, Ethernet is a broadcast-based connectionless technology whereas ATM is a connection-orientated non-broadcast technology.

An alternative method to classify network technologies is to classify them by the network mode they belong to. All network technologies can be mapped to one of three modes: connectionless packet-switched (CL-PS), connection-orientated packet-switched (CO-PS), and connection-orientated circuit-switched (CO-CS). The functional requirements for each mode are different as each mode has different characteristics. Table 5-2 shows examples of VPN network layer technologies and which mode they belong to.

Table 5-2/Y.1314 – Network modes of operation and examples

Mode of operation	Examples
Connectionless packet-switched	IP, Ethernet, MPLS MP2P (Note 1)
Connection-orientated packet-switched	Frame Relay, MPLS P2P/P2MP (Note 2), ATM
Connection-orientated circuit-switched	SDH/SONET, TDM
NOTE 1 – MPLS multipoint-to-point (MP2P) LSPs established using LDP in downstream unsolicited or ordered control mode traversing directly adjacent LDP peers.	
NOTE 2 – MPLS point-to-point (P2P) or point-to-multipoint (P2MP) LSPs established using RSVP-TE traversing RSVP-TE peers, or P2P LSPs established using targeted/directed LDP between non-adjacent LDP peers.	

5.1 Client/server combinations

There are nine possible client/server combinations based on the three network modes, although some combinations are more compatible than others. Table 5-3 describes the client/server combinations possible and provides some information on their compatibility.

A VPN server layer network must support multiplexing/de-multiplexing to provide data plane separation between multiple VPN client layers. VPN server layers must also support client traffic adaptation, which are client/server specific and are dependent on the VPN client and server layer network modes and on the specific technologies employed. One important adaptation requirement for circuit-switched VPN clients being carried by a packet-switched VPN server layer is that the adaptation function must provide rate decoupling (i.e., idle fill) and delineation of the VPN client layer packets. A key requirement for situations where the client/server are both packet-switched (CO or CL) is that the adaptation function must support fragmentation and sequencing if the VPN server layer traffic unit (i.e., the packets MTU) is smaller than the VPN client layer traffic unit. Other adaptation functions that may be required depending on the specific VPN client/server technologies employed include: coding, rate changing, and aligning.

Table 5-3/Y.1314 – Network mode client/server combinations

	CL-PS VPN client layer	CO-PS VPN client layer	CO-CS VPN client layer
CL-PS VPN server layer	– Ideal, although providing per flow delivery guarantees introduces scaling challenges – A common approach, which does not provide per flow delivery guarantees, is to use over-provisioning and class-based priority queuing (to manage any-to-any bursty traffic and congestion) <i>Example: An Ethernet server layer supporting an IP client layer</i>	– Providing per flow delivery guarantees introduces scaling challenges – A common approach, which does not provide per flow delivery guarantees, is to use over-provisioning and class-based priority queuing – VPN client layer must be able to recover from out-of-sequence traffic units (due to the possibility of server layer packet re-ordering) <i>Example: An IP server layer supporting an ATM client layer</i>	– Providing per flow delivery guarantees introduces scaling challenges – A common approach, which does not provide per flow delivery guarantees, is to use over-provisioning and class-based priority queuing – Recovering clock timing is technically challenging – VPN client layer must be able to recover from out-of-sequence traffic units <i>Example: An IP server layer supporting a TDM client layer</i>
CO-PS VPN server layer	– Cost associated with maintaining connection state for on-demand VPNs with short hold times, i.e., SPVCs <i>Example: An ATM server layer supporting an IP client layer</i>	– Ideal <i>Example: A P2P MPLS server layer supporting an ATM client layer</i>	– Recovering clock timing is technically challenging <i>Example: An ATM server layer supporting a TDM client layer</i>
CO-CS VPN server layer	– No statistical multiplexing between aggregates – Bandwidth assigned permanently in course increments resulting in poor network utilization – Slow connection set up response times for on-demand VPNs with short hold times <i>Example: An SDH server layer supporting an Ethernet client layer</i>	– No statistical multiplexing between aggregates – Bandwidth assigned permanently in course increments resulting in poor network utilization – Slow connection set up response times for on-demand VPNs with short hold times <i>Example: An ATM server layer supporting a TDM client layer</i>	– Ideal <i>Example: An optical server layer (e.g., a DWDM channel) supporting a SDH/SONET client layer</i>

5.2 VPN client layer transparency

In a client/server VPN, the functional components (such as routing, signalling, OAM, management, etc.) belonging to the VPN client layer network should be completely independent of the functional components belonging to the VPN server layer network.

Although it is possible to design client/server VPN solutions where the VPN server layer network's functional components interact with the VPN client layer network's functional components, this approach leads to a number of undesirable consequences, for example:

- 1) The VPN service may break if the customer changes any of the VPN client layer functional components.
- 2) The VPN service provider needs to track developments in the customer's VPN client layer technology and implement upgrades in its network accordingly.
- 3) Under fault conditions it becomes difficult to establish if the fault is in the VPN client layer network or the VPN server layer network.

By requiring that the VPN client and server layer networks are able to be run independently of one another, it naturally follows that the VPN server layer should transparently transfer the VPN client layer. For example, if the VPN client layer network is ATM, the VPN client layer network may implement a proprietary feature (e.g., AAL, non-PNNI routing and signalling, OAM) which, if not carried transparently, would break the VPN service.

Client layer transparency is not only a technical requirement, but it also has commercial implications because a VPN service provider is likely to consider the details of its network to be commercially sensitive and will therefore wish to hide those details from any VPN client layer networks. For example, it would not be desirable for the VPN server layer network to peer with the routing and signalling of the VPN client layer in the above example.

6 Peer level VPNs

In clause 5 the VPN topologies described were based on a client/server relationship between a VPN client layer and a VPN server layer. In the client/server VPN model, the VPN server layer adaptation source function adapts the CI of the VPN client layer into AI in the VPN server layer, and the VPN server layer adaptation sink function adapts VPN server layer AI to VPN client layer CI. In basic terms, this adaptation refers to the encapsulation of the client layer frame/signal in a VPN server layer frame/signal.

However, not all VPN topologies are based on the client/server model. VPNs can also be provided using CL-PS network technologies based on a model in which VPN reachability isolation within a shared domain is achieved via some means other than client/server encapsulation. This Recommendation refers to this type of VPN as a peer level VPN. The term "peer level" refers to the fact that the provider transports the customers VPN packets across its shared infrastructure at the same network layer at which it receives the packets from the customer. It does not refer to customer/provider control plane peering, the customer and provider may peer with each other in the control plane regardless of the type of VPN. Only the CL-PS network mode supports this type of VPN because, in the CO-PS and CO-CS cases, the connection-orientated nature of the technology enforces reachability isolation, i.e., NEs can only communicate with NEs that belong to the same P2P or P2MP connection.

In order to support VPNs across a shared domain, the network technology used must have some means of providing VPN isolation, i.e., NEs must only be able to communicate with other NEs belonging to the same VPN or be able to decrypt packets from NEs belonging to the same VPN.

6.1 Packet/route filtering

One way of implementing VPN isolation across a shared domain is to use packet filters along with PEs that are shared between multiple customers. In this approach, all the nodes in the service provider's network know all the customers' routes. This includes the provider edge (PE) nodes that face the customers' sites, and the provider (P) nodes in the core. In this architecture, the PE nodes are shared by different customers. The service provider allocates a portion of its address space to a customer and manages the packet filters on the PE routers to ensure full reachability between sites of a single customer, and isolation between customers.

To overcome the need to maintain consistent routing tables and packet filters on a per customer per site basis, an alternative is to implement a solution based on route filtering rather than packet filtering along with dedicated PEs, i.e., one PE per VPN. In this architecture, the P nodes contain all customers' routes but the PE nodes only contain routes for a single customer. Isolation of customer routes is achieved by route filtering. PE nodes are configured with route filters that only allow customers to learn about routes that belong to them. Border Gateway Protocol (BGP) is an example of a protocol commonly used for this purpose inside the provider backbone due to its versatile route filtering tools. An alternative to route filtering would be to use a different routing protocol instance for each VPN. However, using this approach, the shared network would only be able to support a small number of VPNs due to P nodes only being able to support a finite number of routing protocol instances, and due to the operational complexity of managing multiple protocol instances.

To overcome the need to use a different PE node for each VPN, an alternative approach is to use virtual routers (VRs). In this approach, one physical node is effectively compartmentalized into a number of virtual routers. One (or several) virtual routers can be assigned to a particular customer. In this way, one node can provide compartmentalized routing instances for several customers. Individual virtual routers behave just like separate PE nodes dedicated to a particular VPN. As with the route filtering approach, P nodes contain all customers' routes and therefore route filtering is required at PEs.¹

6.2 Encryption

An alternative to route/packet filtering is to provide full reachability between all customers connected to a shared infrastructure in conjunction with packet encryption. Packet encryption ensures that if customers receive packets from a VPN to which they do not belong, they cannot obtain the information contained inside the packet. The customer may encrypt VPN packets before the traffic goes out over the shared network and therefore the customer is responsible for managing the VPN. In this approach, traffic within the service provider network is routed the same as any other IP traffic, and the service provider has no visibility into the tunnel. Nor does the service provider network need to be configured in any special manner. Alternatively, VPN packets may be encrypted using equipment managed by the provider (i.e., PEs or provider managed CEs) at the edge of the provider's shared network. In this approach, the provider is responsible for managing the VPN.

¹ A natural evolution of this approach is to use MPLS or other tunnelling approaches so that VPN-specific routes do not have to be maintained on backbone routers. However, this creates a client/server VPN topology and therefore this approach is applicable to clause 5 rather than this clause.

An example of an architecture that supports encryption is RFC 2401 – Security Architecture for the Internet Protocol (IPsec). IPsec defines cryptographic algorithms, authentication and key² management routines for creating secure IP traffic tunnels between IPsec gateways/clients. IPsec guarantees the privacy, integrity and data origin authentication in a VPN as the information traverses a shared infrastructure. IPsec is particularly useful for providing VPNs across public networks such as the Internet for site-to-site and remote access VPNs. IPsec functionality may be provided by a PE, CE, or end user device (e.g., a laptop running an IPsec client).

Secure Socket Layer (SSL) VPNs are another type of VPN that use encryption to provide per VPN isolation. A typical use of SSL VPNs is to allow users to access applications and files securely over the Internet. The advantage of this approach is that it does not require any configuration changes to end users' systems, only standard applications need to be supported (e.g., Web browsers, email clients, etc.). Also, SSL VPNs are transparent to the VPN peer layer (as encryption is performed at the application layer) and therefore configuration of routing/switching nodes is not necessary in order to support SSL VPNs.

6.3 Ethernet VLANs

The IEEE 802.1Q standard defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure. VLANs allow end-stations on multiple physical LAN segments to communicate as if they were connected to the same LAN segment. End users and hubs/switches can be moved to different VLANs by changing the VLAN configuration on the port/interface on the 802.1Q-compliant switching device that the end station or hub/switch connects to. Broadcast and multicast frames are constrained by VLAN boundaries so end-stations will only receive broadcast/multicast frames for the VLAN that they belong to. This, in conjunction with how MAC address learning works, ensures that only end-stations belonging to the same VLAN may communicate with each other, and can therefore be considered to be members of the same VPN.

Traffic separation for frames belonging to different VLANs across a shared infrastructure is achieved by inserting a tag with a VLAN identifier (VID) into each frame. A VID must be assigned for each VLAN (1 to 4 096) and must be globally unique within the same physical infrastructure. One of the drawbacks to this approach is that customers also use VLANs within their own network, which introduces VID allocation and limitation issues. To solve this problem a second IEEE 802.1Q-tag can be appended to customer IEEE 802.1Q tagged packets that enter the providers' network (Q-in-Q as defined in IEEE 802.1ad). This separates the providers VLAN space from the customers' VLAN space and allows customers to use whatever VIDs they want³.

2 A key is a piece of information that controls the operation of the encryption/decryption algorithm.

3 Another option is to use a MAC-in-MAC approach (as defined in IEEE 802.1ah) in which a provider appends a second Ethernet header to the customers packet. However, this option creates a client/server VPN rather than a peer level VPN because the customers' frame is encapsulated inside a provider frame.

7 Functional architecture of VPNs

The VPN reference model from ITU-T Rec. Y.1311 is shown in Figure 7-1.

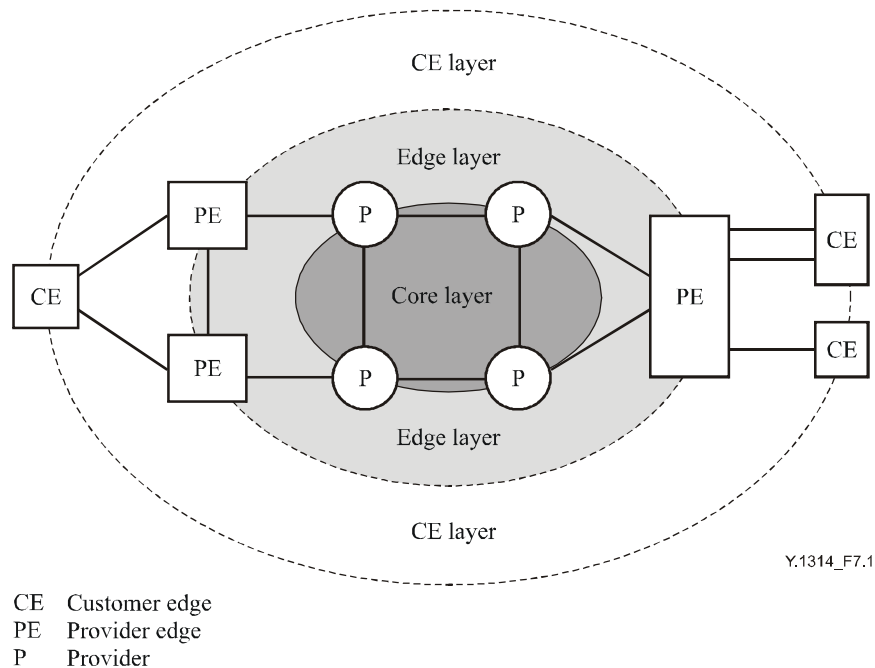


Figure 7-1/Y.1314 – ITU-T Rec. Y.1311 VPN reference model

Although this model shows the physical topology and the different network components, it does not show the different VPN server and client layer topologies or the location of inter-layer adaptation functions.

An alternative method of representing a client/server VPN network is to use functional modelling. The functional architecture of connection-orientated (CO-PS/CO-CS) and connectionless (CL-PS) layer networks can be described using ITU-T Rec. G.805, the "generic functional architecture of transport networks" and ITU-T Rec. G.809, the "functional architecture of connectionless layer networks" respectively.

ITU-T Recs G.805 and G.809 provide useful generic methods for modelling networks from a functional and structural architecture perspective. The terminology defined is technology-independent and can be used to describe the physical and logical components for any given network. This is particularly useful for network inventory and management as the complete network view can be modelled, from the optical fibres in the duct up to the VPN services running over them.

A VPN network can be decomposed into a number of independent layer networks with a client/server relationship between adjacent layer networks. As noted in ITU-T Rec. G.805, layer networks defined using functional modelling should not be confused with the layers of the Open System Interconnection (OSI) Model (ITU-T Rec. X.200). Each layer in the OSI model offers a specific service and the protocols defined at each layer perform a specific function corresponding to that layer, e.g., the transport layer (Layer 4) accepts data from the session layer, and passes it onto the network layer providing an end-to-end delivery service. On the contrary, each layer network in a functional model based on ITU-T Recs G.805 or G.809 offers the same service, i.e., the transport of bits/frames between inputs and outputs. Abstraction is commonly used to hide detail and to focus on the network layers/components of interest, but networks can be modelled right down to the network elements, e.g., Ethernet switches, copper pairs, SDH cross connects, etc.

7.1 Connection-orientated VPN layer networks

VPN client and server layer networks each have their own set of connectivity inputs and outputs known as access points (APs). These may be associated with each other to transfer information transparently across the layer network from input to output. Valid topology constructs of association between APs for CO layer networks are point-to-point (P2P) and point-to-multipoint (P2MP).

VPN server layer APs mark the functional boundary between the VPN server and client layer networks. From the VPN server layers perspective, a VPN server layer AP represents a routing destination that may support a trail. From the VPN client layer's perspective, a VPN server layer AP represents a point at which it is possible to procure link capacity. The functional components and reference points in a CO network layer are illustrated in Figure 7-2.

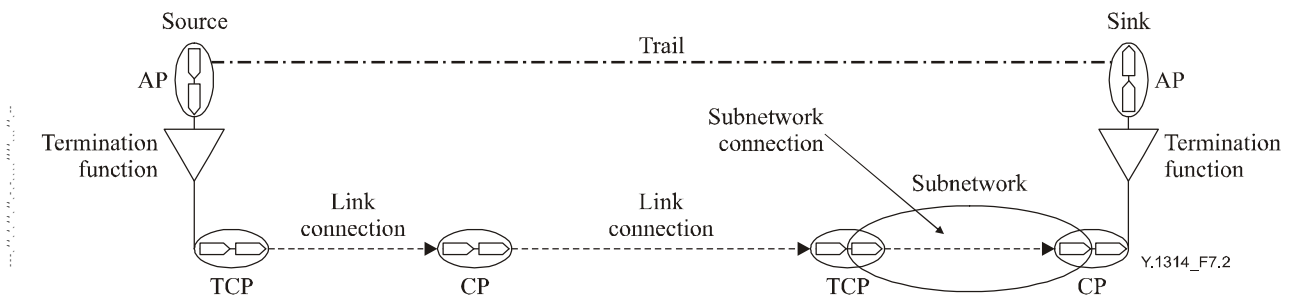


Figure 7-2/Y.1314 – CO functional components and reference points

Connections are transport entities in CO layer networks that consist of an associated pair of unidirectional connections capable of simultaneously transferring information in opposite directions between their respective inputs and outputs. A network connection is a transport entity in a CO layer network formed by a series of contiguous link connections and/or subnetwork connections between termination connection points (TCPs).

A subnetwork is a topological component in a CO layer network used to effect routing of specific characteristic information, and contains a set of points associated with a management function within a single CO network layer. A subnetwork connection transfers information across a subnetwork, and is formed by the association of ports (output of a trail termination source/input of a trail termination sink) on the boundary of the subnetwork.

Link connections interconnect topologically adjacent subnetworks that have a common subset of points. The point at which the input of a link connection is bound to the output of another link connection is a connection point (CP). The point at which a trail termination source output in a CO layer network is bound to the input of the network connection is a source TCP, and the point at which a trail termination sink input is bound to a network connection output is sink TCP. CPs and TCPs have a managed object associated with them and, it is therefore possible to group together TCPs and CPs belonging to the same VPN for management purposes.

7.2 Connectionless VPN layer networks

Unlike CO layer networks, CL layer networks support multipoint-to-multipoint (MP2MP) or any-to-any topologies. CL layer networks use flows rather than connections which are an aggregation of one or more traffic units with an element of common routing. Flows can be unidirectional or bidirectional, with bidirectional flows consisting of two contra-directional unidirectional flows. A network flow is a transport entity in a CL layer network formed by a series of contiguous flows between termination flow points (TFPs). The functional components and reference points in a CL network layer are illustrated in Figure 7-3.

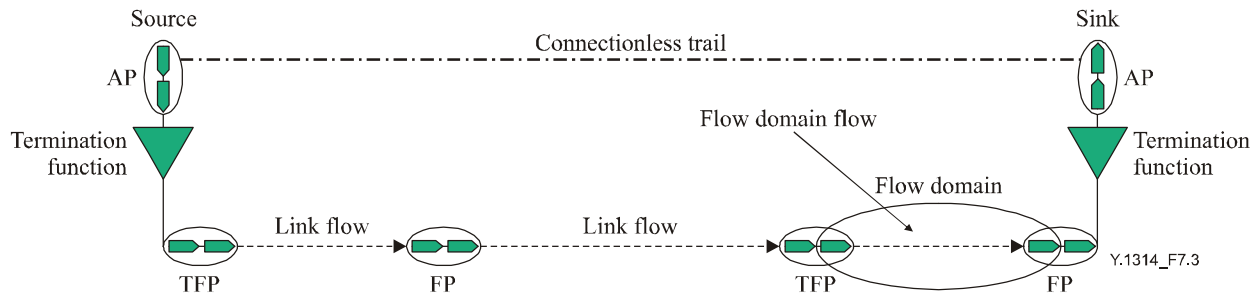


Figure 7-3/Y.1314 – CL functional components and reference points

A flow domain is a topological component in a CL layer network used to effect routing of specific characteristic information. A flow domain flow is a transport entity that transfers information across a flow domain, and is formed by the association of ports on the boundary of the flow domain. A flow domain contains a set of points associated with a management function within a single CL network layer.

Link flows interconnect topologically adjacent flow domains that have a common subset of points. The point at which the input of a link flow is bound to the output of another link flow is a flow point (FP). The point at which a connectionless trail termination source output in a CL layer network is bound to the input of the network flow is a source TFP, and the point at which a connectionless trail termination sink input is bound to a network flow output is a sink TFP. As with CPs and TCPs in the CO case, in the CL case FPs and TFPs have a managed object associated with them and it is, therefore, possible to group together TFPs and FPs belonging to the same VPN for management purposes.

7.3 VPN client/server relationships

In functional terms, a VPN client layer network is a topological component in a client/server VPN that represents the set of access points of the same type associated for the purpose of transferring VPN client layer characteristic information, which are supported by a VPN server layer trail or a connectionless trail. The source/sink TCPs/TFPs for VPN client layer connections/flows may be located in CE nodes, or in nodes/end-systems elsewhere in the customer's network. For example, TCPs in an ATM VPN client layer are likely to be located in CE nodes, whilst TFPs in an Ethernet VPN client layer are likely to be located in end user computers or servers. The location of the VPN client flow/connection TFPs/TCPs is important from a customer perspective, as this is the point in the customer's network where adaptation between the VPN client layer and the layer above must take place. It is also important from an OAM perspective, as this is where the source and sink APs for the trail/connectionless trail associated with a VPN client layer flow/connection are located. Examples of client/server VPNs where the TFPs/TCPs are located in different places are provided in Appendix I.

A VPN server layer network is a topological component in a client/server VPN that represents the set of access points of the same type associated for the purpose of transferring adapted client layer information for one or multiple VPN client layer flows or connections. The VPN server layer contains source/sink adaptation functions that adapt the characteristic information in the VPN client layer into/from adapted information in the VPN server layer. The VPN client and server layers may belong to the same mode (i.e., when the client and server layers are both CO or the client and server layer are both CL), but combinations of the two are also possible, i.e., CO VPN server layers can support CL client layers, and likewise CL server layers can also support CO client layers. Figure 7-4 shows an example of a CL VPN server layer supporting a CL VPN client layer from a functional perspective based on the physical topology of the network model from ITU-T Rec. Y.1311 shown in Figure 7-1. The bottom layer shown in the model is the VPN server layer and the top layer is the VPN client layer. Only the VPN client/server layers are illustrated for simplicity, the customer client layer above the VPN client layer, and the server layer below the VPN server layer are not shown. In this example the VPN server layer is CO (e.g., ATM) whilst the VPN client layer is CL (e.g., Ethernet), although any combination of CO or CL pairs is possible.

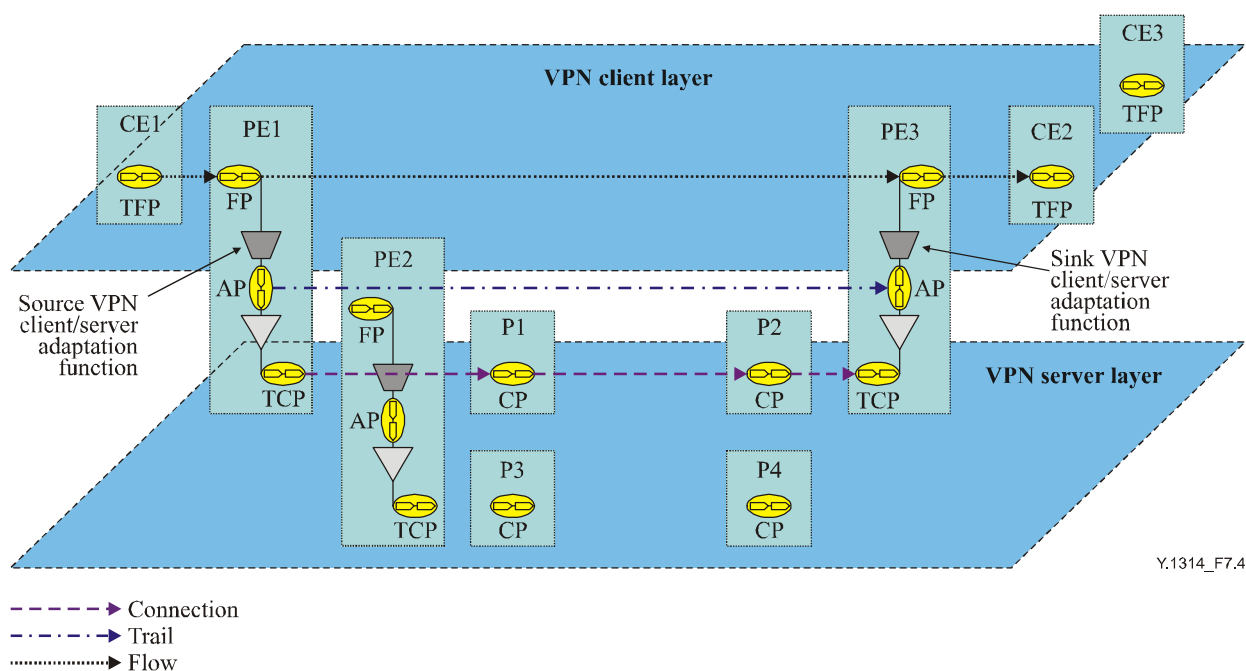


Figure 7-4/Y.1314 – Functional model of client/server VPN

Figure 7-4 shows how the functional model relates to the network diagram in Figure 7-1 by highlighting which functions and network reference points exist in which network element (i.e., CE, PE, or P node). The CE and P nodes belong to the VPN client and server layers respectively, whilst the PE nodes belong to both layers. The TFPs in the VPN client layer identify where (which CE node in this case) the P2P VPN client layer flow starts (its source) and ends (its sink), and the FPs identify which PE nodes the P2P flow passes through. Likewise, the TFPs in the VPN server layer identify the source and sink for the VPN server layer connection, and the FPs identify which P nodes the flow passes through. The APs in the VPN server layer identify the source/sink for the VPN server layer trail.

The following subclauses present each of the four possible client/server VPN combinations using functional models and describe the role of the client/server VPN adaptation functions.