INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Y.1312

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(09/2003)

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

Internet protocol aspects – Transport

Layer 1 Virtual Private Network generic requirements and architecture elements

ITU-T Recommendation Y.1312

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.1312

Layer 1 Virtual Private Network generic requirements and architecture elements

Summary

This Recommendation specifies service definition, service scenarios, service requirements and service architecture elements on Layer 1 Virtual Private Network (L1 VPN).

Source

ITU-T Recommendation Y.1312 was approved on 13 September 2003 by ITU-T Study Group 13 (2001-2004) under the ITU-T Recommendation A.8 procedure.

Keywords

Architecture, Layer 1, Layer 1 VPN, Requirement, 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.

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.

CONTENTS

ITU-T Recommendation Y.1312

Layer 1 Virtual Private Network generic requirements and architecture elements

1 Scope

This Recommendation specifies service definition, service scenarios, service requirements and service architecture elements on Layer 1 Virtual Private Network (L1 VPN).

L1 VPN has specific features compared to generic VPN described in ITU-T Rec. Y.1311, such as connections between CEs rather than tunnels between PEs, and C-plane/U-plane separation. In addition, L1 VPN has features such as connectivity restriction within limited CEs and per-VPN C-plane functionalities, which are achieved by additional functionalities to the basic L1 network. To this end, L1 VPN provides customers with large capacity U-plane resources with a different set of C-plane functionalities. Thus, new kinds of services are expected to emerge, including multi-service backbone, carrier's carrier and L1 resource trading.

This Recommendation addresses service features of L1 VPN including those mentioned above, and also describes service requirements and service architecture elements. In addition, this Recommendation describes several scenarios where the merits of L1 VPN are well expected.

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.

[1] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

[2] ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture for the automatic switched optical network (ASON)*.

[3] ITU-T Recommendation Y.1311 (2002), *Network Based VPNs – Generic architecture and service requirements*.

3 Definitions

This Recommendation defines the following terms:

3.1 L1 VPN: A network formed by a set of CEs and network resources between CEs. A set of CEs is managed by the same authority. Network resources between CEs are provided by the service provider, and may include links, connections and C-plane functionalities. Refer to ITU-T Rec. Y.1311.

3.2 NB L1VPN: Refer to ITU-T Rec. Y.1311.

3.3 CE: The entity receiving U-plane and C-plane service provided by the network to which it is attached. Refer to ITU-T Rec. Y.1311.

3.4 PE: The entity within the Network connected to CE, that provides service to customers. Refer to ITU-T Rec. Y.1311.

3.5 **P**: The entity within the network, and connected to P or PE devices. Refer to ITU-T Rec. Y.1311.

3.6 **link**: U-Plane resource connecting adjacent network devices in the same layer (in the OSI sense) and within the same layer network (in the G.805 sense), e.g. connecting CE and PE, PE and P.

3.7 **connection**: For L1 VPN, a connection is established between a pair of CEs. See Annex A for a more detailed description.

3.8 **customer**: The entity that has authority over a set of CEs within the same VPN (e.g. the owner of the CEs). The customer is the billable entity to which L1 VPN service is provided. The customer of a Layer 1 VPN has typically at least 3 CEs, while the customer of a private line service has exactly two CEs.

3.9 **shared U-plane**: U-plane in which link resources can be multiplexed (over time) between different VPNs. At any instant in time the resources are either dedicated to one VPN or are unallocated.

3.10 **dedicated U-plane**: U-plane in which link resources are allocated exclusively to a specific VPN.

3.11 **shared C-plane**: C-plane in which the same control resources are used by multiple VPNs.

3.12 **dedicated C-plane**: C-plane in which control resources are allocated exclusively to a specific VPN.

3.13 **Shared U-Plane Private Network (SUPN)**: L1VPN with shared U-plane.

3.14 **Dedicated U-Plane Private Network (DUPN)**: L1VPN with dedicated U-plane.

3.15 **Shared C-Plane Private Network (SCPN)**: L1VPN with shared C-plane.

3.16 **Dedicated C-Plane Private Network (DCPN)**: L1VPN with dedicated C-plane.

3.17 **site**: The network behind a CE, that is managed by the same authority as the CE.

4 Abbreviations

This Recommendation uses the following abbreviations:

AAA Authentication, Authorization and Accounting

CE Customer Edge

CNM Customer Network Management

CSM Customer Service Management

DCN Data Communication Network

P Provider

PE Provider Edge

PM Performance Measurement

VPN Virtual Private Network

5 Service definition and service reference model

5.1 Basic L1 service reference model and features

5.1.1 Basic L1 service reference model

Figure 5-1 shows the reference network model where a customer edge (CE) is using a L1 service. Separation between the service provider and the customer is provided by L1 service interface. Basic L1 service provides U-plane resources between CEs in a point-to-point manner, i.e. connection oriented.

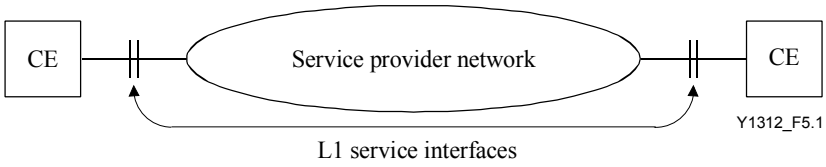


Figure 5-1/Y.1312 – Basic L1 service reference model

5.1.2 Basic L1 services features

Basic layer 1 service is characterized in terms that include:

– Connectivity: between a pair of CEs;

– Capacity: for example, bit rate for a TDM service;

– Transparency: for example, for a SDH network, overhead transparency etc.;

– Availability: the percentage of time that the quality service meets the agreed criteria. To achieve the required level of availability for the customer connections, the service provider's network may use restoration or protected resources;

– Performance: e.g., number of error seconds per month.

5.2 L1 service categories, L1 VPN reference model and definition

5.2.1 L1 service categories

Layer 1 services can be categorized based on the combination of connectivity features (U-plane) and service control capability (C-plane) available to the customer. A CE is associated with the service interface between a customer site and the network. Type 1 enables one connection between a pair of CEs. Type 2 enables multiple connections among a set of CEs. Type 2 may involve a variety of C-plane types depending on the customer. Table 5-1 shows the classification of the services. Layer 1 VPN can be defined as a subset of the Type 2 service category. Compared to Type 1 services, the Layer 1 VPN service has features such as separate policy per VPN and distribution of membership information. For either Type 1 or Type 2 services, connections are point-to-point and can be permanent, soft-permanent, or switched. For a static service, the network is responsible for the management of both the network infrastructure and the end user connections. For dynamic service, the network is only responsible for the configuration of the infrastructure; end user connections are established dynamically by the network.

Table 5-1/Y.1312 – Types of layer 1 services including layer 1 VPN

Types of Layer 1 services		
Type 1 Single connection service (one customer between two CEs)	Static service	• Permanent connection service (classic private line service)
	Dynamic service	• Switched connection service • Customer-controlled soft permanent connection service
Type 2 Multiple connection service (one customer; three or more CEs)	Static service	• Private network service
	Dynamic service **Layer 1 VPN**	• Customer-controlled soft permanent connection service • Switched connection service • Separate policy per VPN, and distribution of membership information within the group of CEs
NOTE – Single connection service may be supported by multiple connections (e.g. protection purpose).		

5.2.2 L1 VPN reference model

Figure 5-2 shows a reference model for L1 VPN.

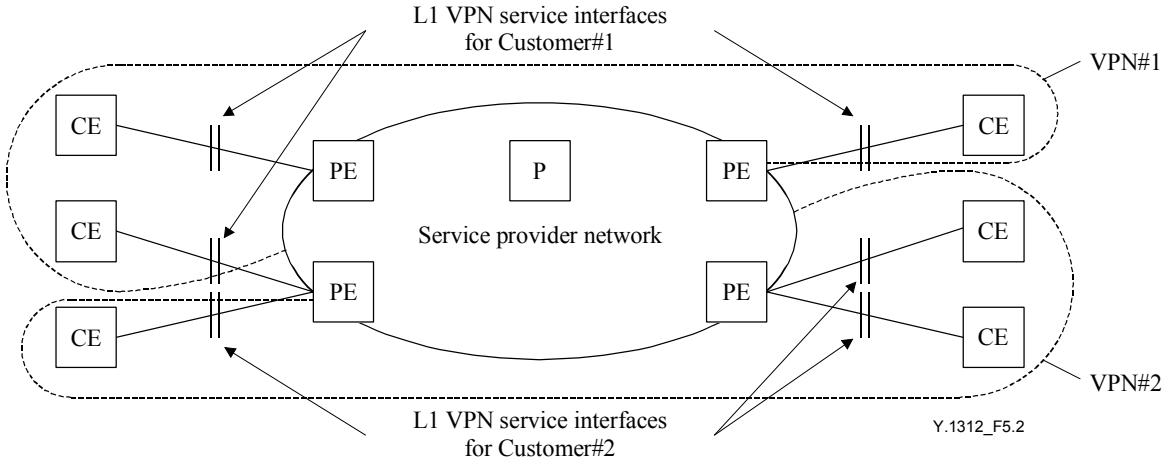


Figure 5-2/Y.1312 – L1 VPN reference model

NOTE 1 – Customer may outsource management of VPN to a different organization. In this case, this organization has an authority to manage the VPN.

NOTE 2 – The CE and PE are logical entities; the implementation is dependent on the network application. For example:

a) The CE and PE may be implemented in the same building, or even in the same equipment. In this case, the CE and PE are still regarded as logically separated entities.

b) There could be a network on the user side of CE, i.e. site.

c) The link between the CE and PE may be provided by the (static) network of another network operator.

5.2.3 L1 VPN service definition and features

A Layer 1 VPN is a VPN whose U-plane operates at layer 1. Thus, the L1 VPN service provides optical or TDM connections between CEs. In addition to the service features of basic L1 service described above, the Layer 1 VPN service has the following features:

- U-plane: Layer 1 connectivity is provided to a limited set of CEs (This set of CEs forms the Layer 1 VPN membership.);
- C-plane: Some level of control and management capability is provided to the customer.

6 Service scenarios

6.1 Multi-service backbone

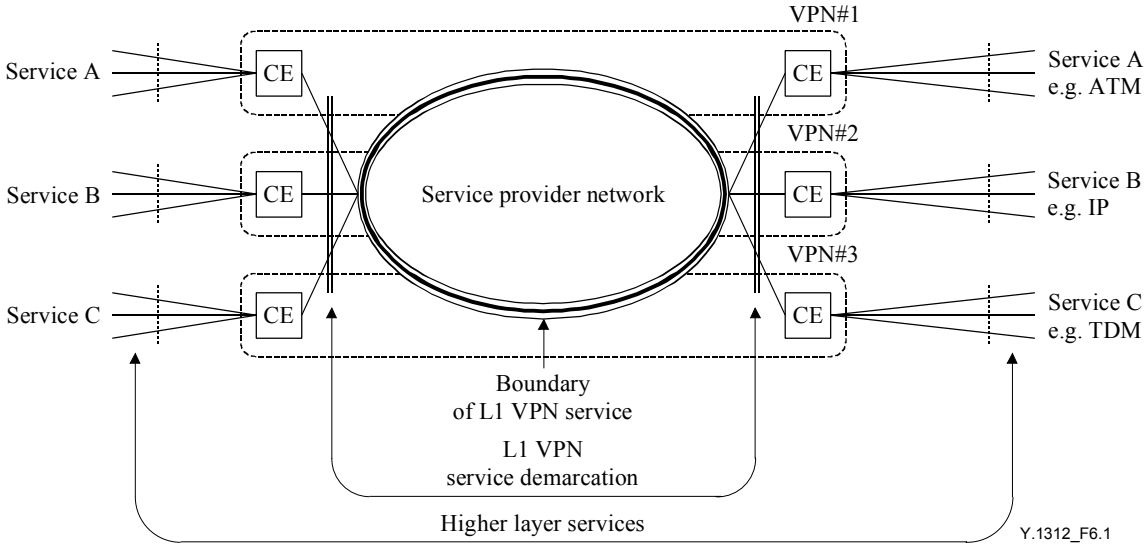


Figure 6-1/Y.1312 – Multi-service backbone

Multi-service backbone is characterized in terms such that one service department of a carrier receiving the carrier's L1 VPN service provides different kinds of higher-layer service.

The customer receiving L1 VPN service can offer its own services whose payloads can be any layer (e.g. ATM, IP, TDM). From the L1 VPN service provider point of view, these services are not visible and are not part of the L1 VPN service. That is, the type of service being carried within the L1 payload is not known by the service provider.

The benefit is that the same L1 core network resources are shared by multiple services. A large capacity backbone network (U-plane) can be built economically by having the resources shared by multiple services, usually with flexibility to modify topologies, while separating the control functions. Thus, each customer can select a specific set of features that are needed to provide their own service.

6.2 Carrier's carrier

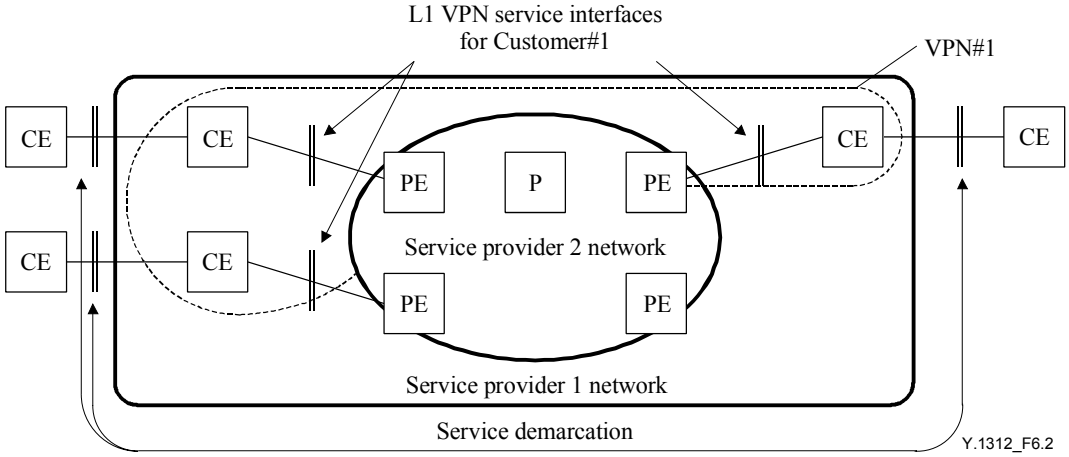


Figure 6-2/Y.1312 – Carrier's carrier

Carrier's carrier is characterized in terms such that one carrier receiving anther carrier's L1 VPN service provides its own service. In this service scenario, provider 1 and provider 2 in Figure 6-2 are in different organizations. Therefore, it is expected that more limited information is provided at the service demarcation point, and more strict control is carried out than in the case of multi-service backbone. For example, customers of L1 VPN service receive:

– limited view of L1 VPN service provider network;

– limited control over L1 VPN service provider network.

One of the merits is that each provider can concentrate on a specific service. For example, provider 1 more focuses on L3 service, e.g. providing secure access to the Internet, while provider 2 more focuses on L1 service, i.e. providing a long haul bandwidth between cities. Provider 1 can construct its own network using L1 resources provided by the provider 2, usually with flexibility to modify topologies, and dedicated C-plane functionalities.

6.3 L1 resource trading

In addition to the scenarios where the second tier service provider is using a single core service provider as is mentioned above, it is possible for the second tier provider to have service from more than one service provider, as shown in Figure 6-3. In this service scenario, there are some benefits for the second tier service provider such as dynamic carrier selection based on the price and route redundancy.

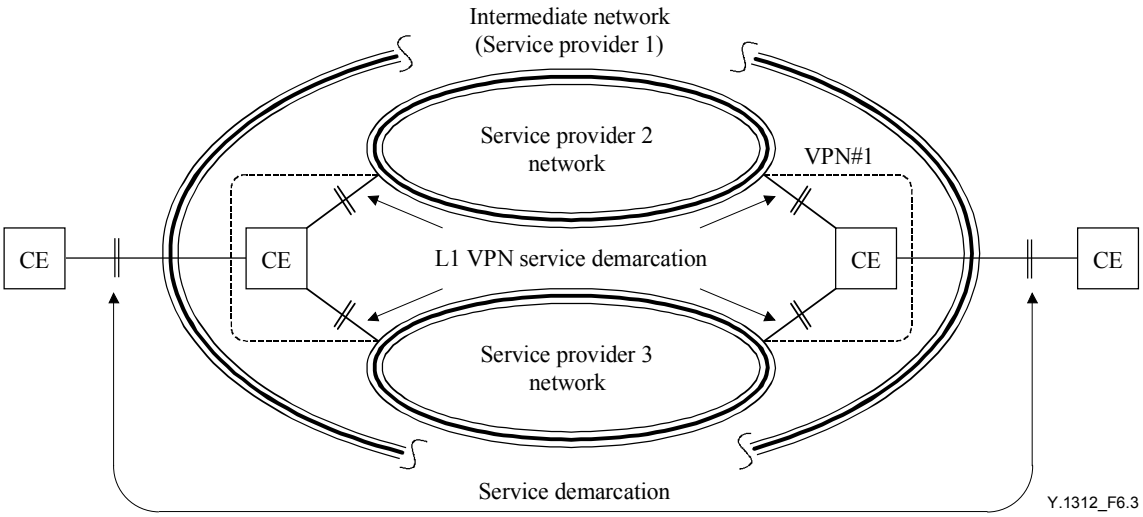


Figure 6-3/Y.1312 – L1 resource trading

The following additional features are required to realize L1 resource trading.

Extended service provider resource notification: Primary tier service providers that the second tier provider is able to obtain L1 service from have a capability to publish resource information to the second tier provider. This information can be used by the second tier provider to make decisions about which service provider to obtain L1 service from. An example of such information is pricing.

Service provider dual homing: The second tier provider is aware that it can use different service providers as opposed to having two demarcation points to the same provider. This is needed for making decisions based on provider characteristics like price. It is also needed for making two requests that are to be obtained in separate service providers.

With these additional capabilities, the second tier provider can support a function that enables an L1 resource trading service. Using resource information published by its service providers, a second tier provider can decide how best to use those providers. For example, if one service provider is no longer able to satisfy requests for service, the alternate service provider can be used. The second tier provider can choose to respond to price changes over time. Another example of second tier provider use is to reduce exposure to failures in each provider (improve availability).

NOTE – There could be several service requirements derived from this service scenario. The detailed service requirements for L1 resource trading are for further study.

6.4 Inter-SP L1 VPN

In addition to the scenarios where a single connection between two CEs is routed over a single service provider, it is possible that a connection is routed over multiple service providers. This service scenario is called Inter-SP L1 VPN. For example, this scenario is beneficial in the case where an L1 VPN is constructed by receiving service from multiple regional providers. There could be variety of business relationships smong providers and customers. In this case, the detailed business relationship among providers and customers is for further study. Also, there could be several service requirements derived from this service scenario. The detailed service requirements for inter-SP L1 VPN are for further study.

7 Service requirements

Table 7-1 shows the list of requirements for L1 VPN with categorization as mandatory or optional.

Table 7-1/Y.1312 – Service requirements for L1 VPN

Item number	Service requirement	Mandatory	Optional
1	Basic layer 1 service features	Connectivity, Capacity, Transparency, Availability, Performance.	
2	Dynamic control of layer 1 connection	Soft-permanent, or switched.	
3	Notification of connection rejection	Network notifying the originating CE giving a reason for the failure, in the case where the network can not complete a service request.	
4	Subscription of multiple VPNs at the service interface		Enabling CE to simultaneously make connections within different VPNs.
5	Parallel connection with public network		A CE or an entity in site is connected to the public network, as well as the L1 VPN service provider.
6	Authentication	Validation of CE identity prior to allowing access to service.	
7	Authorization	Preventing CE from performing unauthorized control of the network in the L1 VPN.	
8	Accounting		Recording the quantitative information on the usage.
9	Connectivity restrictions	Restricting connectivity based on source and destination VPN membership.	
10	Explicit link selection (NOTE – Typically only for DUPN)		Customer specifying an explicit link or series of links (e.g. route).
11	Distribution of membership information		Network distributing list of current members.
12	Distribution of member availability information		Network distributing ability or willingness of current members to participate in the VPN.
13	Transfer of resource information (NOTE – Typically only for DUPN)		Network providing network topology view, performance, utilization, resource status.
14	Transfer of connectivity information		Network providing list of current active connections within the VPN.

Table 7-1/Y.1312 – Service requirements for L1 VPN

Item number	Service requirement	Mandatory	Optional
15	Transparent transfer of control information between customer entities		For example, topologies of isolated sites are shared when connected over a common provider.
16	Network participation in customer domain routing		For example, a common provider may use topology and status information of isolated sites to optimize routing.
17	Per-VPN policy	Ability to enforce policy to each VPN instance	Example: link selection policy. Network enforcing some policy on link selection for a connection. When there are multiple policies available, a customer may be able to select which policy to be applied in connection request.
18	Selection of L1 class of service (e.g. availability level)		Customer requesting a class of service per connection basis, by which the network is mandated to select the survivability mechanisms corresponding to it.
19	CNM		The customer's ability to view and control the service across an interface to the management system.
20	Per-CE policy and its management		The customer's ability to modify per-CE policy.
21	Transfer of performance information		The network providing the performance information of a L1 connection provided by the service provider. (NOTE – may include C-plane status).
22	Transfer of fault information		The customer can receive fault information for the U-plane and C-plane resources.
NOTE – Requirement #15 means control information transfer over control plane. When control information is transferred over a connection between CEs, transparent transfer of control information between CEs is realized without any service-related functions in the provider network.			

Naming:

A unique address within the context of the VPN must be assigned to each CE. This address is used by the CE when making connection requests. This address may be either:

i) A public address assigned by the network operator:

In this case the CE may translate connection request for the local client address to the assigned public address. The network may use this public address directly for connection routing.

ii) Or A private address assigned by the Customer:

In this case the network may translate the private address into a network address to support connection routing.

By using AAA, each customer can receive a different set of features and functionalities mentioned herein. For example, customer A and customer B receive different membership information and resource information. Another example is that customer A receives resource information, but customer B does not, based on the contract. This forms the per-VPN C-Plane functionality feature.

8 Service architecture elements

8.1 C-plane and U-plane combinations

The elements that constitute a VPN are the U-plane resources and C-plane resources defined below. The services realized vary greatly depending on whether these resources are shared by multiple VPNs, or dedicated to an individual VPN. It is thus necessary to clarify which type is assumed in referring to L1 VPN services.

8.1.1 U-plane resources

U-plane resources are the network facilities used for the transport of user information and, include ports, physical interfaces, TDM channels or wavelengths (e.g. links).

a) "Shared U-plane resources" means that the resources are used by multiple VPNs in a time-sharing manner. In other words, a specific L1 resource is used for one VPN for a certain time, and is used for another VPN after the first VPN releases the link. A layer 1 VPN with shared U-plane resources is called a Shared U-Plane Private Network (SUPN).

b) "Dedicated U-plane resources" means that resources are VPN allocated exclusively to a VPN for its lifetime. A layer 1 VPN with dedicated U-plane is called a Dedicated U-Plane Private Network (DUPN).

Note that connection management method in the U-plane is independent of whether the U-plane is shared or dedicated.

8.1.2 C-plane resources

C-plane resources are connection control facilities including routing software processes and routing tables. These resources are used to realize specific algorithm and policy involved in the connection control of the U-plane resources. The function performed by these C-plane resources can be grouped into three broad categories:

i) Common support functions, for example:

- Physical communications channel for signalling.

In General these functions are shared across multiple VPNs.

ii) Functions that do not require explicit knowledge of the L1 resources for example:

- VPN membership;
- VPN policy;
- Transparent transfer of user control information.

These functions are always dedicated to a single VPN.

iii) Functions that require explicit knowledge of the L1 resources for example:

- Link resource management;
- Routing topology.

These functions may be either shared or dedicated.

The classification of shared C-plane and dedicated C-plane are applied in the context of the functions described in iii) above. The classification of dedicated C-plane is only used in the case where none of the functions described in iii) are shared.

a) "Shared C-plane resources" means that the same C-plane resources (to support the functions identified in iii)) may be used for the control of multiple VPNs. A layer 1 VPN with shared C-plane resources is called a Shared C-Plane Private Network (SCPN).

b) "Dedicated C-plane resources" means that different C-plane resources are assigned to different VPNs (to support the function identified in iii)). A layer 1 VPN with dedicated C-plane resources is called a Dedicated C-Plane Private Network (DCPN).

When the network provides service in a SUPN way, it would be enough to use SCPN. In this way, the customer can expect to receive L1 VPN service in an economical way.

When the U-plane resources are shared, it is invalid to have the functions that manage U-plane resources dedicated per VPN (i.e. a dedicated C-plane).

The customer of a DUPN may wish to take greater control over the management of his VPN. In such a case, resource availability information may be exchanged between CEs and the network, allowing CEs to make their own selection among the dedicated U-plane resources. In order to achieve this level of service, it may be necessary to dedicate C-plane resources to individual VPNs.

On the other hand, it is possible to have dedicated U-plane resources while sharing C-plane resources. The customer relies on the network to control connections in a common way. A lightweight solution would be to make the network maintain the mapping between the U-plane and the VPN. An example would be a link colouring technique by which the network would keep track of link ownership through a unified mechanism.

The C-plane uses the Data Communications Network (DCN), which is logically independent from the layer 1 U-plane. Items to be investigated both for C-plane and U-plane in order to address the above-mentioned features include:

- Reliability: The availability of the U-plane must be monitored by the C-plane, which is built on a network that may be independent of the U-plane. A failure in the C-plane must not directly affect the availability of any already established U-plane connections. When the C-plane is restored, it must be able to resynchronize with the U-plane.
- Routing: The route information relative to the U-plane must be held in the C-plane, which is built on a network that may be independent of the U-plane.

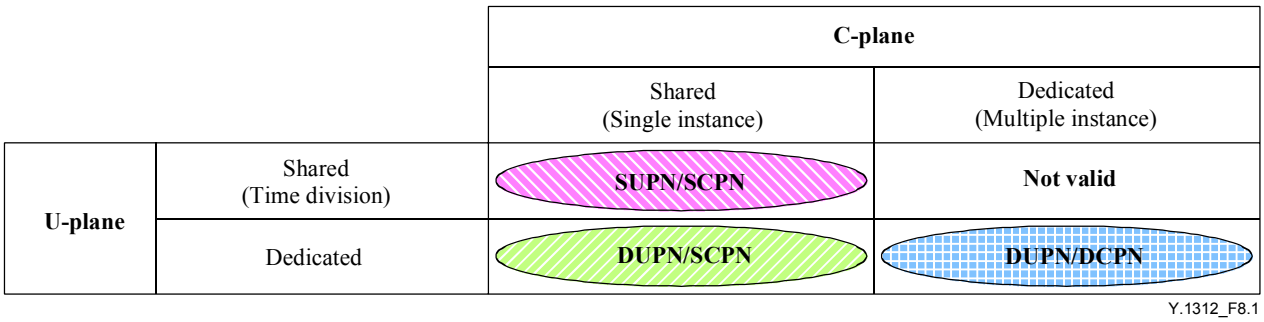


Figure 8-1/Y.1312 – U-plane – C-plane PN combinations

8.2 Description of service examples based on C-plane and U-plane combination

8.2.1 DUPN

DUPN is supported by a set of permanently allocated (or dedicated) resources. Details of the resources allocated to the partition can be made visible to the customer. Note that, in general, links

presented to the VPN will transit other flexibility points in the network that are not visible in the abstraction provided to the VPN.

Topology – If required, the geographic location of link ends and details of the route taken by the server layer (down to the duct level) can be provided as part of the service contract in the same way that the routing of dedicated private lines is provided today.

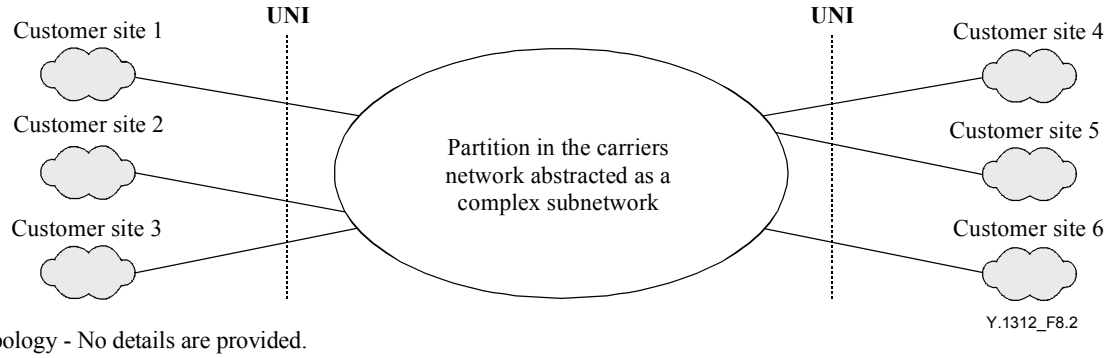
Link status – Can be provided for links within the network and links between CE and PE via a CNM interface.

Routing policy – The customer can provide routing constraints via the CNM interface.

Connection status and Performance Measurements (PMs) – The PMs can be provided on a per-connection basis via a CNM interface. Note that in some cases, this interface is referred to as a *Customer Service Management* (CSM) interface.

8.2.2 SUPN

SUPN is supported by a set of resources that are allocated, on demand, from a common pool with a guarantee of the minimum available and maximum allowed capacity between customer sites defined in the service contract. The resources in the carriers network are not visible to the customer. The VPN partition is presented as a set of links connecting each customer site to a subnetwork that represents the partition within the carrier's network as shown in Figure 8-2.



Topology - No details are provided.
Link Status - Can be provided for links between CE and PE via a CNM interface.
Connection status and PMs - The PMs can be provided on a per-connection basis via a CNM interface.
Note that in some cases this interface is referred to as a CSM (Customer Service Management) interface.

Figure 8-2/Y.1312 – Shared U-plane Private Network (SUPN)

8.3 L1 VPN functional model

Figure 8-3 shows the L1 VPN reference model including functional entities. Note that Figure 8-3 is a high level description of a functional model. Functional entities may be implemented by extended basic network control functional entities, such as signalling and routing, or may be implemented as separate functional entities. The functional entities in the network may be implemented in PE, P, or in the centralized fashion. Also, functional entities in the customer may be implemented in CE or in the centralized fashion. Details of functional entities are as follows.

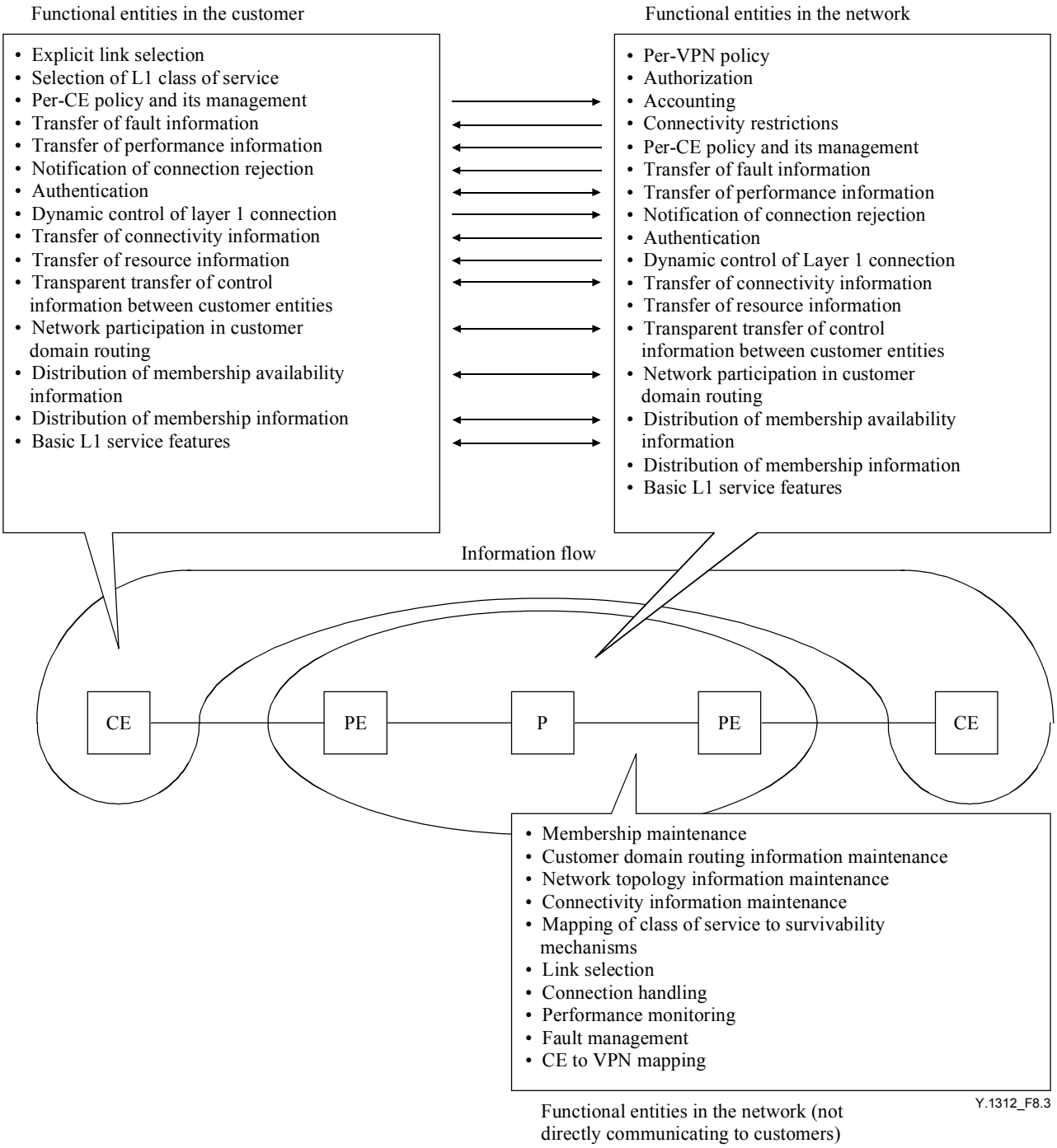


Figure 8-3/Y.1312 – L1 VPN reference model with functional entities

1) *Functional entities with information exchange between customer and network as indicated in the figure*

The following service requirements are realized by functional entities which are accompanied with information exchange between customer and network.

NOTE 1 – An actual information termination point may not reside in CE or PE. For example, proxies may be used. Thus, functional entities may not reside in CE or PE.

– Basic L1 service features: This service feature is realized by CE sending information to network, and network sending information to CE.

– Distribution of membership information: This service feature is realized by network detecting the addition/deletion (in terms of physical connectivity availability) of CE, and distributing information of this addition/deletion to the customer for that VPN.

– Distribution of membership availability information: This service feature is realized by CE informing the network about the ability or willingness, and the network informing the customer of that VPN about this information.
– Network participation in customer domain routing: This service feature is realized by customer informing the network about its domain's routing information (i.e. network topology information within site), and the network informing the customer of that VPN about this information. The network uses customer domain routing information in order to optimize routing.
– Authentication: This service feature is realized by the customer requesting the network to validate their access to network service, and the network responding to the customer about its validity.
– Transparent transfer of control information between customer entities: This service feature is realized by the customer transferring the control information to the network, and the network transparently transferring this control information to the customer.

2) *Functional entities with information flow from network to customer as indicated in the figure*

The following service features are realized by functional entities which are accompanied with information flow from network to customer.

– Transfer of resource information: This service feature is realized by the network informing the customer about topology view, performance, utilization and resource status.
– Transfer of connectivity information: This service feature is realized by the network informing the customer list of current active connections within the VPN. The network obtains information about the list of current active connections via functional entities for Dynamic control of Layer 1 connection.
– Notification of connection rejection: This service feature is realized by the network informing the customer about a reason for failure, when the network can not complete a service request.
– Transfer of performance information: This service feature is realized by the network informing the customer about performance information of a connection.
– Transfer of fault information: This service feature is realized by the network informing the customer about fault information (working or failure). Here, fault information includes about a connection, and may include U-plane and/or C-plane resources dedicated for a specific VPN.

3) *Functional entities with information flow from customer to network as indicated in the figure*

The following service features are realized by functional entities which are accompanied with information flow from customer to network.

– Dynamic control of layer 1 connection: This service feature is realized by the customer requesting the network to create, delete and modify connections. Note that when layer 1 connection control is realized by signalling type of mechanism, the information exchange becomes both ways, thus categorized as 1, since the remote CE receives the connection request that the local CE has sent.

NOTE 2 – At the request of a customer to network for dynamic control of layer 1 connection, information such as customer's explicit request on link selection (e.g. explicit route), or class of survivability, may be included. This is one of the possible forms that realize service features of explicit link selection and selection of L1 class of service.

– Per-CE policy and its management: This service feature is realized by the customer requesting the network to modify the per-CE policy.

4) *Functional entities in the network*

The following service features are realized by functional entities residing in the network.

– Connectivity restrictions: This service feature is realized by network accepting or rejecting the request from the dynamic control of layer 1 connection.

– Authorization: This service feature is realized by network preventing the user from performing unauthorized control of the network in the L1 VPN.

– Accounting: This service feature is realized by network recording quantitative information on usage.

– Per-VPN policy: This service feature is realized by network enforcing policy per VPN basis. The trigger to enforce policy may include request from a customer (e.g. via dynamic control of layer 1 connection) or failure.

In addition to functional entities directly communicating to customers, there are several additional functional entities within the provider network that support the L1 VPN service. Those functional entities include:

– Membership maintenance: The functional entity to maintain membership information, so that the provider can provide membership information to customers.

– Customer domain routing information maintenance: The functional entity to maintain customer domain routing information, so that the provider can participate in customer domain routing.

– Network topology information maintenance: The functional entity to maintain network topology information within the provider network, so that provider can route connections as well as provide topology information to customers.

– Connectivity information maintenance: The functional entity to maintain connectivity information within the provider network, so that provider can provide connectivity information to customers.

– Mapping of class of service to survivability mechanisms: The functional entity to map a requested class of service for a customer connection to the corresponding survivability mechanisms.

– Link selection: The functional entity to manage resources within the provider network, including route selection algorithm and connection admission control mechanisms.

– Connection handling: The functional entity to set up/delete/modify connections between CEs.

– Performance monitoring: The functional entity to monitor the performance of U-plane connections (link and connection), e.g., by power monitoring, BER monitoring and overhead byte monitoring.

– Fault management: The functional entity to handle faults within the network, including fault localization, recovery and notification.

– CE to VPN mapping: The functional entity that maps CE and VPN.

5) *Functional entities in the customer*

The following service feature is realized by the functional entity residing in the customer.

- Explicit link selection: This service feature is realized by the customer explicitly selecting a link or series of links to use for a connection that the customer likes to request, by using the resource information provided from the network.
- Selection of L1 class of service: This service feature is realized by the customer requesting a class of service on a per-connection basis.

Table 8-1 categorizes how each functional entity exchanges information, namely in U-plane, C-plane or M-plane. Note that U-plane, C-plane and M-plane in Table 6-1 means the plane over which the information can be transferred, rather than the plane to which the information belongs.

Table 8-1/Y.1312 – Mapping of functional entities with U/C/M plane

Functional entity	U-plane	C-plane	M-plane
Basic layer 1 service features	X		
Distribution of membership information		X	X
Distribution of membership availability information		X	X
Network participation in customer domain routing		X	X
Transparent transfer of control information between customer entities		X	X
Transfer of resource information		X	X
Transfer of connectivity information		X	X
Dynamic control of layer 1 connection		X	X
Authentication (see NOTE 1)		X	X
Notification of connection rejection		X	X
Transfer of fault information		X	X
Transfer of performance information			X
Per-CE policy and its management			X
NOTE 1 – When PE terminates information from CE for authentication, PE may communicate with the functional entity that actually performs the authentication (e.g., authentication server) in M-plane. NOTE 2 – There is a variety of ways to realize the functional entities mentioned herein. Functional entities may be realized by a distributed system, or by a centralized system.			

9 Security aspects

The information exchange between customer and network must be guaranteed in its integrity and confidentiality.

In addition, the network must provide services only to valid customers, by means of authentication and authorization, as mentioned in clause 7.

Annex A

Functions performed by the CE in a L1 VPN

This annex provides a more detailed description of the CE in the context of a L1 VPN.

The CE is a container that is visible at the service interface between a customer site and the network. The CE is a logical construct that hides the implementation and topology of the customer site. Therefore, the network has no visibility of the location of the functions contained within the CE.

The functions contained by the CE are:

Connection User (CU): This entity is the (client) application that uses a trail and interacts directly with G.805 access points by presenting and receiving adapted information. This is the point at which the payload is assembled (and disassembled).

Customer Call Agent (CCA): This is the entity that requests the network to establish or release connections for a CU or that accepts a connection establishment or release request from the network. It is also responsible for the transfer of the customer site topology between CEs or between the CE and the network.

The CE is attached to the PE within the network by a link. When viewed from the network, the CE represents the logical termination of the bearer connections in the link and the control plane messages as shown in Figure A.1.

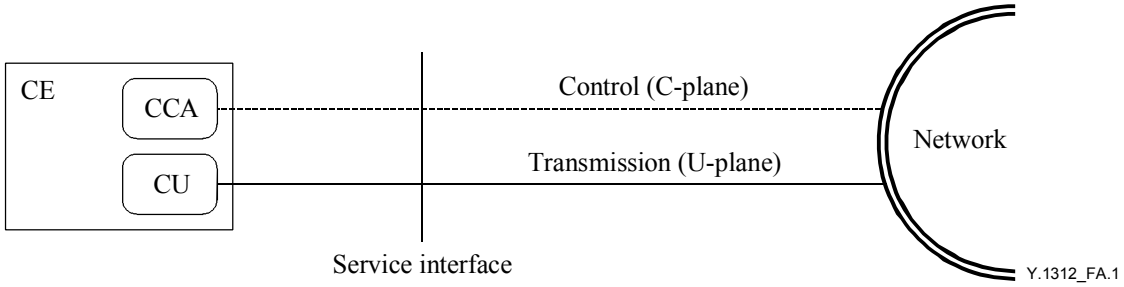


Figure A.1/Y.1312 – Relationship between the CE and the network

A CE may participate in more than one VPN, it may also access the public network, in this case the link may also be shared.

In the case of a nested L1 VPN shown in Figure A.2, the CU function is physically located in the end-CE. The CCA function associated with each CE is implemented within the customer site. The CCA makes a call request to the network in the context of the other CEs belonging to the same VPN that are also attached to that network. In this case, the CCA is also responsible for conveying the context of the original call request to the intermediated CCA. In the example network below, the CCA in CE_{p11} must convey the destination address (CE_{c2}) provided by the originating CCA (in CE_{c1}) to CE_{p12}.

In this case, provider 1 may share the VPN service from provider 2 among several customer VPNs. Provider 2 need not be aware of this sharing. Also the customer VPNs of provider 1 need not be aware that provider 1 is using a VPN from provider 2.

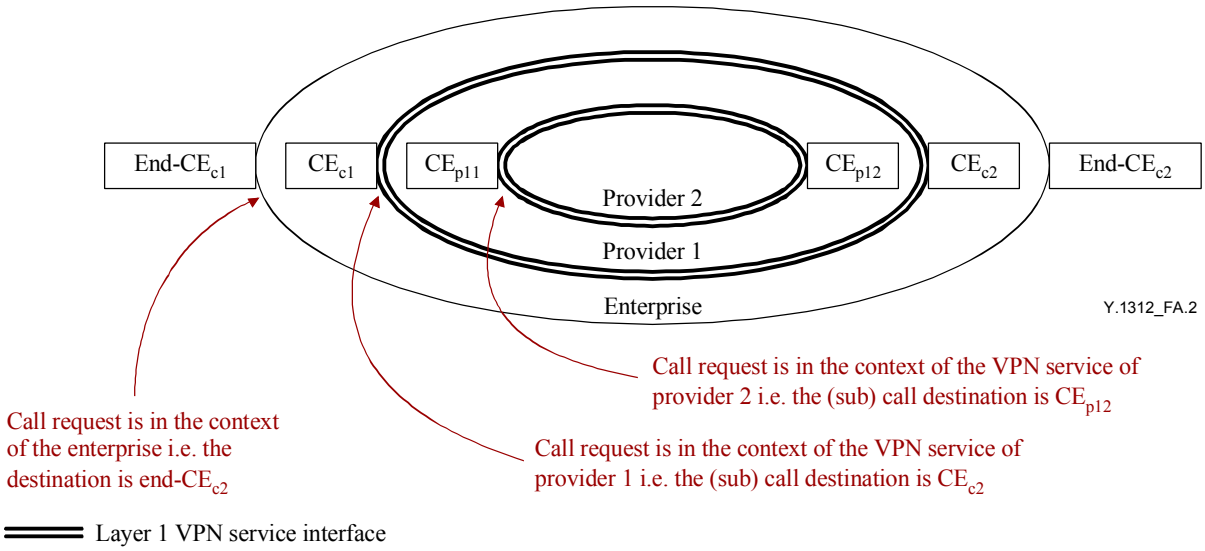


Figure A.2/Y.1312 – Example of a nested VPN application

Appendix I

Relationship with L2/L3 VPNs

I.1 Multipoint connectivity for L3/L2 VPN and layer 1 VPN

A layer 2 or 3 application may be associated with multiple Connection Users (CUs) (see Annex A). Each CU can support a point-to-point connection. Each connection exists between a pair of CUs (and not between more than two CUs). The basic requirement for layer 1 VPN is to support any-to-any point-to-point communication within the context of the VPN. Point-to-multipoint connectivity between the layer 2 or layer 3 applications using the CU is achieved by the use of multiple (layer 1) point-to-point connections.

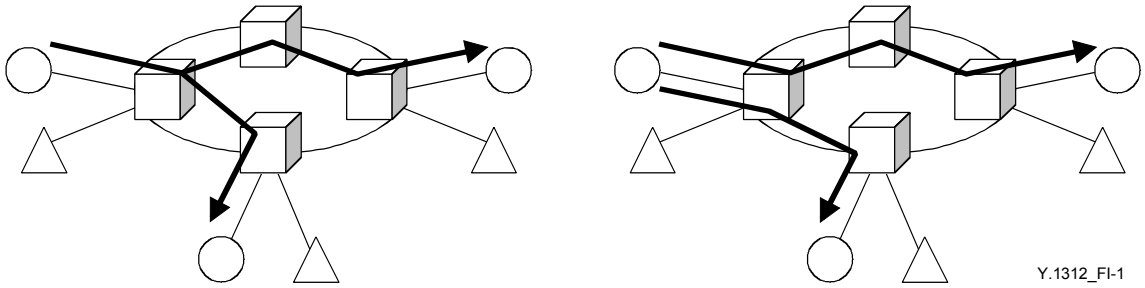
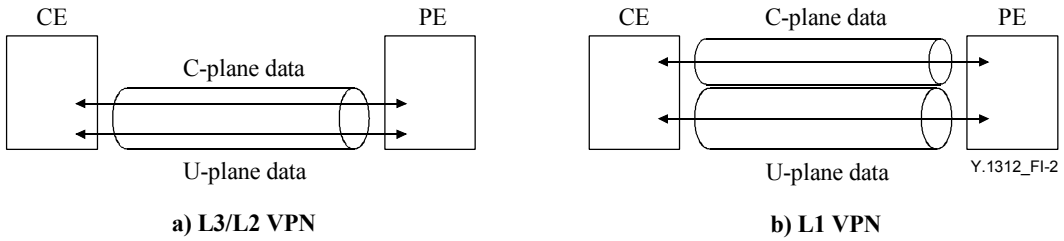


Figure I.1/Y.1312 – Multipoint connectivity for L3/L2 VPN and layer 1 VPN

I.2 C/U-planes for L3/L2 VPN and layer 1 VPN

The layer 1 U-plane transports the information of higher layers transparently. Therefore, unlike L3/L2 VPNs, it is not possible to decode control messages carried on the layer 1 U-plane. A physically separated C-plane network must be constructed in order to exchange control messages.



a) L3/L2 VPN **b) L1 VPN**

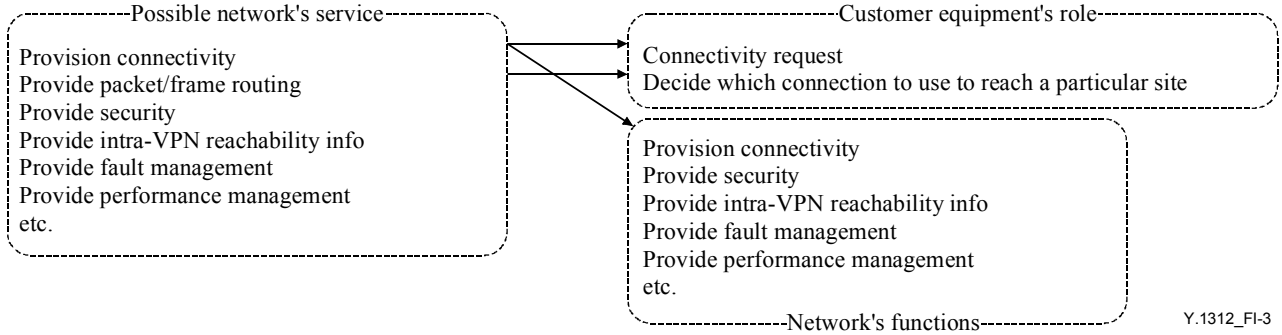
Figure I.2/Y.1312 – C/U-Planes for L3/L2 VPN and Layer 1 VPN

NOTE – In L2/L3 VPN, it would be possible to have a physically separated C-plane network, but that is not usual.

The service demarcation is between the CE and the network. If there are nested service interfaces, as in the case of nested VPNs, then Customer Call Agents (CCAs) (see Annex A), will be nested also as described in Annex A. No assumption of an implementation on the service provider side is made.

With layer 1 VPNs, in addition to the user plane and the control plane separation, the service is always connection-oriented. The CU is associated with the user plane. For any connection, there are exactly two CUs, one at each end. This is where the data from higher layers gets put into the layer 1 payload. The CCA is associated with the control plane. There is a CCA wherever there is an optical service interface across which a connection request can be made.

Figure I.3 shows further differences between network-based L3/L2 VPNs and network-based layer 1 VPN with respect to the role of customer equipment.



a) Network-based L3/L2 VPN **b) Network-based L1VPN**

Figure I.3/Y.1312 – Network and customer equipment functional differences

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, Internet protocol aspects and Next Generation Networks**
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2004