INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# Y.1313

(07/2004)

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

Internet protocol aspects – Transport

## Layer 1 Virtual Private Network service and network architectures

ITU-T Recommendation Y.1313

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.1313

## Layer 1 Virtual Private Network service and network architectures

### Summary

This Recommendation specifies functions and architectures to support Layer 1 VPN services described in ITU-T Rec. Y.1312, along with examples of detailed architectures.

### Source

ITU-T Recommendation Y.1313 was approved on 22 July 2004 by ITU-T Study Group 13 (2001-2004) under the ITU-T Recommendation A.8 procedure.

### Keywords

Architecture, Function, Layer 1 VPN, Layer 1, 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.

© ITU 2004

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

## CONTENTS

Page

Page

# ITU-T Recommendation Y.1313

## Layer 1 Virtual Private Network service and network architectures

## 1 Scope

This Recommendation describes the functions and architectures required to support the Layer 1 VPN services defined in ITU-T Rec. Y.1312. It provides some of the architecture examples related to the use of dedicated and shared C-Plane and U-Plane resources. The architecture also provides examples of networks where the functions are distributed or centralized.

## 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.

### 2.1 Normative references

| | |
|---|---|
| [ITU-T G.805] | ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*. |
| [ITU-T G.807] | ITU-T Recommendation G.807/Y.1302 (2001), *Requirements for Automatic Switched Transport Networks (ASTN)*. |
| [ITU-T G.7713.1] | ITU-T Recommendation G.7713.1/Y.1704.1 (2003), *Distributed Call and Connection Management (DCM) based on PNNI*. |
| [ITU-T G.7713.2] | ITU-T Recommendation G.7713.2/Y.1704.2 (2003), *Distributed Call and Connection Management: Signalling mechanism using GMPLS RSVP-TE*. |
| [ITU-T G.7713.3] | ITU-T Recommendation G.7713.3/Y.1704.3 (2003), *Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP*. |
| [ITU-T G.7714.1] | ITU-T Recommendation G.7714.1/Y.1705.1 (2003), *Protocol for automatic discovery in SDH and OTN networks*. |
| [ITU-T G.8080] | ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture for the Automatically Switched Optical Network (ASON)*. |
| [ITU-T Y.1311] | ITU-T Recommendation Y.1311 (2002), *Network-based VPNs – Generic architecture and service requirements*. |
| [ITU-T Y.1312] | ITU-T Recommendation Y.1312 (2003), *Layer 1 Virtual Private Network generic requirements and architecture elements*. |
| [IETF RFC 1771] | IETF RFC 1771 (1995), *A Border Gateway Protocol 4 (BGP-4)*. |
| [IETF RFC 2328] | IETF RFC 2328 (1998), *OSPF version 2*. |
| [IETF RFC 2748] | IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*. |

[IETF RFC 3472] IETF RFC 3472 (2003), *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions*.

[IETF RFC 3473] IETF RFC 3473 (2003), *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*.

[OIF UNI 1.0] OIF Implementation Agreement OIF-UNI01.0 (2001), *User Network Interface (UNI) 1.0 Signaling Specification*.

[OIF Signaling E-NNI 1.0] OIF Implementation Agreement OIF-E-NNI-Sig-01.0 (2004), *Intra-Carrier E-NNI Signaling Specification*.

## 2.2 Informative references

[IETF RFC 3474] IETF RFC 3474 (2003), *Documentation of IANA assignments for Generalized MultiProtocol Label Switching (GMPLS) Resource Reservation Protocol – Traffic Engineering (RSVP-TE) Usage and Extensions for Automatically Switched Optical Network (ASON).*

[IETF RFC 3475] IETF RFC 3475 (2003), *Documentation of IANA assignments for Constraint-Based LSP setup using LDP (CR-LDP) Extensions for Automatic Switched Optical Network (ASON).*

[IETF RFC 3476] IETF RFC 3476 (2003), *Documentation of IANA Assignments for Label Distribution Protocol (LDP), Resource ReSerVation Protocol (RSVP), and Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) Extensions for Optical UNI Signaling*.

# 3 Definitions

**3.1** This Recommendation makes use of the following terms defined in the following ITU-T Recommendations:

a) **L1 VPN (Layer 1 VPN)**: Refer to ITU-T Rec. Y.1312.

b) **CE**: Refer to ITU-T Rec. Y.1312.

c) **PE**: Refer to ITU-T Rec. Y.1312.

d) **P**: Refer to ITU-T Rec. Y.1312.

e) **Customer**: Refer to ITU-T Rec. Y.1312

f) **shared U-plane**: Refer to ITU-T Rec. Y.1312.

g) **dedicated U-plane**: Refer to ITU-T Rec. Y.1312.

h) **shared C-plane**: Refer to ITU-T Rec. Y.1312.

i) **dedicated C-plane**: Refer to ITU-T Rec. Y.1312.

j) **connection**: Refer to ITU-T Rec. Y.1312.

k) **Connection Point (CP)**: Refer to ITU-T Rec. G.805.

l) **link**: Refer to ITU-T Recs G.805 and Y.1312.

m) **link connection**: Refer to ITU-T Rec. G.805.

n) **subnetwork**: Refer to ITU-T Rec. G.805.

o) **trail**: Refer to ITU-T Rec. G.805.

p) **SNP**: Refer to ITU-T Rec. G.8080/Y.1304.

q) **SNPP**: Refer to ITU-T Rec. G.8080/Y.1304.

r) **SNP link connection**: Refer to ITU-T Rec. G.8080/Y.1304.

s) **SNPP link**: Refer to ITU-T Rec. G.8080/Y.1304.

**3.2** This Recommendation defines the following terms:

**3.2.1 Provider Centralized Controller (PCC)**: The centralized entity which performs some L1 VPN functions for the provider network.

**3.2.2 Customer Centralized Controller (CCC)**: The centralized entity which performs some L1 VPN functions for the customer network.

**3.2.3 provider entity**: The entity which performs some L1 VPN functions for the provider network. The provider entity may be PE/P or PCC, depending on implementation of functions.

**3.2.4 customer entity**: The entity which performs some L1 VPN functions for the customer network. The customer entity may be CE or CCC, depending on implementation of functions.

## 4 Abbreviations

This Recommendation uses the following abbreviations:

| | |
|---|---|
| AAA | Authentication, Authorization and Accounting |
| BGP | Border Gateway Protocol |
| CCC | Customer Centralized Controller |
| CE | Customer Edge |
| CNM | Customer Network Management |
| COPS | Common Open Policy Service |
| CORBA | Common Object Request Broker Architecture |
| CP | Connection Point |
| CUG | Closed User Group |
| DCN | Data Communications Network |
| E-NNI | External Network-to-Network Interface |
| EPL | Ethernet Private Line |
| FTP | File Transfer Protocol |
| GMPLS | Generalized Multi-Protocol Label Switching |
| I-NNI | Internal Network-to-Network Interface |
| LRM | Link Resource Manager |
| NNI | Network-Network Interface |
| OAM | Operation, Administration and Maintenance |
| OSPF | Open Shortest Path First |
| OTN | Optical Transport Network |
| P | Provider |
| PCC | Provider Centralized Controller |
| PDP | Policy Decision Point |

| | |
|---|---|
| PE | Provider Edge |
| PEP | Policy Enforcement Point |
| SNMP | Simple Network Management Protocol |
| SNP | Subnetwork Point |
| SNPP | Subnetwork Point Pool |
| SPC | Soft Permanent Connection |
| TCA | Threshold Crossing Alert |
| TL1 | Transaction Language 1 |
| TMF | TeleManagement Forum |
| UNI | User Network Interface |
| VPN | Virtual Private Network |
| XML | eXtensible Markup Language |

## 5 Classification of functions

In order to support service functions, the L1 VPN providing network must perform the following functions, as described in ITU-T Rec. Y.1312. Some of the functions can be optional.

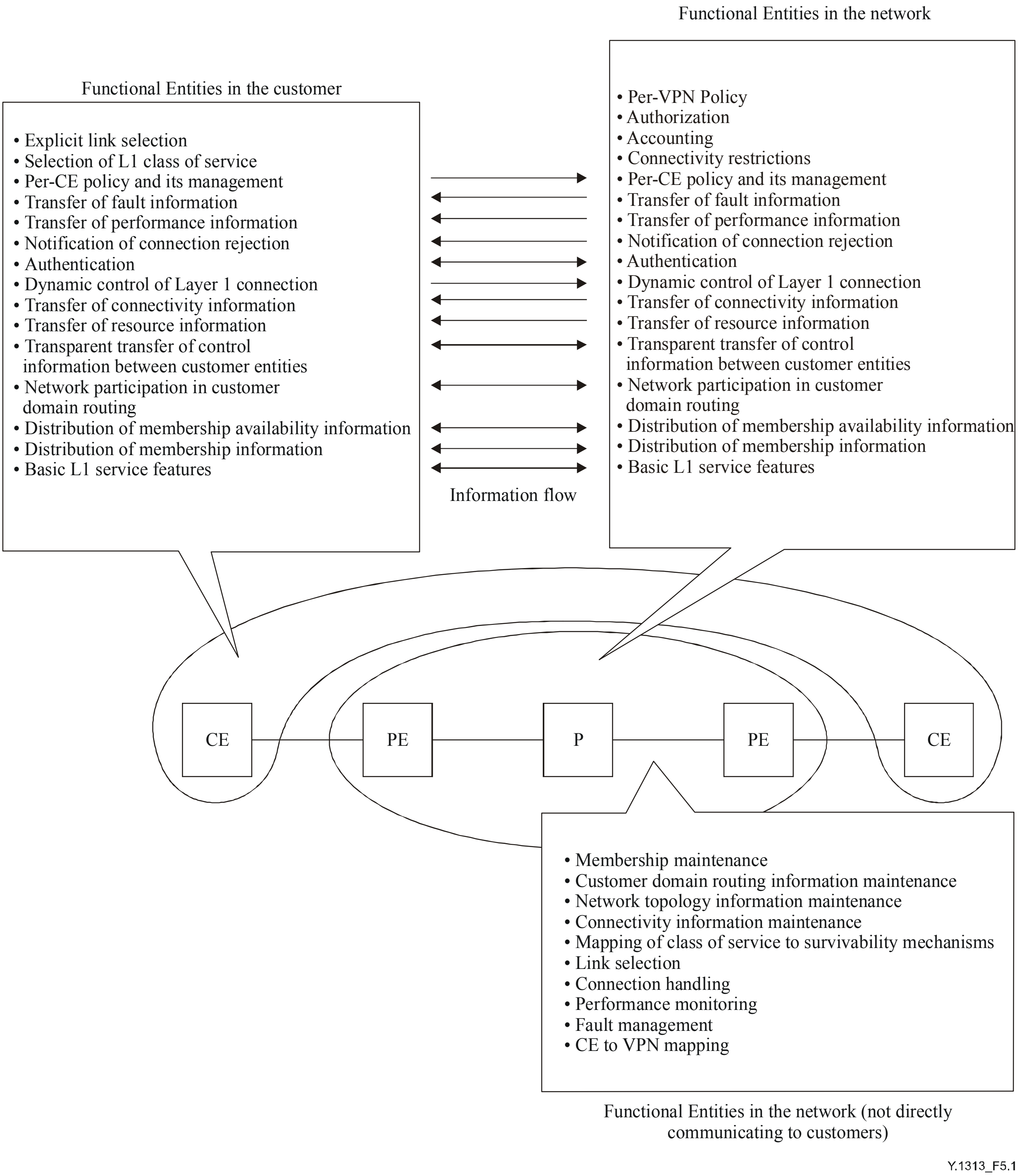

Functional Entities in the customer
• Explicit link selection
• Selection of L1 class of service
• Per-CE policy and its management
• Transfer of fault information
• Transfer of performance information
• Notification of connection rejection
• Authentication
• Dynamic control of Layer 1 connection
• Transfer of connectivity information
• Transfer of resource information
• Transparent transfer of control information between customer entities
• Network participation in customer domain routing
• Distribution of membership availability information
• Distribution of membership information
• Basic L1 service features
Information flow
Functional Entities in the network
• Per-VPN Policy
• Authorization
• Accounting
• Connectivity restrictions
• Per-CE policy and its management
• Transfer of fault information
• Transfer of performance information
• Notification of connection rejection
• Authentication
• Dynamic control of Layer 1 connection
• Transfer of connectivity information
• Transfer of resource information
• Transparent transfer of control information between customer entities
• Network participation in customer domain routing
• Distribution of membership availability information
• Distribution of membership information
• Basic L1 service features
CE
PE
P
PE
CE
• Membership maintenance
• Customer domain routing information maintenance
• Network topology information maintenance
• Connectivity information maintenance
• Mapping of class of service to survivability mechanisms
• Link selection
• Connection handling
• Performance monitoring
• Fault management
• CE to VPN mapping
Functional Entities in the network (not directly communicating to customers)
Y.1313_F5.1

**Figure 5-1/Y.1313 – L1 VPN reference model with functional entities**

Functional entities described in Figure 5-1 can be further categorized as follows, along with some other functions.

1) *Membership information maintenance*

This is related to the information exchange and maintenance involving membership information, and includes the following functions:

– distribution of membership information (between the customer and the network);

– distribution of membership availability information (between the customer and the network);

- membership maintenance (only within the network);
- CE to VPN mapping (only within the network).

2) *Routing information maintenance and route computation*

A) *Routing information maintenance*

This is related to the information exchange and maintenance involving topology information (about both for network and customer). Specifically, there are three types of information concerning routing information maintenance, namely, customer domain routing information, network topology information and connectivity information. Customer domain routing information may be maintained within the network and used for route optimization purpose, or may be transparently transferred between customer entities. Network topology information is maintained within the network, and partitioned portion of network topology information per VPN may be transferred to the customer. Topology information includes information about how links are connected, as well as resource utilization. Connectivity information means information concerning how CEs are connected to one another, and may include route information on which a connection is routed. Functional entities classified in routing information maintenance include functions to maintain three types of information mentioned above within the network, as well as functions to transfer these types of information between the customer and the network.

Routing information maintenance includes the following functions:

- network participation in customer domain routing (between the customer and the network);
- transfer of resource information per VPN (between the customer and the network);
- transfer of connectivity information per VPN (between the customer and the network);
- customer domain routing information maintenance (only within the network);
- network topology information maintenance (only within the network);
- connectivity information maintenance (only within the network);
- transparent transfer of control information between customer entities (between the customer and the network).

Note that transparent transfer of control information between customer entities is typically for transferring routing information, but may be used for transferring other information.

B) *Route computation*

Route computation is the mechanism to select links for a connection, by using topology information obtained by functions of routing information maintenance, as well as by using restriction and/or preference described in policies. After a route is calculated, a connection is established along this route by connection control functions.

Route computation includes the following functions:

- link selection (only within the network);
- explicit link selection (only within the customer).

3) *Connection control*

This is related to the information exchange and connection configuration involving connection setup/delete/modify request/response, and includes the following functions:

- dynamic control of Layer 1 connection (between the customer and the network);
- connection handling (only within the network);

- notification of connection rejection (between the customer and the network).

4) *Management*

This is related to the decision process as well as logging and error handling concerning the above-mentioned functions, and includes the following functions:

A) *AAA*

- Authentication (between the customer and the network).
- Authorization (only within the network).
- Accounting (only within the network).

B) *Policies*

Policies indicate how to behave to a particular event, including route computation and fault. Policies can be the input for route computation as well as OAM and fault handling. Policies relating to route computation include parameter setting relating what kind of connection should be preferred (e.g., weighting of each link). Policies relating to fault handling include indication of protection and restoration behaviour for a connection. Also, policies are applied for connection request admission control, including connectivity restriction between different VPNs and within the same VPN, as well as confirmation of requested L1 class of service against service contract.

Policies include the following functions:

- per-CE policy and its management (between the customer and the network);
- per-VPN policy (only within the network);
- connectivity restriction (only within the network);
- selection of L1 class of service (only within the customer);
- mapping of class of service to survivability mechanisms (only within the network).

C) *OAM and fault handling*

OAM and fault handling may use policies as inputs. For examples, protection and restoration behaviour may differ depending on policies for each connection and/or VPN.

OAM and fault handling includes the following functions:

- transfer of performance information (between the customer and the network);
- transfer of fault information (between the customer and the network);
- performance monitoring (only within the network);
- fault management (only within the network).

D) *Layer 1 VPN configuration check*

There should be some mechanisms to check that configuration is correctly made. Mechanisms for this function are for further study.

5) *Others*

Following is a list of non-L1 VPN specific functions required for the Layer 1 VPN in accordance with the above-mentioned functions:

- routing in control plane (e.g., DCN routing);
- discovery and maintenance of link resource information (e.g., LRM).

Note that detailed functions for accounting may defer depending on business scenarios. This requires further study. Also, note that these functional entities imply only functions that they perform, and do not imply any specific implementation. In addition, several functional entities may be implemented by the same mechanism. For example, "connection control" and "routing information maintenance" or "transfer of fault information" may be implemented by the same mechanism, when feedback information from connection control can be used to update routing information, as well as to inform fault.

## 6 Service scenarios, service features and required functions

### 6.1 Description of functions with service features

Clause 5 classifies functions into several building blocks. Among them, in order to provide L1 VPN services, connection control, AAA (except accounting), connectivity restriction of policies, routing information maintenance and route computation within the network, membership information maintenance within the network, OAM and fault handling within the network are essential functions, as described in ITU-T Rec. Y.1312. These functions enable customers to initiate a connection request between CEs within the same VPN, the provider to select the route for a connection, and the provider to manage the network.

If the customer would like to know the list of CEs within the same VPN, membership related functions need to be supported. This service feature is important especially when CEs participate in the VPN dynamically. If the customer would like to receive a differentiated service, capabilities to specify policies per VPN basis is required. Also, if CEs within the same VPN would like to receive different grade of service, then capabilities to specify per CE policy is required. With single administration, meaning every CE in the same VPN belonging to the same administration, per VPN policy and possibly per CE policy may be required. With multiple administrations, meaning CEs within the same VPN belonging to different administrations, it would be difficult to define one common policy over the whole VPN. If the customer would like to receive OAM or fault information, so that the customer can make decision to respond to failures, OAM and fault handling related functions are necessary between the customer and the network. If the customer would like to know provider internal topology so that the customer can enforce much more control on connection routing (e.g., advanced traffic engineering), then routing information requires to be informed to the customer. The customer then performs route computation for a new connection request. These service features are additional value-added features.

Note that per VPN policy is an essential feature that the provider must have, but customers need not necessarily use it. In this context, per VPN policy is a value-added service feature from customer's perspective.

**Table 6-1/Y.1313 – Functions with service features**

| Functions | | Service features |
|---|---|---|
| Membership information maintenance | | – Dynamic membership management |
| Routing information maintenance and route computation | | – Providing network design capability for customers (customer's participation in traffic engineering) |
| Connection control | | – Mandatory |
| Management | AAA | – Mandatory (except for accounting) |
| | Policies | – Connectivity restriction is mandatory<br>– Providing differentiated services, as well as different policies per CE |
| | OAM and fault handling | – Providing customers the ability to know what is happening within the network, by which customers can make their decision as to how to respond. |

### 6.2 Examples of service scenarios and required functions

Possible service scenarios are described, including some from ITU-T Rec. Y.1312, along with desired service features and required functions.

- *Content distribution (e.g., mirroring)*

  In this scenario, customers request large capacity to mirror the content based on necessity. Time-scale to request/release connections is within the range of hours, possibly daily or weekly scheduled basis. The number of CEs is expected to be relatively small. Each CE may belong to the same administration (mirroring within the same organization), or different administrations (mirroring with different organizations). Membership information tends to be static (mirroring to the same set of CEs every day or week). Customers are considered to be less involved in management of the optical network.

  Providing multiple point-to-point connections is a required feature, and network wide design, such as complex traffic engineering for dynamic traffic pattern, is not necessary.

  In addition to mandatory functions to support L1 VPN services, required functions could be OAM and fault handling. Customers may require per VPN policy when CEs are within the same administration, if they want to receive differentiated services.

- *Videoconference*

  In this scenario, a group of CEs is formed, and information for videoconference is transferred within them. Connections are necessary only while the videoconference is held. CEs within the same group may belong to different administrations. A group may be formed in a dynamic way, meaning dynamic participation of CEs, as well as dynamic creature of the group itself. Customers are considered to be less involved in management of the optical network. This is similar to a public service with CUG (Closed User Group).

  In this scenario, it could be difficult to define one common policy over the whole VPN, especially if CEs belong to different administrations.

  In addition to mandatory functions to support L1 VPN services, required functions could be membership related functions. OAM and fault handling related functions may be required to provide an additional service feature.

- *Carrier's carrier*

  In this scenario, one carrier receiving another carrier's L1 VPN service provides its own services. The number of CEs could be relatively large. Traffic may vary with relatively short interval (e.g., day time and night time traffic variation), as well as with long-term that usually involves network topology design. Customers are expected to be relatively used to managing the network by them.

  Capability to configure network wide topology for customers is required. Also, advanced policies per VPN and possibly per CE are required in order to well manage the network.

  In addition to mandatory functions to support L1 VPN services, required functions could be OAM and fault handling, and policy related function. Membership related functions may also be required. Routing related functions with limited topology exchange may be desired, depending on service requirements.

- *Multiservice backbone*

  In this scenario, one service department of a carrier receiving the carrier's L1 VPN service provides different kinds of higher-layer services. Traffic may vary with relatively short interval (e.g., day time and night time), as well as with long-term that usually involves network topology design. Customers are expected to be relatively used to managing the network by them.

Capability to configure network wide topology for customers is required. Also, advanced policies per VPN and possibly per CE are required in order to well manage the network.

In addition to mandatory functions to support L1 VPN services, required functions could be OAM and fault handling, and policy related function. Membership related functions may also be required. Compared to carrier's carrier, more detailed topology information exchange between the customer and the network is expected. Customers may perform path computation by using topology information provided from the provider.

**Table 6-2/Y.1313 – Mapping service scenarios with required functions**

| | **Conditions** | | | | | **Required functions** |
|---|---|---|---|---|---|---|
| | **Number of CEs** | **Traffic pattern** | **Advanced network operation by customers** | **Membership** | **Administration** | |
| Content distribution | Small | On-off | Less likely | Static | Single/Multiple (CEs may belong to the same administration or different administrations.) | OAM and fault handling, (policies) |
| Video-conference | Small-Large | On-off | Less likely | Dynamic | Multiple (CEs belong to different administrations.) | (OAM and fault handling), membership information maintenance |
| Carrier's carrier | Large | Short-term and long-term variation | Likely | Static | Single (Every CE belongs to the same administration.) | OAM and fault handling, policies, (membership information maintenance), (routing information maintenance and route computation) |
| Multiservice backbone | Large | Short-term and long-term variation | Likely | Static | Single (The provider and the customer are within the same administration.) | OAM and fault handling, policies, (membership information maintenance), routing information maintenance and route computation |

## 7 Architecture classification

Based on functional implementations, architectures are classified as distributed, centralized, or hybrid. In the hybrid architecture, some functions are distributed while some other functions are centralized.

Although there could be some relationship between the provider network side architecture and the customer network side architecture, these two network architectures will be described separately in 7.1 and 7.2.

Functions for management are separately discussed in 7.3.

### 7.1 Provider network architecture

In the provider network architecture, some functions involve information exchange with customers, and others involve information exchange or actions only within the provider network.

### 1) Distributed architecture

In the distributed architecture, functions of membership information maintenance, routing information maintenance and route computation, and connection control are distributed, as well as some functions for management are distributed. In the distributed architecture, the PE is the entity to communicate with the customer entity, which is typically the CE.

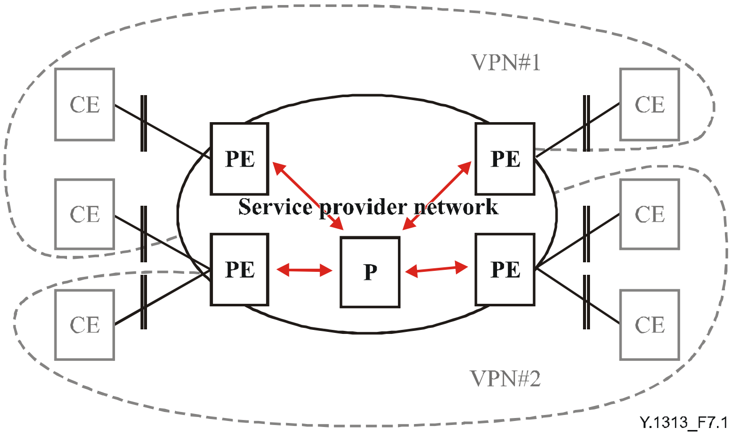


**Figure 7-1/Y.1313 – Distributed L1 VPN provider network architecture**

Some more detailed explanation of the distributed provider network architecture is described as follows, along with how functions of membership information maintenance, routing information maintenance and route computation, and connection control described in clause 5 are realized in terms of interaction and information exchange between the PE and the P.

- *Membership information maintenance*

The PE contains membership information, whereas the P does not necessarily contain membership information. A PE may directly communicate with remote PEs, by which the PE can obtain all membership information for each VPN. Note that a PE does not need to obtain membership information of a specific VPN, if the PE is not connected with customer entities belonging to that VPN. This increases scalability.

The PE may also communicate with customer entities attached to that PE, in order to obtain membership information of that VPN, and to provide membership information of the VPN to which those customer entities belong.

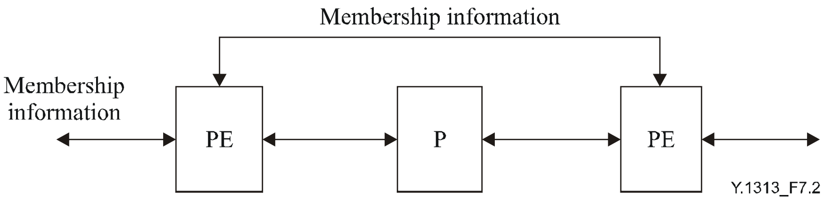


**Figure 7-2/Y.1313 – Membership information maintenance**

- *Routing information maintenance and route computation*

A) *Routing information maintenance*

There are three kinds of information that belong to routing information, as described in clause 5, namely, customer domain routing information, network topology information and connectivity information. These kinds of information may be conveyed by the same instance/mechanism, or different instances/mechanisms.

a) *Customer domain routing information*

When the network participates in customer domain routing, the PE contains customer domain routing information. On the other hand, the P does not necessarily contain customer domain routing information. A PE may directly communicate with remote PEs to obtain the whole customer domain routing information for each VPN. Note that a PE does not need to obtain customer domain routing information of a specific VPN, if the PE is not connected with customer entities belonging to that VPN. This increases scalability.

At the same time, the PE communicates with customer entities attached to that PE, in order to obtain routing information of those customer domains, and to provide customer domain routing information of the VPN to which those customer entities belong.

When transparent transfer of control information between customer entities is desired, neither the PE nor the P necessarily contains customer domain routing information. The PE may simply provide tunnelling mechanisms for customer domain routing information to transparently flow between customer entities.

b) *Network topology information*

Both of the PE and the P contain network topology information. The PE and the P communicate with connected PEs and Ps.

At the same time, the PE may communicate with customer entities attached to that PE, in order to provide topology information of the provider network. Note that this is typically applicable to dedicated U-Plane case. Information transferred to customer entities is restricted to the topology dedicated for the VPN to which those customer entities belong. Also, information transferred to customer entities may be abstracted (e.g., hiding the detailed topology).

c) *Connectivity information*

The PE contains connectivity information, whereas the P does not necessarily contain connectivity information. A PE may directly communicate with remote PEs, by which the PE can obtain all connectivity information for each VPN. Note that a PE does not need to obtain connectivity information of a specific VPN, if the PE is not connected with customer entities belonging to that VPN. This increases scalability.

The PE may also communicate with customer entities attached to that PE, in order to obtain connectivity information of that VPN, and to provide connectivity information of the VPN to which those customer entities belong.

B) *Route computation*

A route may be calculated by the CE and specified, for example, within a connection control request. Or, a route may be calculated by the PE, or by the PE and the P.

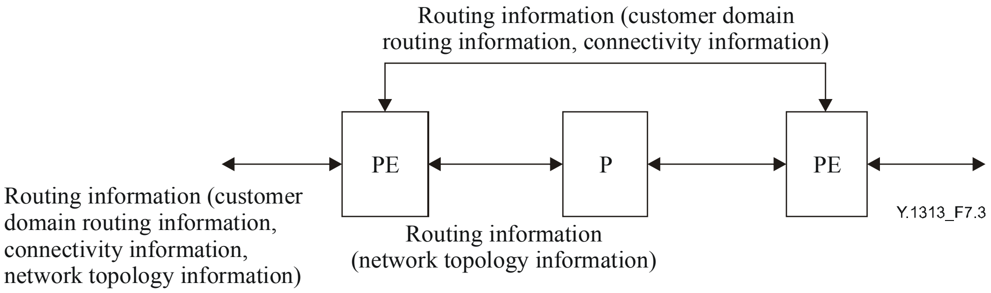

Routing information (customer domain routing information, connectivity information)
PE
P
PE
Routing information (customer domain routing information, connectivity information, network topology information)
Routing information (network topology information)
Y.1313_F7.3

**Figure 7-3/Y.1313 – Routing information maintenance and route computation**

- *Connection control*

The PE and the P contain connection control related information. The PE and the P communicate with connected PEs and Ps. Also, there could be direct information exchange related to connection control between PEs, for example, VPN specific connection control.

At the same time, the PE communicates with customer entities attached to that PE, in order to receive connection requests from those customer entities, and to send connection requests to customer entities of the other end, when necessary.

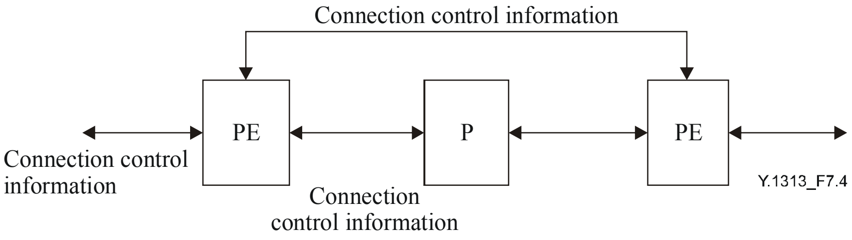

Connection control information
PE
P
PE
Connection control information
Connection control information
Y.1313_F7.4

**Figure 7-4/Y.1313 – Connection control**

Note that mechanisms or protocols to exchange information within the provider network (between PEs, a PE and a P, and Ps) and between the provider network and the customer network (between a PE and a customer entity) may be different for membership information maintenance, routing information maintenance and connection control.

**2) Centralized architecture**

In the centralized architecture, functions of membership information maintenance, routing information maintenance and route computation, and connection control are centralized, as well as some functions for management are centralized. The centralized entity can be called as a Provider Centralized Controller (PCC). In the centralized architecture, the PCC is the entity to communicate with the customer entity, which is typically the CCC (Customer Centralized Controller).

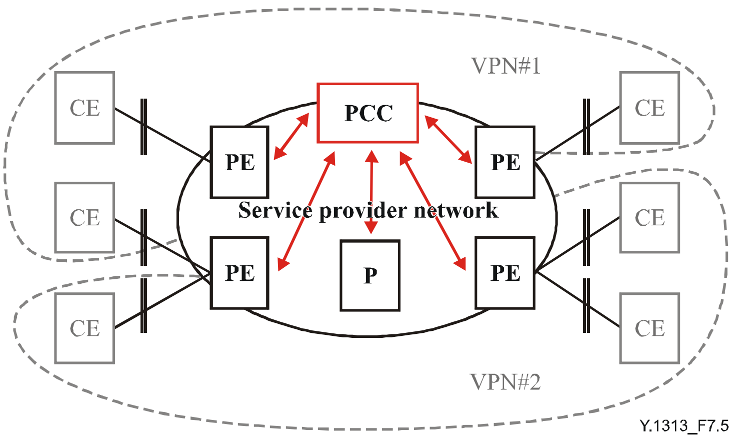


**Figure 7-5/Y.1313 – Centralized L1 VPN provider network architecture**

Some more detailed explanation of the centralized provider network architecture is described as follows, along with how functions of membership information maintenance, routing information maintenance and route computation, and connection control are realized in terms of interaction and information exchange among the PE, the P and the PCC.

- *Membership information maintenance*

The PCC contains membership information, whereas the PE and the P do not necessarily contain membership information. The PCC may communicate with customer entities, in order to obtain membership information, as well as to transfer membership information.

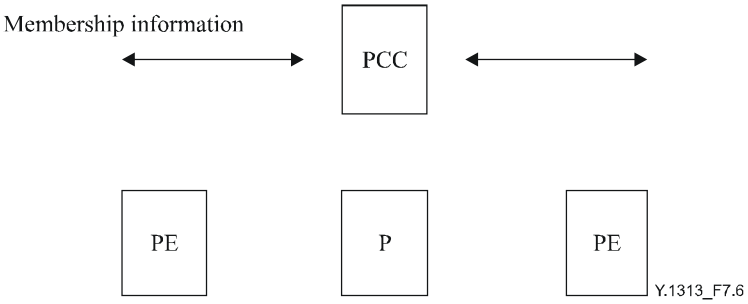


**Figure 7-6/Y.1313 – Membership information maintenance**

- *Routing information maintenance and route computation*

A) *Routing information maintenance*

There are three kinds of information that belong to routing information, as described in clause 5, namely, customer domain routing information, network topology information and connectivity information.

a) *Customer domain routing information*

When the network participates in customer domain routing, the PCC contains customer domain routing information, but the PE and the P do not necessarily need to contain customer domain routing information.

When transparent transfer of control information between customer entities is desired, the PCC does not necessarily need to contain customer domain routing information. The PCC simply passes the information received from a particular entity to one or more other entities.

b) *Network topology information*

The PCC, the PE and the P contain network topology information. The PCC communicates with PEs and/or Ps, and obtains whole network topology information. The PE and the P contain local topology information, but do not necessarily contain topology information of the whole network. At the same time, the PCC may communicate with customer entities, in order to provide topology information of the provider network. Note that this is typically applicable to dedicated U-Plane case. Information transferred to customer entities is restricted to the topology dedicated for the VPN to which those customer entities belong. Also, information transferred to customer entities may be abstracted (e.g., hiding the detailed topology).

c) *Connectivity information*

The PCC contains connectivity information, but the PE and the P do not necessarily contain connectivity information.

B) *Route computation*

A route may be calculated by the CE and specified, for example, within a connection control request. Or, a route may be calculated by the PCC.

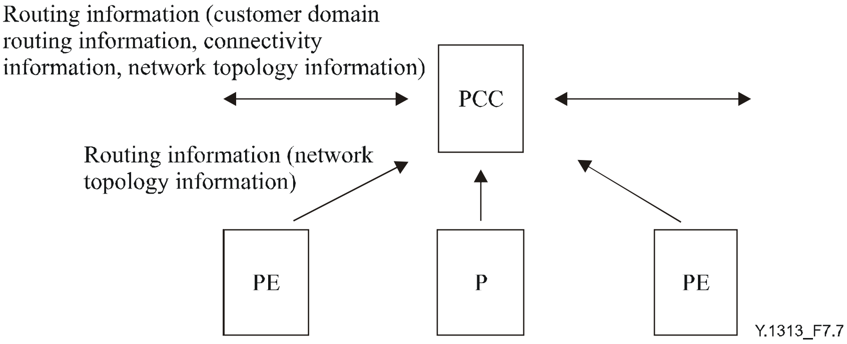

Routing information (customer domain routing information, connectivity information, network topology information)
PCC
Routing information (network topology information)
PE
P
PE
Y.1313_F7.7

**Figure 7-7/Y.1313 – Routing information maintenance and route computation**

- *Connection control*

The PCC, the PE and the P contain connection control information. The PCC communicates with customer entities to receive connection requests, and then the PCC communicates with PEs and Ps to set up connections. Note that the PE and the P contain nodal connection information (e.g., nodal cross-connect information), but do not necessarily contain whole connection information (e.g., explicit route information).

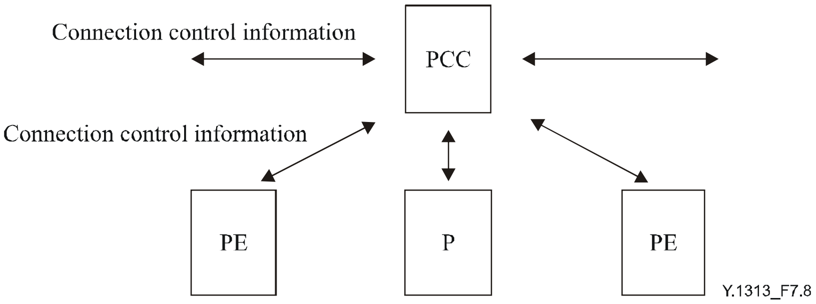

Connection control information
PCC
Connection control information
PE
P
PE
Y.1313_F7.8

**Figure 7-8/Y.1313 – Connection control**

### 3) Hybrid architecture

In the hybrid architecture, some functions of membership information maintenance, routing information maintenance and route computation, and connection control are distributed, and some other functions are centralized.

There are various types for the hybrid architecture. Essentially, in the hybrid provider network architecture, functions to communicate with the customer are hybrid, meaning some functions are centralized (i.e., PCC and CCC communication) and some others are distributed (i.e., PE and CE communication), and/or functions within the provider network (i.e., PE/P and PCC communication) are hybrid.

One example is distribution of functions where L1 VPN specific service functions, such as membership information maintenance, as well as management functions are centralized, while common functions to provide L1 connections, such as connection control, are distributed.

## 7.2 Customer network architecture

### 1) Distributed architecture

Every CE has one or more entities which perform control functions, and the CE is controlled by corresponding entities. In the distributed architecture, the CE is the entity to communicate with the provider entity, which is typically the PE.

In the distributed architecture, functions of membership information maintenance, routing information maintenance and route computation, and connection control are distributed.

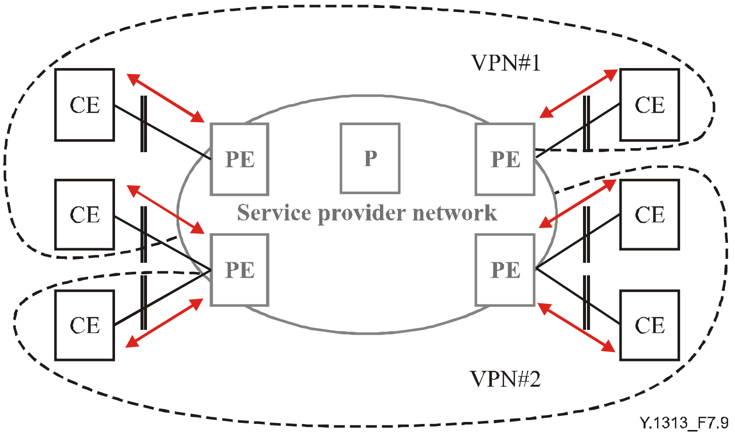


**Figure 7-9/Y.1313 – Distributed L1 VPN customer network architecture**

### 2) Centralized architecture

A centralized entity performs control functions required on behalf of more than one CE connected to the provider network.

In the centralized architecture, a Customer Centralized Controller (CCC) is the entity to communicate with the provider entity, which is typically the PCC. In some cases, the CCC only transfers control information requested from CEs to the provider entity. In other cases, the CCC can participate in control functions but CEs are always controlled by the CCC; a typical example of which is that these CEs are only for receiving connections from other CEs such as CCCs receiving access from active CEs.

In the centralized architecture, functions of membership information maintenance, routing information maintenance and route computation, and connection control are centralized.

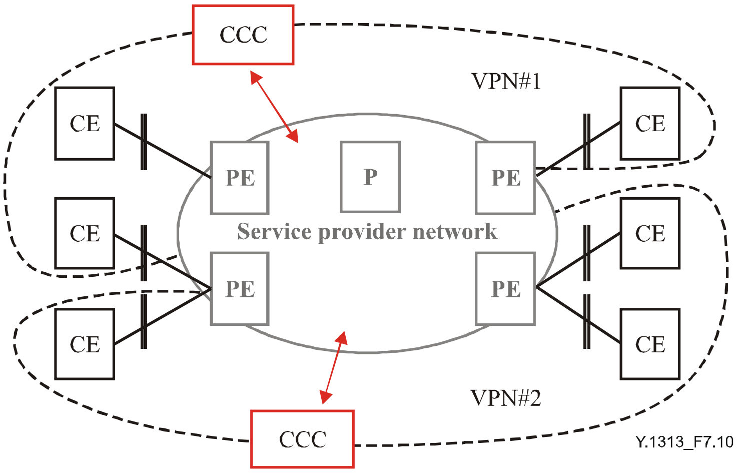


**Figure 7-10/Y.1313 – Centralized L1 VPN customer network architecture**

### 3) Hybrid architecture

In the hybrid architecture, some functions of membership information maintenance, routing information maintenance and route computation, and connection control are distributed, while some functions are centralized.

## 7.3 Management architecture

There are two aspects for management. One is management by the provider, and the other is management by the customer.

### 7.3.1 Provider management architecture

Some functions of management are centralized independently from how functions of membership information maintenance, routing information maintenance and route computation, and connection control are distributed (i.e., centralized or distributed). Typical examples are authorization and accounting.

Policies contain two entities. One entity is for decision, and the other entity is for enforcement. The former is called PDP (Policy Decision Point), and the latter is called PEP (Policy Enforcement Point). PDP and PEP may be located differently in the network.

Table 7-1 describes a typical example of how management functions are distributed, when functions of membership information maintenance, routing information maintenance and route computation, and connection control are distributed and centralized, respectively.

**Table 7-1/Y.1313 – Distribution of management functions**

| | **Distributed provider network architecture** | **Centralized provider network architecture** |
|---|---|---|
| AAA | Centralized (Note 1) | Centralized |
| Policies | PDP: Distributed or centralized<br>PEP: Distributed | PDP: Centralized<br>PEP: Centralized |
| OAM and fault handling | Distributed or centralized (Note 2) | Centralized (Note 3) |
| NOTE 1 – Authentication may be distributed, meaning that PEs identify which customer entity they are communicating with.<br>NOTE 2 – Some functions, such as performance monitoring, may be always distributed.<br>NOTE 3 – Some functions, such as functions for protection and restoration, may be distributed. | | |

### 7.3.2 Customer management architecture

The customer may have an interface to the provider's management system. It is the Customer Network Management (CNM) interface. The customer can delegate the capabilities of this interface to one or more of its CEs in part or in whole. See Figure 7-11 for a depiction of these interfaces.

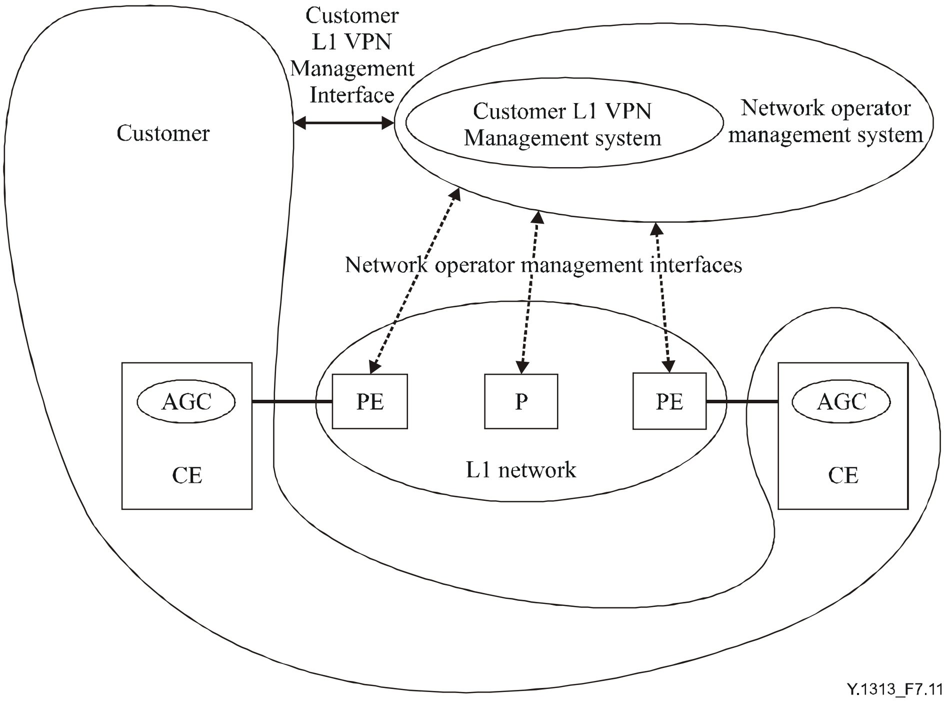


**Figure 7-11/Y.1313 – Interfaces between the customer and the network**

The functions of the CNM interface are:

- Similar functionalities with the PCC and the CCC communication described in 7.1, item 2) (i.e., request PE-PE soft-permanent connections within the customer's L1 VPN, view the topology of dedicated links assigned to customer's L1 VPN, query the status of dedicated links assigned to customer's L1 VPN, query the status of membership information).
- Authenticate and authorize customer access.
- Request the addition or removal of a CE, a shared link, or a dedicated link.
- Test the dedicated links assigned to the customer's L1 VPN.

- Set thresholds for Threshold Crossing Alerts (TCAs) for dedicated links assigned to the customer's L1 VPN.
- Report alarms and TCAs for dedicated links assigned to the customer's L1 VPN.
- Query and report performance information for dedicated links assigned to the customer's L1 VPN.
- Trace a connection across the customer's L1 VPN.
- Report billing information relative to the customer's L1 VPN.

# 8 Layer 1 VPN functional architecture concepts

## 8.1 Architecture constructs

### 8.1.1 U-Plane construct

A link connection is a transport entity capable of transferring information between two connection points (CPs), where a connection point refers to the input-output function of the link connection. Examples of link connection are VC-3 and VC-4.

A series of contiguous link connections and subnetwork connections can be compounded to form a serial-compound link. In this Recommendation, the term link will often be used as a short form for serial-compound link. Note that the switching matrix of a cross-connect is an example of a subnetwork.

Multiple link connections with CPs on the same two subnetworks respectively can also be compounded in parallel. This is called a link bundle.

Links are constructed based on the server layer trails in the U-Plane. Links are the anchor points for providing Layer 1 VPN management functions, especially fault and performance management.

### 8.1.2 C-Plane construct

A subnetwork point (SNP) link connection is a control relationship between two SNPs. SNPs are C-Plane entities which can be bound to U-Plane CPs. SNP link connections exist for the purpose of routing and unlike links, cannot transfer information by themselves.

All SNP-CP potential associations are determined by configuration, while actual associations are determined at the time a connection is made. When a SNP gets bound to a CP, their corresponding links also get bound.

Multiple SNP link connections with SNPs on the same two subnetworks respectively can be compounded in parallel to form a subnetwork point pool (SNPP) link. All SNP link connections within a SNPP link are treated the same for the purpose of routing (in GMPLS equivalent terms, a SNPP link corresponds to a TE link).

Furthermore, in ITU-T Rec. Y.1311, VPNs are scoped to be "port-based" only. In this architecture, Layer 1 VPNs are port-based too, where a Y.1311 port is instantiated to a SNPP.

### 8.1.3 M-Plane construct

The U-Plane and C-Plane constructs defined above are accessible in the M-Plane. As a result, the M-Plane has two different but related views on network resources, a C-Plane view and a U-Plane view. This is shown in Figure 8-1.

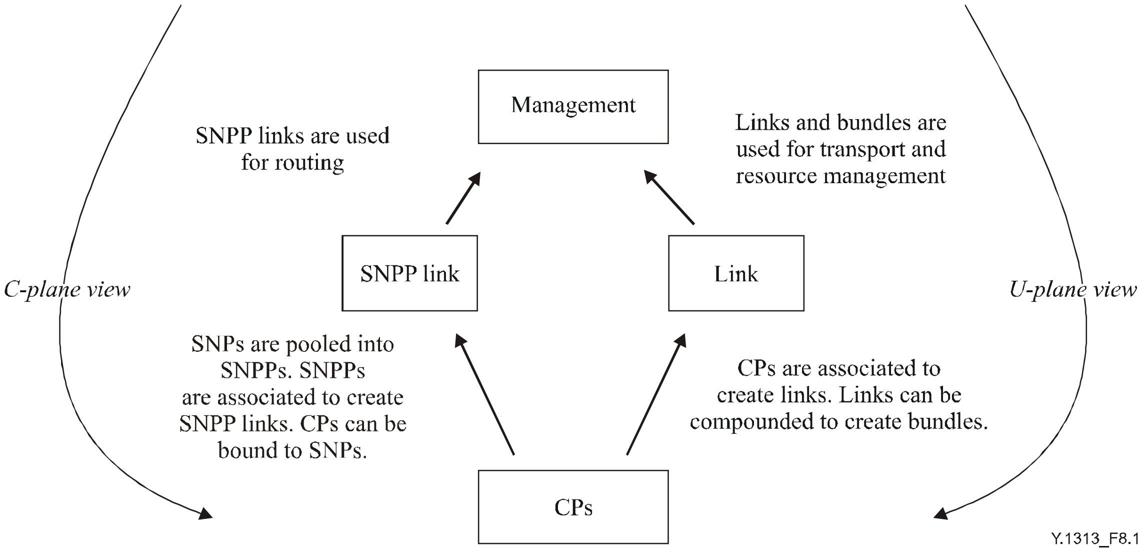

Management
SNPP links are used for routing
Links and bundles are used for transport and resource management
SNPP link
Link
C-plane view
U-plane view
SNPs are pooled into SNPPs. SNPPs are associated to create SNPP links. CPs can be bound to SNPs.
CPs are associated to create links. Links can be compounded to create bundles.
CPs
Y.1313_F8.1

**Figure 8-1/Y.1313 – Links for U-Plane and SNPP links for C-Plane**

## 8.2 Resource allocation schemes

### 8.2.1 Shared and dedicated U-Plane

The Layer 1 VPN service architecture from ITU-T Rec. Y.1312 demands that shared U-Plane resources and dedicated U-Plane resources are supported. Shared U-Plane resources mean that resources are used by multiple VPNs in a time-sharing manner. Dedicated U-Plane resources mean that resources are allocated exclusively to a VPN for its lifetime.

From the point of view of U-Plane constructs, a shared link is a link configured to be used by more than one given Layer 1 VPN. A dedicated link is a link configured to be used by one and only one Layer 1 VPN.

From the point of view of C-Plane constructs, a SNPP link must be configured to be used by only one Layer 1 VPN – in other words, SNPP links are not shared. The SNPs in a SNPP assigned to a Layer 1 VPN can only be bound to the CPs assigned to the same Layer 1 VPN on a shared or dedicated basis.

As a special case, a publicly shared link is a link configured to be used by any Layer 1 VPN. If a SNPP has not been assigned to a Layer 1 VPN, then its SNPs can only be bound to publicly shared CPs. This ensures compatibility with non-Layer 1 VPN links.

Note that this notion applies not only within the provider network, but also between the CE and the PE.

Figure 8-2 depicts an example with two Layer 1 VPNs. Layer 1 VPN A has two dedicated CPs. Layer 1 VPN B has two dedicated CPs. Layer 1 VPN A and Layer 1 VPN B share two CPs. In the last case, the binding of a CP to a SNP in one Layer 1 VPN will not be possible if the CP is already bound to a SNP in the other Layer 1 VPN – the first SNP is then said to be busy.

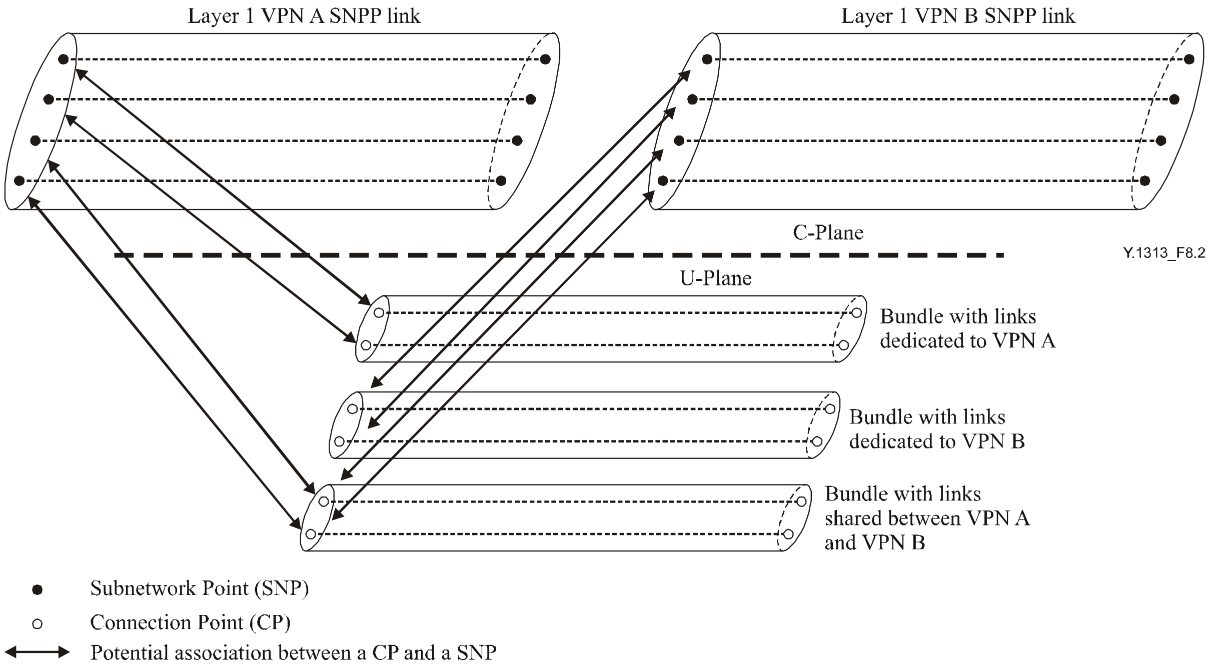

Layer 1 VPN A SNPP link
Layer 1 VPN B SNPP link
C-Plane
Y.1313_F8.2
U-Plane
Bundle with links dedicated to VPN A
Bundle with links dedicated to VPN B
Bundle with links shared between VPN A and VPN B
● Subnetwork Point (SNP)
○ Connection Point (CP)
Potential association between a CP and a SNP

**Figure 8-2/Y.1313 – Relationship between U-Plane CPs and C-Plane SNPs**

### 8.2.2 Shared and dedicated C-Plane

There are two forms for C-Plane resource allocation for each VPN, namely shared and dedicated as described in ITU-T Rec. Y.1312. In dedicated C-Plane resources, different C-Plane resources are assigned to different VPNs, while in shared C-Plane resources, the same C-Plane resources may be used for the control of multiple VPNs.

#### 1) Dedicated C-Plane

In this form, U-Plane resources are typically dedicated, and resource availability information of the customer domain as well as the provider network may be exchanged between the customer and the network, allowing customers to make their own link selection among the dedicated U-Plane resources, as described in ITU-T Rec. Y.1312. Here, the resource availability information of the provider network may be abstracted, in a sense that customers may be provided not exactly the same U-Plane resource information that are dedicated within the provider network. The level of abstraction may vary depending on the service contract between the customer and the provider. Note that there could be a service contract in which a whole provider network can be considered as one node.

One way to implement dedicated C-Plane is to allocate different instances and databases for each VPN, e.g., virtual router. Databases for membership information, routing information and connection control, as well as policy, are dedicated. Customers communicate dedicated instances for exchanging membership information, routing information and connection control information.

To forward information received from customers, network has to have a function to identify to which VPN information should belong. Methods for address disambiguation mentioned in 8.3.2 may be used for this purpose.

Within the provider network, shared instances and databases could be used. In this case, information exchange between dedicated databases/instances and shared databases/instances is expected. Address translation may be required. Also, information filtering from shared databases to dedicated databases may be required.

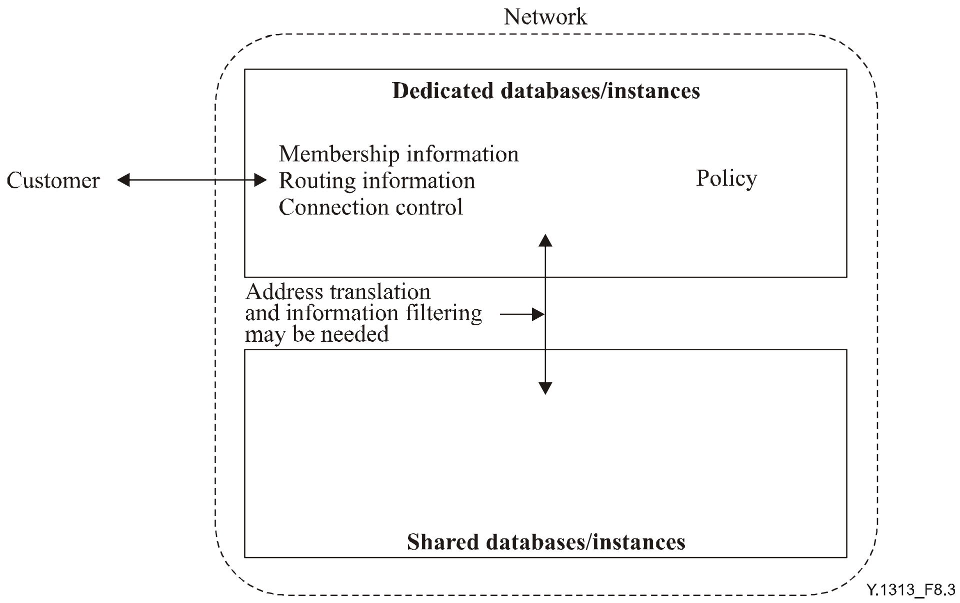


**Figure 8-3/Y.1313 – Dedicated C-Plane example**

Another type of C-Plane resource is control links. Control links are used to transfer control messages related to resource management, membership maintenance, routing information, and connection control. A control link can be dedicated to a Layer 1 VPN.

**2) Shared C-Plane**

In Shared C-Plane, address space is common over all VPNs within the provider network.

In this form, U-Plane resources are dedicated or shared.

One way to implement shared C-Plane is to allocate the same instance and database for all VPNs. However, membership information and policy are always dedicated, as described in ITU-T Rec. Y.1312.

Note that even though instances for routing are shared, it would be possible to dedicate U-Plane resources by using a mechanism such as colouring. In this case, U-Plane resources dedicated to a VPN are used in link selection process.

Shared instances and databases are used within the provider network. Information exchange between dedicated databases/instances and shared databases/instances is expected. In this case, address translation may be required. Also, information filtering from shared databases to dedicated databases may be required.

Since address space is common over VPNs within the provider network, if there is no mechanism to identify to which VPN information received from customers should belong, a public address must be assigned for identifying a CE-PE SNPP link. However, private addresses can be used within the customer site. A connection request is received by connection control functions, followed by connectivity restriction based on membership information.

On the other hand, if there is a mechanism to identify to which VPN information received from customers should belong, such as methods for address disambiguation mentioned in 8.3.2, by having an address translation table per VPN, private addresses can be used.

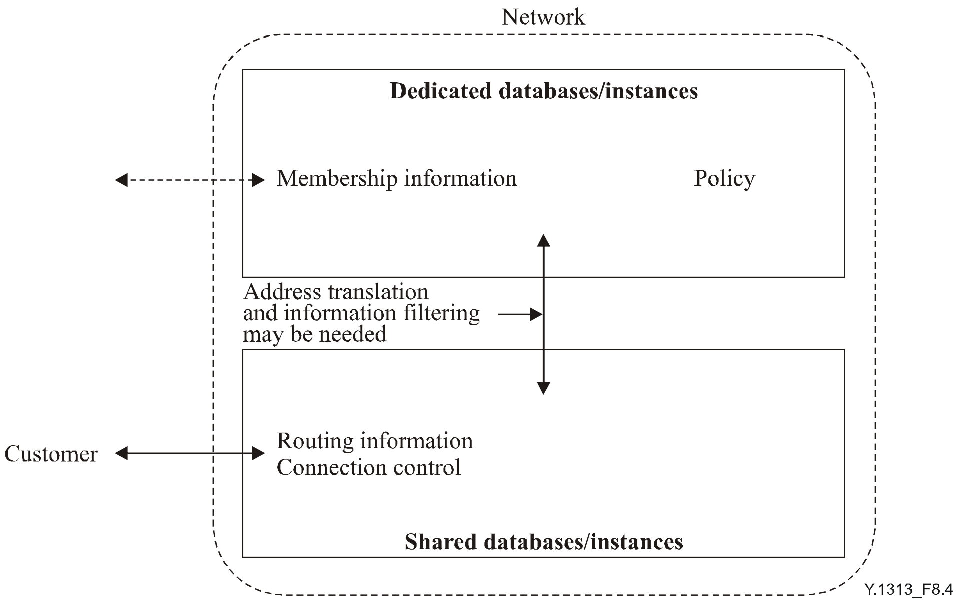

Network
Dedicated databases/instances
Membership information
Policy
Address translation and information filtering may be needed
Customer
Routing information
Connection control
Shared databases/instances
Y.1313_F8.4

**Figure 8-4/Y.1313 – Shared C-Plane example**

A control link is another type of C-Plane resource which can be shared among several Layer 1 VPNs. Control messages received over a shared control link across a CE-PE interface must be disambiguated with respect to the Layer 1 VPN to which they apply. This disambiguation must be done by referring to a Layer 1 VPN explicitly in the control message or by public address.

## 8.3 Private addressing

### 8.3.1 Requirements

In a Layer 1 VPN, each CE-PE SNPP link must have an address unique in the context of the VPN according to ITU-T Rec. Y.1312. This address may be a public address assigned by the provider network operator or a private address assigned by the customer. In the latter case, the provider network may translate the private address to a public address in order to support connection control within the provider network.

### 8.3.2 Contexts for disambiguating private addresses

Unlike public addresses, Layer 1 VPN private addresses can overlap and it is essential that the provider be able to disambiguate them, that is, determine to which Layer 1 VPN address space they belong. There are two general methods for Layer 1 VPN address disambiguation: implicit and explicit.

The implicit method involves dedicating a control link to each Layer 1 VPN. Since the control link is then in one-to-one relationship with a Layer 1 VPN, the private addresses contained in the messages sent over this control link will be interpreted in the context of this Layer 1 VPN. There is no need to explicitly refer to the Layer 1 VPN as part of control messages.

The explicit method assumes that a control link is shared among Layer 1 VPNs. In that case, disambiguation must be done explicitly by the provider. This can be done by tagging control messages with a globally unique Layer 1 VPN identifier.

### 8.3.3 Address translation

In the case when Layer 1 VPN private addresses must be translated to public addresses, the provider entity will have to make a request to a directory. The directory is essentially a database which can be distributed to all PEs or centralized in the network.

## 9 Layer 1 VPN functional entities architecture

### 9.1 Membership information maintenance and connectivity policy management

Membership information means a list of CEs within the same VPN. Membership information is maintained within the provider network, and connectivity among CEs is restricted based on membership information. On the contrary, it is sometimes required that connectivity is restricted even within the same VPN. In this case, connectivity restriction based on connectivity policy for each VPN must be managed.

### 9.1.1 Membership information maintenance

Membership information is a list of CEs within the same VPN. In a more detailed description, membership information can be represented as a list of CE-PE SNPP Names within the same VPN. Provider must maintain membership information.

Connectivity must be restricted based on membership information, by which connectivity is restricted only within the same VPN. In the distributed provider network architecture, membership information must be distributed in every PEs, possibly by automatic mechanisms.

Within the provider network, membership information should be maintained with an associating PE's ID and CE-PE SNPP Name. This information can be used for identifying an appropriate provider network egress point for connection routing.

The mechanism to distribute and maintain membership information and the mechanism to distribute and maintain connectivity policy information may be the same.

### 9.1.2 Connectivity policy management

#### 9.1.2.1 Requirements

ITU-T Rec. Y.1312 describes a number of requirements relative to connectivity policies. These policies define which member of a L1 VPN can set up connections with other members of the L1 VPN at any given point in time.

#### 9.1.2.2 Connectivity policies

Connection request admission control can be performed based on the connectivity policies configured for a particular CE in a particular L1 VPN. L1 VPN connection request admission control is supported by a provider entity as defined in ITU-T Rec. Y.1312.

Connectivity policies can be captured by two lists of addresses for each L1 VPN: an admissible outgoing connection request address list and an admissible incoming connection request address list.

If a provider entity receives an L1 VPN outgoing connection request, from a L1 VPN customer entity to the provider, containing a destination address not appearing on the admissible outgoing connection request address list for this L1 VPN, then it rejects this connection request. If a provider entity receives an L1 VPN incoming connection request, from the provider to a L1 VPN customer entity, containing a source address not appearing on the admissible incoming connection request address list for this L1 VPN, then it rejects this connection request. The use of both admissible outgoing and incoming connection request address lists allows for asymmetrical connectivity policies among L1 VPN members. This is depicted in Figure 9-1.

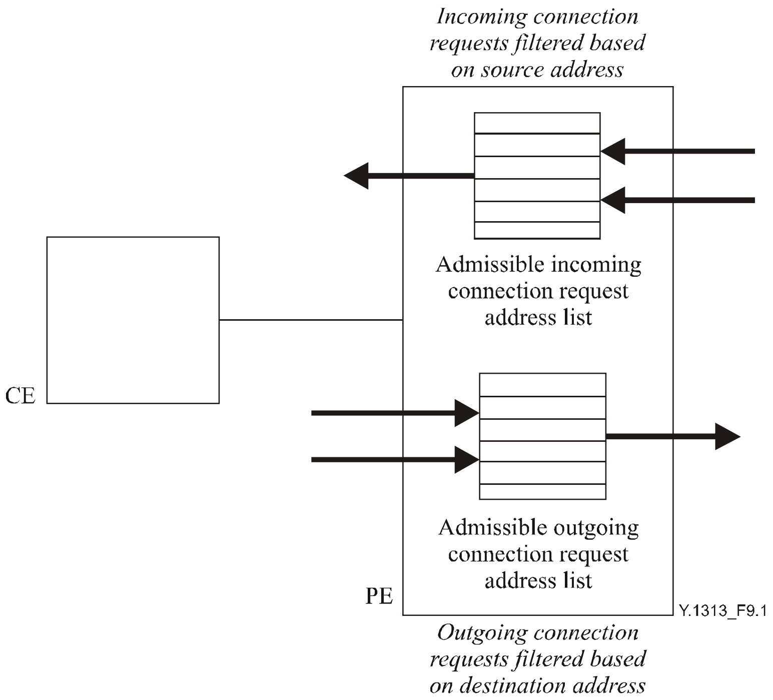

Incoming connection requests filtered based on source address
Admissible incoming connection request address list
CE
Admissible outgoing connection request address list
PE
Y.1313_F9.1
Outgoing connection requests filtered based on destination address

**Figure 9-1/Y.1313 – Incoming and outgoing connection request admission control**

### 9.1.2.3 Configuration of connectivity policies

In the distributed provider network architecture, admissible outgoing and incoming connection request address lists for each L1 VPN on each PE must be populated and maintained. The rules are the following:

1) The admissible incoming connection request address list is always configured.

2) The admissible outgoing connection request address list can be either statically configured or can be automatically discovered and dynamically maintained. The latter allows single ended provisioning of admissible connection request address lists.

Note that when both lists are statically configured, then the solution is similar to Closed User Groups (CUG).

### 9.1.2.4 L1 VPN connectivity policy exchange of information between PE and CE

The previous clauses describe the management of connectivity policy between PEs. Connectivity policy management can be extended to the CE-PE interface as a supplementary service. There are two cases for this service:

1) The CE may request the PE to change the configuration of its admissible incoming connection request address list. Among other things, this will trigger dynamic maintenance of the admissible outgoing address lists.

2) The PE may pass an updated admissible outgoing connection request address list to the CE after receiving a dynamic maintenance message.

## 9.2 Routing information maintenance and route computation

There are two aspects for routing information maintenance and route computation. One is between the customer and the network, and the other is within the network.

### 1) Between the customer and the network

If the customers are permitted to signal for connections and include an explicit route in the request then topology and status information must be provided in a timely fashion to allow the customer to perform route computation. In this case, in the distributed architecture, the CE to PE control channel must support both a signalling and a routing protocol. The scope of the routing information must be restricted to the resources provided as part of the L1 VPN service.

There are two kinds of routing: unidirectional routing and bidirectional routing. With unidirectional routing, L1 VPN topology information is passed from the PE to the CE. In addition, connectivity information may be passed from the PE to the CE. With bidirectional routing, customer network topology information is also passed from the CE to the PE, as this topology relates to the L1 VPN. See clause 5 for more detailed description of topology and connectivity information.

Note that transparent transfer of information between customer entities in L1 VPN can be used for carrying customer domain routing information.

### 2) Within the network

Routing information is used to route a connection. Customer domain routing information may be used in order to optimize route computation. A route is calculated based on network resource availability obtained by routing information maintenance mechanism, network provider's policy and customer's policy (per VPN policy). Specifically, route computation differs depending on how U-Plane resources are allocated. When U-Plane resources are dedicated, route computation is performed in a way that only dedicated portion of resources is used. On the other hand, when U-Plane resources are shared, route computation is performed in a way that resources can be used by multiple VPNs.

Note that when routing information is exchanged between the customer and the network, customers may specify an explicit route, as described in 9.3. In this case, the network may not need to perform route computation.

## 9.3 Connection control

Connection control requires two features. First, connection requests may include L1 VPN private addresses for source and destination. Second, connection requests may include an explicit route to be used for the connection. Information about these explicit routes is available by virtue of the routing information exchange described above.

## 9.4 Management

There are two aspects in management. One is management by the provider and the other is management by the customer, as described in 7.3. Management by the provider must ensure secure, reliable and fault-tolerant operation of the network. Management by the provider also deals with service specific functions, such as AAA and per VPN policies.

At the same time, the customer may access the management capabilities by CNM interface. CNM interface enables customers to manage dedicated portion of the provider network.

In addition, management capabilities must support two different but related views on network resources, a C-Plane view and a U-Plane view, as described in 8.1.3.

# 10 Examples of functional architecture

## 10.1 Distributed provider network architecture

Three examples of the detailed distributed provider network architecture are described based on architectural classification criteria mentioned in clauses 7 and 8.

### 1) Dedicated C-Plane

Instances and databases are dedicated per VPN in the PE and the P. Communication channels between dedicated instances may be realized by logically separating the common communication channel.

**Service perspective**: Routing information can be provided to customers. Private addresses can be easily supported. No address translation mechanism is required.

**Membership information maintenance**: Membership information may be incorporated in the routing information described below. Connectivity policy information may be conveyed by the same manner.

**Routing information maintenance and route computation**: The same instance may be used for customer domain routing information, network topology information, and connectivity information. Here, network topology information dedicated per VPN is exchanged by each dedicated instance. Also, the same mechanism or protocol may be used within the network and between the customer and the PE. A route may be calculated by the CE and specified within a connection control request. Or, a route may be calculated by the PE, or by the PE and the P.

**Connection control**: The same mechanism or protocol may be used within the network and between the customer and the PE. A single session may be established between CEs.

**Management**: Some of the functions are performed distributedly, as described in 7.3.

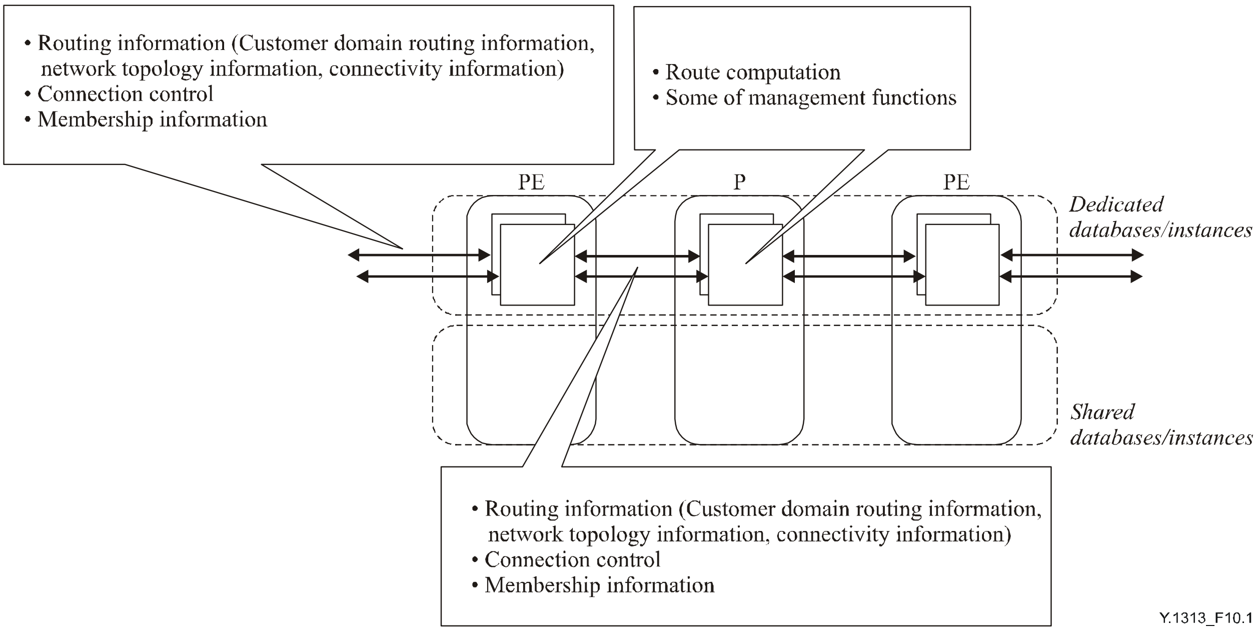

• Routing information (Customer domain routing information, network topology information, connectivity information)
• Connection control
• Membership information
• Route computation
• Some of management functions
PE
P
PE
Dedicated databases/instances
Shared databases/instances
• Routing information (Customer domain routing information, network topology information, connectivity information)
• Connection control
• Membership information
Y.1313_F10.1

**Figure 10-1/Y.1313 – Dedicated C-Plane**

### 2) PE dedicated C-Plane

Instances and databases are dedicated in the PE, but shared in the P. Communication channels between dedicated instances/databases in PEs are formed, for example by tunnelling mechanism. This communication channel conveys information, such as membership information, customer domain routing information and connectivity information. Information such as connection control and network topology information is exchanged between shared and dedicated databases/instances.

**Service perspective**: Routing information can be provided to customers. To support private addresses, address translation is required.

**Membership information maintenance**: Membership information is exchanged over the communication channel between dedicated instances/databases in PEs. Membership information may be incorporated in the routing information described below. Note that membership information could be passed to the shared database/instance, rather than directly transferred to the remote PE. Membership information is then transferred to the remote PE's shared database/instance via a communication channel between PEs. Connectivity policy information may be conveyed by the same manner.

**Routing information maintenance and route computation**: Customer domain routing information and connectivity information is exchanged over a communication channel between dedicated instances/databases in PEs. Network topology information is transferred from the shared database/instance to dedicated databases/instances at PEs. Network topology information exchanged between shared instances is concerning the whole network, while network topology information transferred from the shared database/instance to dedicated databases/instances at PEs is per VPN. Note that it is less likely that customer domain routing information is passed to the shared database/instance, rather than directly transferred to the remote PE. This is because of a scalability issue. As for customer domain routing information and connectivity information, the same mechanism or protocol could be used within the network and between the network and the customer. As for network topology information, different mechanisms or protocols could be used within the network and between the network and the customer. A route may be calculated by the CE and specified within connection control information. Or, a route may be calculated by the PE, or the PE and the P.

**Connection control**: Mechanisms or protocols within the network and between the network and the customer may be the same, or may be different. Therefore, a single session or multiple sessions (e.g., CE to PE session and PE to PE session) can be established between CEs.

**Management**: Some of the functions are performed distributedly, as described in 7.3.

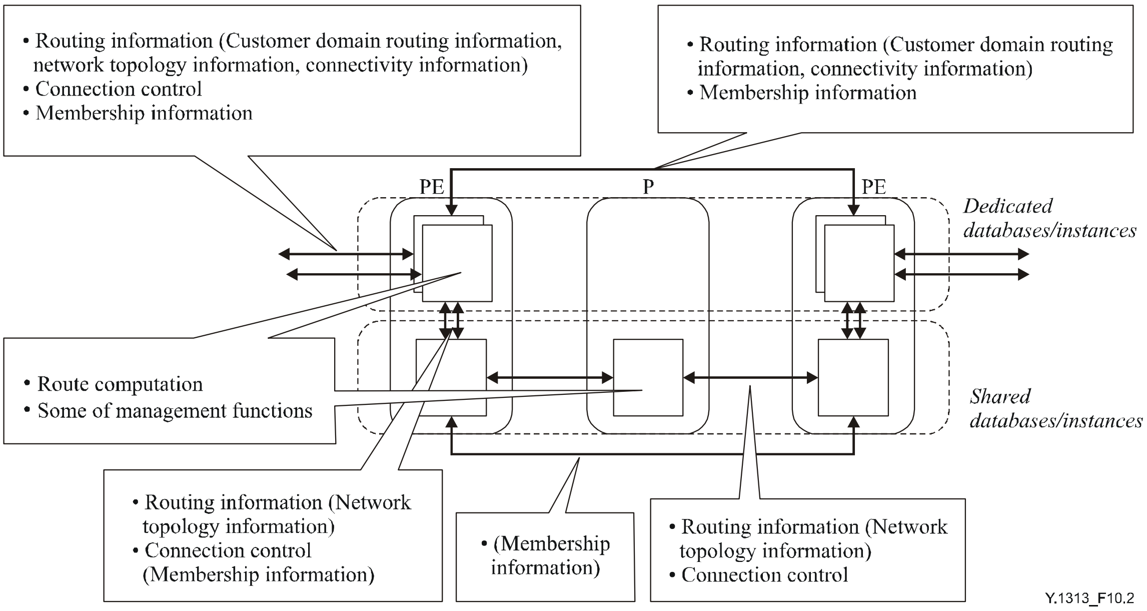

• Routing information (Customer domain routing information, network topology information, connectivity information)
• Connection control
• Membership information
• Routing information (Customer domain routing information, connectivity information)
• Membership information
PE
P
PE
Dedicated databases/instances
Shared databases/instances
• Route computation
• Some of management functions
• Routing information (Network topology information)
• Connection control (Membership information)
• (Membership information)
• Routing information (Network topology information)
• Connection control
Y.1313_F10.2

**Figure 10-2/Y.1313 – PE Dedicated C-Plane**

### 3) Shared C-Plane

Basically, instances/databases are shared in the PE and the P, except membership information and policy. A communication channel is formed between shared instances/databases in PEs, which may convey membership information.

**Service perspective**: Routing information cannot be provided to customers, whereas connection control is provided to customers. To support private addresses specifying CE-PE SNPP link, address translation is required.

**Membership information maintenance**: Membership information is transferred over a communication channel connecting shared C-Plane of remote PEs. Membership information is then passed to the dedicated databases. Membership information may be incorporated in the routing information described below. Connectivity policy information may be conveyed by the same manner.

**Routing information maintenance and route computation**: Routing information is not provided to customers. Customers specify CE-PE SNPP link address, and a route is calculated by the PE, or by the PE and the P.

**Connection control**: A single session or multiple sessions can be established between CEs.

**Management**: Some of the functions are performed distributedly, as described in 7.3.

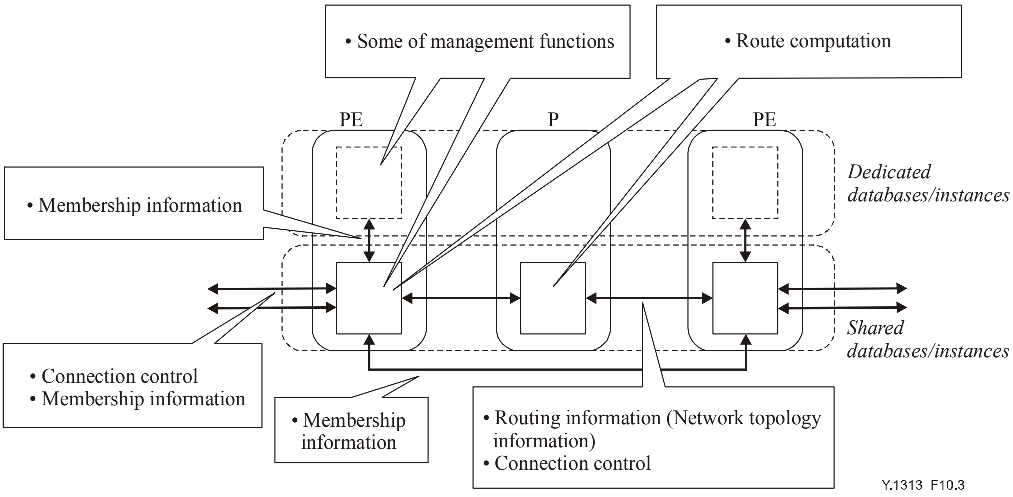


**Figure 10-3/Y.1313 – Shared C-Plane**

## 10.2 Hybrid provider network architecture

One example of the hybrid provider network architecture is distribution of functions where L1 VPN specific service functions, such as membership information maintenance, as well as management functions are centralized, while common functions to provide L1 connections, such as connection control, are distributed, as shown in Figure 10-4.

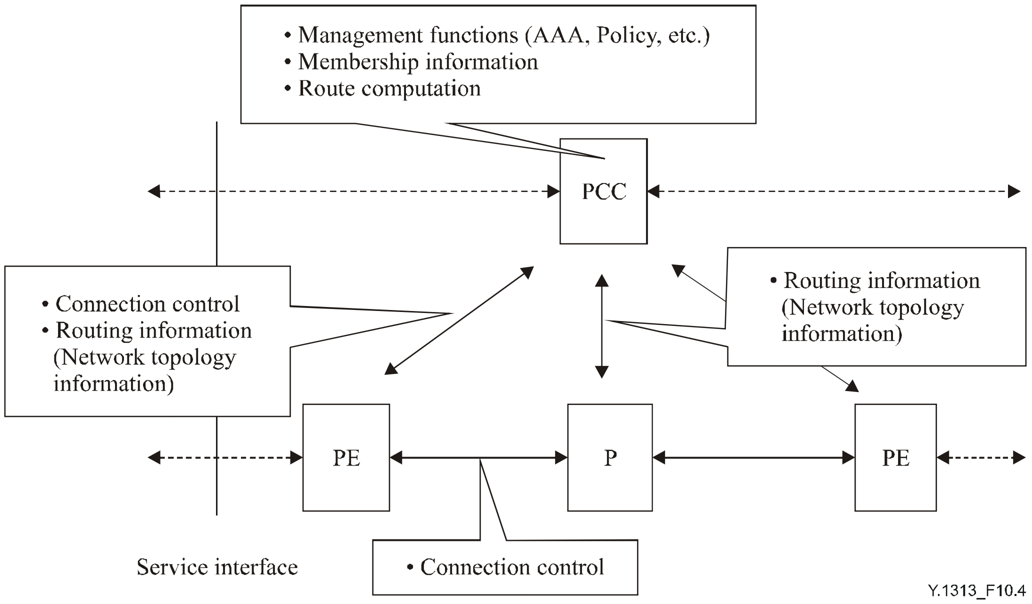

• Management functions (AAA, Policy, etc.)
• Membership information
• Route computation
PCC
• Connection control
• Routing information (Network topology information)
• Routing information (Network topology information)
PE
P
PE
Service interface
• Connection control
Y.1313_F10.4

**Figure 10-4/Y.1313 – Hybrid provider network architecture**

The PCC is the Provider Centralized Controller. In the hybrid provider network architecture, the PCC performs most of decision process. The PCC performs functions including connectivity restriction by using membership information, per VPN policy check, and route computation by using topology information. The PCC also performs AAA functions. After computing a route, the PCC communicates with a PE to set up a connection. A connection is set up by distributed connection control functions. The PCC may have dedicated C-Plane.

Another notable feature of the hybrid provider network architecture is that it is easy to communicate with customer entities by distributed fashion as well as by centralized fashion. In the former case, the PE communicates with the customer entity, which is most likely the CE. In the latter case, the PCC communicates with the customer entity, which is most likely the CCC.

By the PCC communicating with PEs and Ps to obtaining topology information, possibly by distributing routing functions, the PCC can have consistent topology information with PEs and Ps.

### 1) Distributed communication with the customer

In this model, the PE communicates with customer entities, such as CEs. The PE receives a connection request from a customer, and passes connection request information to the PCC. The PCC checks whether a connection is allowed by applying connectivity restriction check as well as service class check. Then, the PCC computes a route, and returns a route to the PE. The PE communicates with Ps and PEs, and sets up a connection along with the route specified by the PCC. The PCC performs as PDP, while the PE performs as PEP, as mentioned in 7.3. The PE may identify from which VPN a connection request is made, by using the mechanism mentioned in 8.2.2.

When membership information is optionally exchanged between the customer and network, the PCC communicates with PEs, and PEs communicates with CEs to exchange membership information. In addition, when routing information is optionally exchanged between the customer and network, the PCC and PEs have dedicated C-Plane to separate topology information per VPN basis. If Ps also have dedicated C-Plane, dedicated C-Plane of the PCC communicates with dedicated C-Plane of PEs, and dedicated C-Plane of PEs communicates with CEs to inform per VPN resource information of the provider network. Also, dedicated C-Plane of PEs may communicate with CEs to exchange customer domain routing information and connectivity information.

If Ps have shared C-Plane, the PCC separates network topology information per VPN basis, by transferring network topology information from a shared instance to dedicated instances, using similar mechanisms mentioned in PE Dedicated C-Plane in 10.1. Dedicated C-Plane of the PCC communicates with dedicated C-Plane of PEs, and dedicated C-Plane of PEs communicates with CEs.

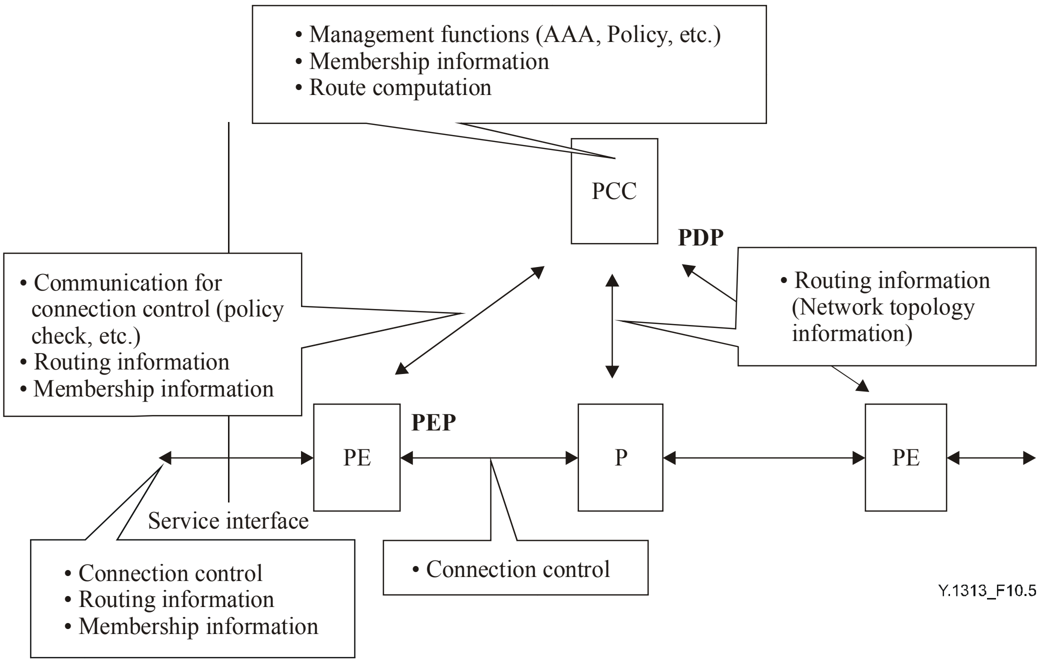


**Figure 10-5/Y.1313 – Distributed communication with the customer**

### 2) Centralized communication with the customer

In this model, the PCC communicates with customer entities, such as CCCs. The PCC receives a connection request from a customer, and checks whether a connection is allowed by applying connectivity restriction check as well as service level check. Then, the PCC calculates a route, and communicates with a PE. The PE communicates with Ps and PEs and establishes a connection along the route specified by the PCC. The PCC performs as PDP and PEP, as mentioned in 7.3. The PCC must identify from which VPN a connection request is made.

The PCC may optionally communicate with customer entities to exchange membership information. In addition, the PCC may optionally have dedicated C-Plane to separate topology information per VPN basis. The PCC may communicate with customer entities to inform per VPN resource information of the provider network. Also, the PCC may communicate with customer entities to exchange customer domain routing information and connectivity information.

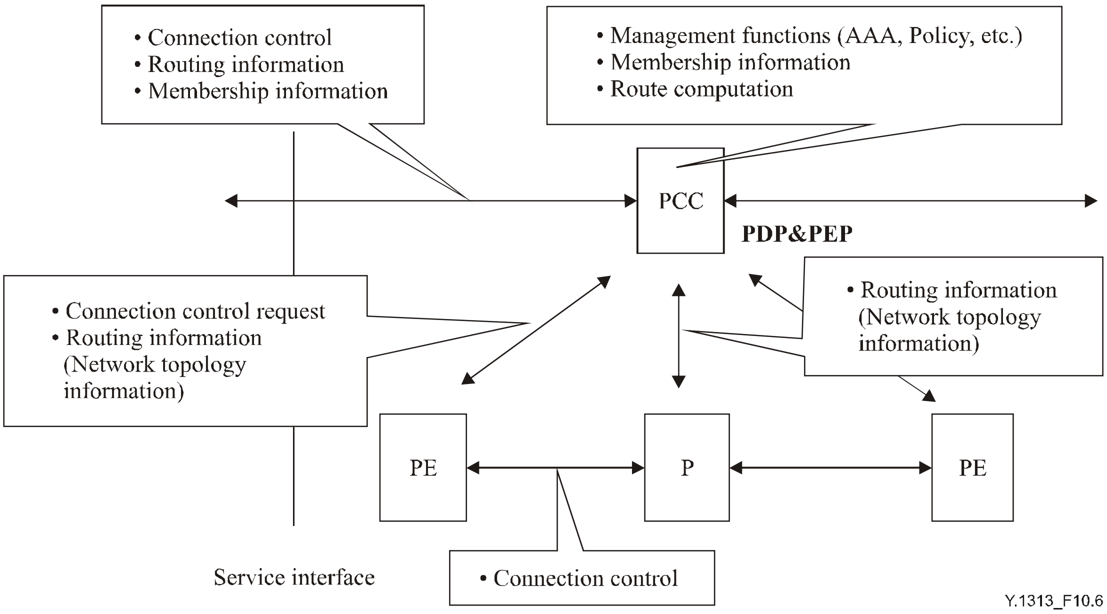


**Figure 10-6/Y.1313 – Centralized communication with the customer**

### 10.3 Centralized provider network architecture

In this model, the PCC communicates with customer entities, which is typically CCCs. In addition, the PCC communicates with PEs and Ps to obtain network topology information as well as to request connection control.

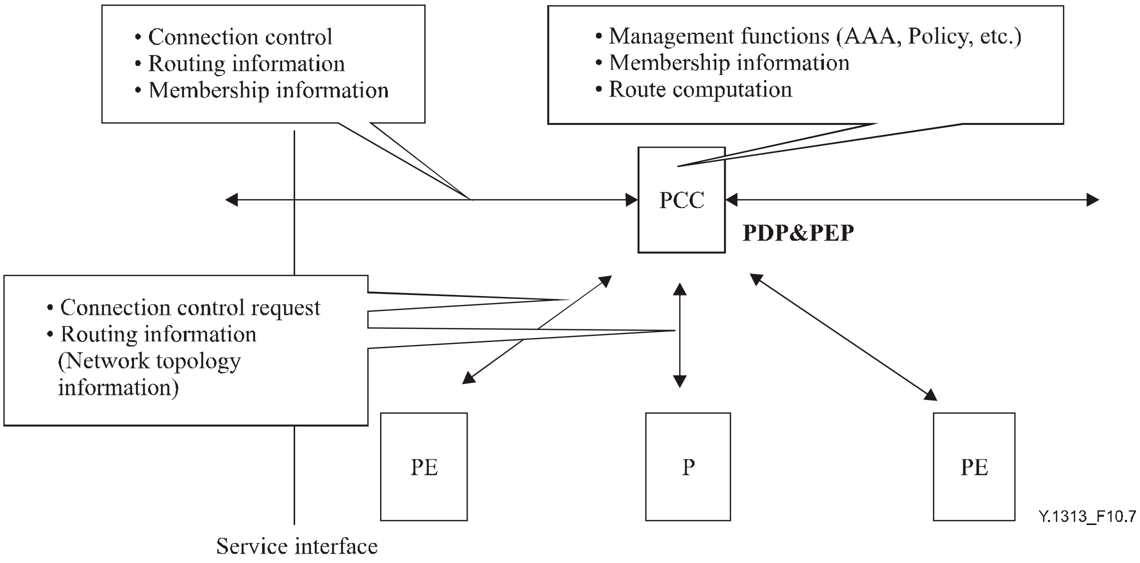


**Figure 10-7/Y.1313 – Centralized provider network architecture**

## 11 Implementation examples of functional architecture

### 11.1 Overview

Existing mechanisms that can be applied to L1 VPN may vary depending on types of L1 VPN architectures. However, in general, the following assumptions can be considered.

- *Membership information maintenance*

Mechanisms for L2 and L3 VPNs may be applied. For example, routing based (e.g., BGP-based [IETF RFC 1771]) or directory based mechanisms may be applied. Similar mechanisms can be used for network discovery (e.g., remote PE discovery, PCC discovery).

Mechanisms to distribute membership information within the provider network may be different from mechanisms to communicate with customer entities.

- *Routing information maintenance and route computation*

Link state protocols, such as OSPF, may be applied (e.g., [IETF RFC 2328]) with appropriate extensions. To separate topology information per VPN, virtual router based mechanisms or extension of routing protocols to convey VPN ID specifying to which VPN information belongs, may be applied.

Mechanisms to distribute topology information within the provider network may be different from mechanisms to communicate with customer entities.

Static information, such as contracted dedicated resource information, may be provided via the CNM interface.

Note that route computation is a local decision process, and usually does not involve any protocol.

- *Connection control*

Optical control plane signalling protocols (e.g., [IETF RFC 3473], [IETF RFC 3472], [IETF RFC 3474], [IETF RFC 3475], [IETF RFC 3476], [ITU-T G.7713.1], [ITU-T G.7713.2], [ITU-T G.7713.3], [OIF UNI 1.0], [OIF Signaling E-NNI 1.0]) may be applied.

- *Management*

As for management related information, such as performance information and record (billing) information, the CNM interface may be used, via mechanisms, such as CORBA, Web Services, and FTP.

For communication between the PCC and the PE/P, TMF814, SNMP, XML and TL-1 may be applied. In addition, in the hybrid provider network architecture, mechanisms to communicate between the PCC and the PE are required, and policy protocols, such as COPS [IETF RFC 2748], may be applied.

Another class of mechanisms encompasses aspects of network configuration management (auto-discovery mechanisms) and fault/performance management (such as technology specific OAM mechanisms).

- *L1 bearer*

L1 bearer can support basic L1 services, which is described in ITU-T Rec. Y.1312. Concerned L1 bearer technologies include SONET/SDH, OTN, and Ethernet Private Line (EPL).

The following clauses describe possible detailed mappings of existing mechanisms to L1 VPN functions, in various architecture examples mentioned in clause 10. As indicated later on, these mechanisms are provided only as examples and candidate solutions, their actual applicability being out of scope of this Recommendation.

Appendix I lists possible implementation examples of these mechanisms.

## 11.2 Distributed provider network architecture

Clause 10.1 describes three models of the distributed provider network architecture, namely, dedicated C-Plane, PE dedicated C-Plane and shared C-Plane. The following text describes how existing mechanisms can be applied to each model.

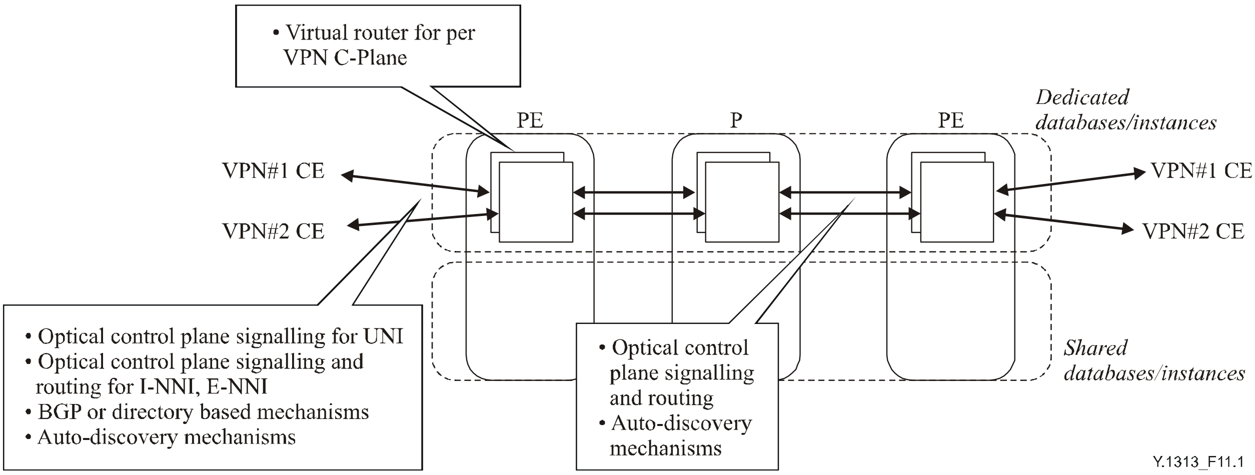
### 1) Dedicated C-Plane

In this model, U-Plane resources are typically dedicated.

Virtual routers can be applied to separate C-Plane per VPN. In addition, optical control plane signalling and routing can be used to communicate within dedicated C-Plane. Some examples of mechanisms/protocol solutions are provided in Table 11-1 and Figure 11-1 below.

**Table 11-1/Y.1313 – Dedicated C-Plane**

| | | **CE-PE** | | **Within the provider network** |
|---|---|---|---|---|
| | | **No routing information exchange** | **With routing information exchange** | |
| Membership information maintenance | | BGP, directory based mechanisms | BGP, directory based mechanisms, mechanism for routing information maintenance | BGP, directory based mechanisms, mechanism for routing information maintenance |
| Routing information maintenance | Customer domain routing information | None | Optical control plane routing for I-NNI, E-NNI | Per VPN optical control plane routing |
| | Connectivity information | | | |
| | Network topology information | | | |
| Connection control | | Optical control plane signalling for UNI | Optical control plane signalling for I-NNI, E-NNI | Per VPN optical control plane signalling |
| Management aspects | | Auto-discovery mechanisms, OAM mechanisms | Auto-discovery mechanisms, OAM mechanisms | Auto-discovery mechanisms, OAM mechanisms |



• Virtual router for per VPN C-Plane
PE
P
PE
Dedicated databases/instances
VPN#1 CE
VPN#2 CE
VPN#1 CE
VPN#2 CE
• Optical control plane signalling for UNI
• Optical control plane signalling and routing for I-NNI, E-NNI
• BGP or directory based mechanisms
• Auto-discovery mechanisms
• Optical control plane signalling and routing
• Auto-discovery mechanisms
Shared databases/instances
Y.1313_F11.1

**Figure 11-1/Y.1313 – Dedicated C-Plane**

### 2) PE Dedicated C-Plane

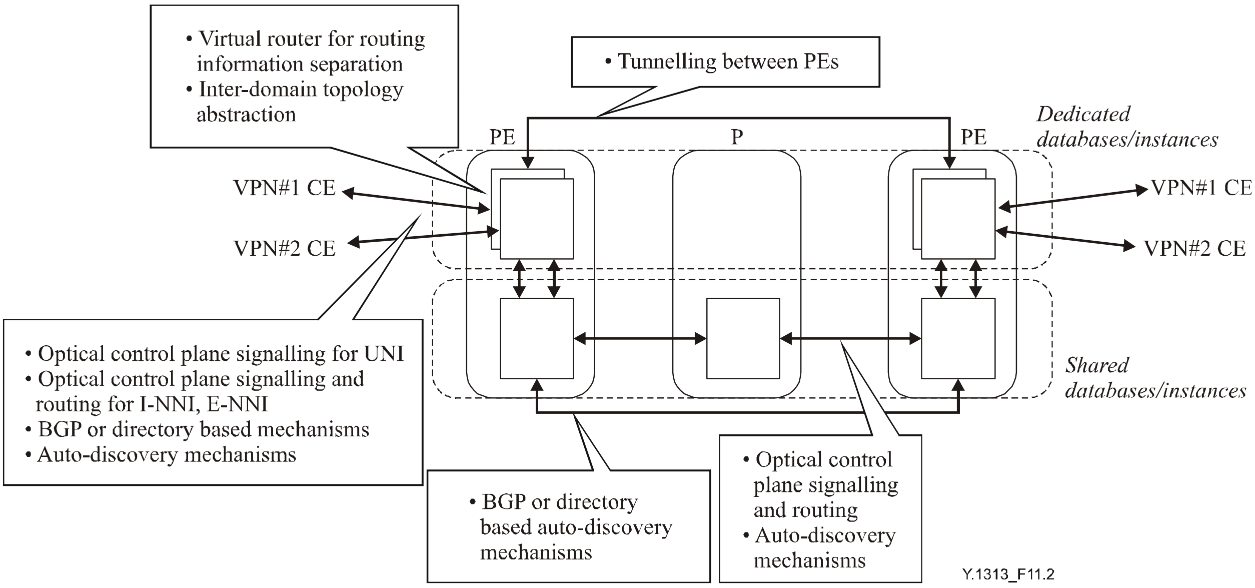
In this model, U-Plane resources are dedicated or shared.

At the CE (or customer entity) to PE interface, different mechanisms can be applied based on whether routing information is exchanged between the customer and the network. If routing information is not exchanged, optical control plane signalling for UNI can be used for connection control. In addition, BGP or directory based mechanisms can be applied for membership information maintenance. Membership information may also be incorporated in the routing information. On the other hand, if routing information is exchanged, optical control plane signalling and routing can be used for routing information maintenance and connection control. At the PE, virtual routers can be used to separate routing information per VPN basis. In addition, inter-domain topology abstraction mechanisms can be applied when providing abstracted topology information to customers. Between PEs, tunnelling mechanisms, such as IP based tunnelling, can be applied to provide a tunnel between PEs over C-Plane. In addition, BGP or directory based auto-discovery mechanisms can be used to discover remote PEs.

Within the provider network, optical control plane routing and signalling can be used for routing information maintenance and connection control. Note that to separate network topology information per VPN basis at the PE, for example, VPN ID attached routing information may be exchanged within the provider network, specifying to which VPN each link belongs. Some examples of mechanisms/protocol solutions are provided in Table 11-2 and Figure 11-2 below.

**Table 11-2/Y.1313 – PE dedicated C-Plane**

| | | CE-PE | | Within the provider network |
|---|---|---|---|---|
| | | **No routing information exchange** | **With routing information exchange** | |
| Membership information maintenance | | BGP, directory based mechanisms | BGP, directory based mechanisms, mechanism for routing information maintenance | BGP, directory based mechanisms, mechanism for routing information maintenance |
| Routing information maintenance | Customer domain routing information | None | Optical control plane routing for I-NNI, E-NNI | Per VPN optical control plane routing over C-Plane tunnel between PEs |
| | Connectivity information | | | |
| | Network topology information | | | Common optical control plane routing |
| Connection control | | Optical control plane signalling for UNI | Optical control plane signalling for I-NNI, E-NNI | Common optical control plane signalling |
| Management aspects | | Auto-discovery mechanisms, OAM mechanisms | Auto-discovery mechanisms, OAM mechanisms | Auto-discovery mechanisms, OAM mechanisms |



• Virtual router for routing information separation
• Inter-domain topology abstraction
• Tunnelling between PEs
PE
P
PE
Dedicated databases/instances
VPN#1 CE
VPN#2 CE
VPN#1 CE
VPN#2 CE
• Optical control plane signalling for UNI
• Optical control plane signalling and routing for I-NNI, E-NNI
• BGP or directory based mechanisms
• Auto-discovery mechanisms
Shared databases/instances
• BGP or directory based auto-discovery mechanisms
• Optical control plane signalling and routing
• Auto-discovery mechanisms
Y.1313_F11.2

**Figure 11-2/Y.1313 – PE dedicated C-Plane**

### 3) Shared C-Plane

In this model, U-Plane resources are dedicated or shared.

Since there is no routing information exchange between the customer and the network, optical control plane signalling for UNI can be used between the CE (or customer entity) and the PE. In addition, BGP or directory based mechanisms can be applied for membership information maintenance. Membership information may also be incorporated in the routing information. Auto-discovery may be provided by various mechanisms.

Within the provider network, optical control plane signalling and routing can be applied for routing information maintenance and connection control. In addition, BGP or directory based auto discovery and membership exchange mechanisms can be used between PEs. Some examples of mechanisms/protocol solutions are provided in Table 11-3 and Figure 11-3 below.

**Table 11-3/Y.1313 – Shared C-Plane**

| | | **CE-PE** | | **Within the provider network** |
|---|---|---|---|---|
| | | **No routing information exchange** | **With routing information exchange** | |
| Membership information maintenance | | BGP, directory based mechanisms | – | BGP, directory based mechanisms, mechanism for routing information maintenance |
| Routing information maintenance | Customer domain routing information | None | – | – |
| | Connectivity information | | | – |
| | Network topology information | | | Common optical control plane routing |
| Connection control | | Optical control plane signalling for UNI | – | Common optical control plane signalling |
| Management aspects | | Auto-discovery mechanisms, OAM mechanisms | – | Auto-discovery mechanisms, OAM mechanisms |

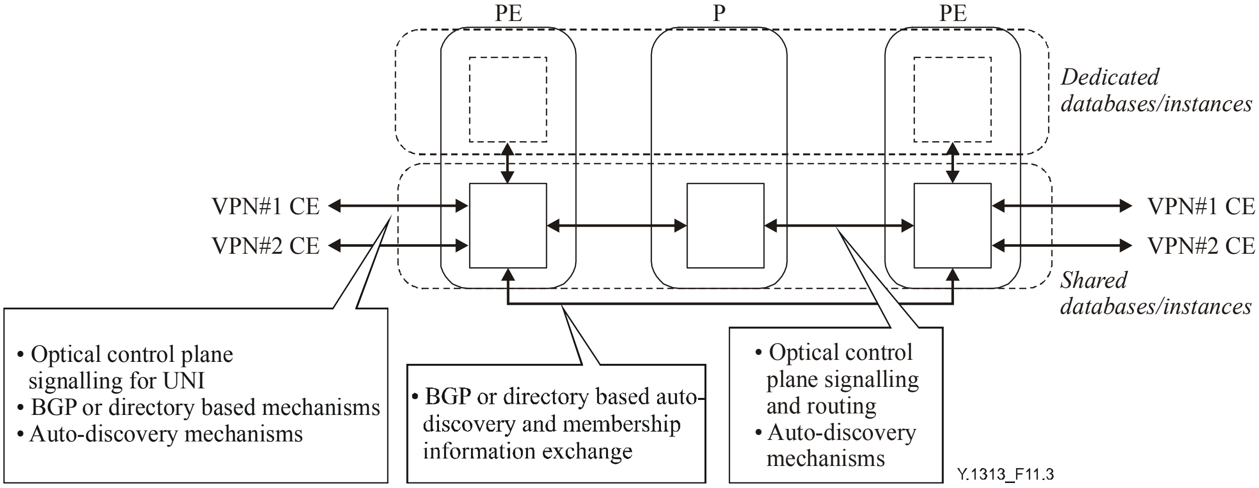

PE
P
PE
Dedicated databases/instances
VPN#1 CE
VPN#2 CE
VPN#1 CE
VPN#2 CE
Shared databases/instances
• Optical control plane signalling for UNI
• BGP or directory based mechanisms
• Auto-discovery mechanisms
• BGP or directory based auto-discovery and membership information exchange
• Optical control plane signalling and routing
• Auto-discovery mechanisms
Y.1313_F11.3

**Figure 11-3/Y.1313 – Shared C-Plane**

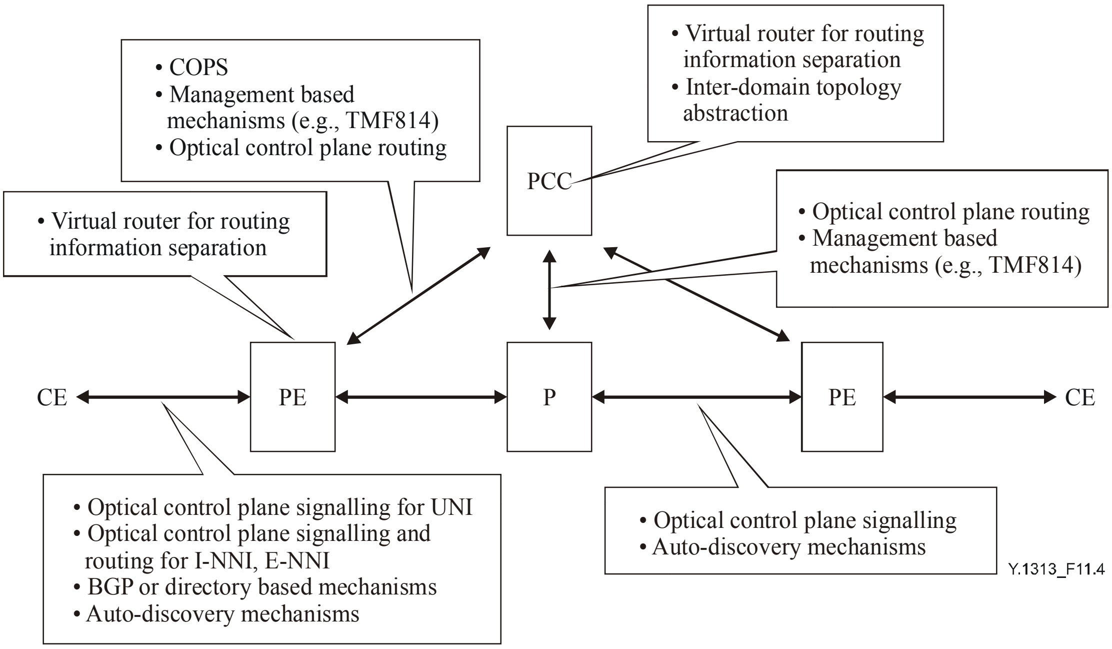
### 11.3 Hybrid provider network architecture

Clause 10.2 describes one example of the hybrid provider network architecture, where L1 VPN specific service functions, such as membership information maintenance, as well as management functions are centralized, while common functions to provide L1 connections, such as connection control, are distributed. In this architecture type, two models of communication with the customer can be considered. One is distributed communication, and the other is centralized communication. Even though there are many common functions in two models, required functions differ between the two models in some areas. As such, differences between the two models exist on how existing mechanisms can be applied to L1 VPN functions.

#### 1) Distributed communication with the customer

In this model, at the CE (or customer entity) to PE interface, different mechanisms can be applied based on whether routing information is exchanged between the customer and the network. If routing information is not exchanged, optical control plane signalling for UNI can be used for connection control. In addition, BGP or directory based mechanisms can be applied for membership information maintenance. Auto-discovery may be provided by various mechanisms. On the other hand, if routing information is exchanged, optical control plane routing and signalling can be used for routing information maintenance and connection control.

Within the provider network, optical control plane signalling can be used for connection control. Policy protocols, such as COPS or TMF814, can be applied for communication for connection control between the PCC and the PE. The PCC participates in optical control plane routing, and obtains topology information of the provider network. Or the PCC collects topology information of the provider network via management based mechanisms, such as TMF814. When routing information is exchanged between the customer and the network, virtual routers can be applied for separating routing information per VPN basis at the PCC as well as at the PE. When topology information provided to the customer is abstracted, inter-domain topology abstraction can be applied at the PCC. Per VPN topology information obtained at the PCC is exchanged with PE's virtual routers, and PE's virtual routers communicate with CEs (or customer entities) to exchange routing information. See Figure 11-4.



• COPS
• Management based mechanisms (e.g., TMF814)
• Optical control plane routing
• Virtual router for routing information separation
• Inter-domain topology abstraction
PCC
• Virtual router for routing information separation
• Optical control plane routing
• Management based mechanisms (e.g., TMF814)
CE
PE
P
PE
CE
• Optical control plane signalling for UNI
• Optical control plane signalling and routing for I-NNI, E-NNI
• BGP or directory based mechanisms
• Auto-discovery mechanisms
• Optical control plane signalling
• Auto-discovery mechanisms
Y.1313_F11.4

**Figure 11-4/Y.1313 – Distributed communication with the customer**

### 2) Centralized communication with the customer

In this model, at the CCC (or customer entity) to PCC interface, different mechanisms can be applied based on whether routing information is exchanged between the customer and the network, as well as types of interface. If routing information is not exchanged, optical control plane signalling for UNI can be used for connection control. In addition, BGP or directory based mechanisms can be applied for membership information maintenance. On the other hand, if routing information is exchanged, optical control plane routing and signalling can be used for routing information maintenance and connection control. If CNM or management type of interface is used between the CCC (or customer entity) and the PCC, management based mechanisms are used for exchanging information between the CCC (or customer entity) and the PCC.

Within the provider network, optical control plane signalling can be used for connection control. SPC (Soft Permanent Connection) mechanisms can be used between the PCC and the PE to initiate connection set-up at the PE. The PCC participates in routing, and obtains topology information of the provider network. Or the PCC collects topology information of the provider network via management based mechanisms, such as TMF814. When routing information is exchanged between the customer and the network, virtual routers can be applied for separating routing information per VPN basis at the PCC. When topology information provided to the customer is abstracted, inter-domain topology abstraction can be applied at the PCC.

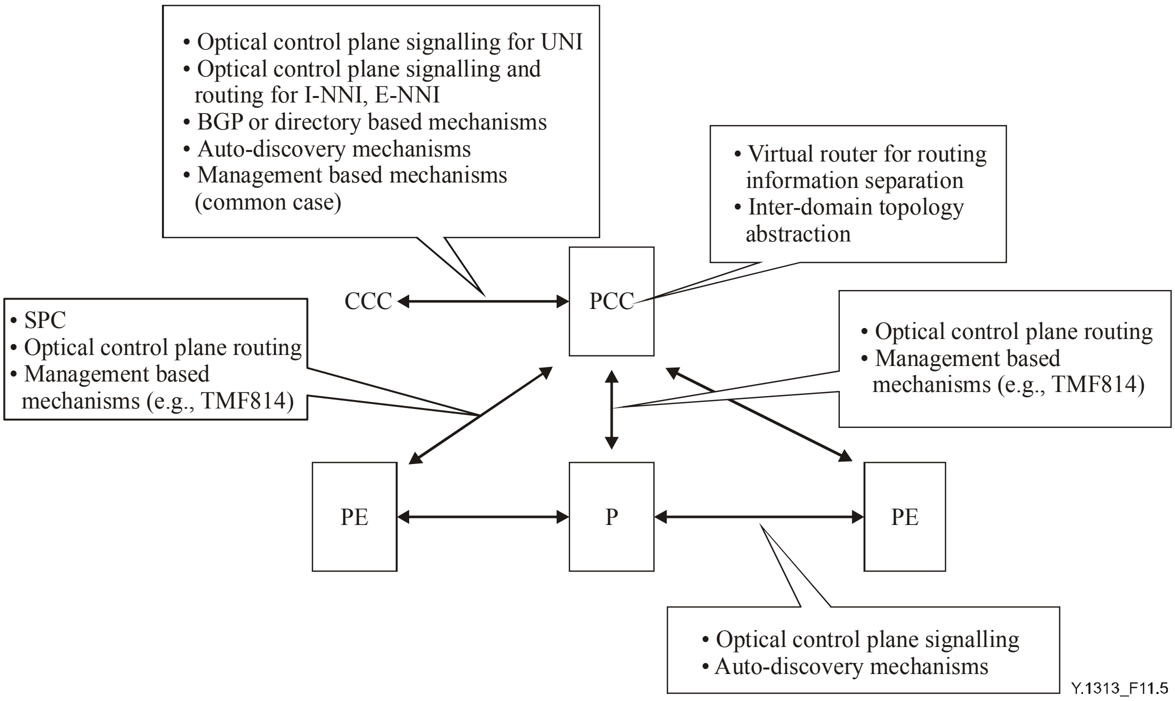

• Optical control plane signalling for UNI
• Optical control plane signalling and routing for I-NNI, E-NNI
• BGP or directory based mechanisms
• Auto-discovery mechanisms
• Management based mechanisms (common case)
• Virtual router for routing information separation
• Inter-domain topology abstraction
CCC
PCC
• SPC
• Optical control plane routing
• Management based mechanisms (e.g., TMF814)
• Optical control plane routing
• Management based mechanisms (e.g., TMF814)
PE
P
PE
• Optical control plane signalling
• Auto-discovery mechanisms
Y.1313_F11.5

**Figure 11-5/Y.1313 – Centralized communication with the customer**

## 11.4 Centralized provider network architecture

In the case of the centralized provider network architecture, typically, the PCC communicates with the CCC with management based mechanisms. In addition, the PCC communicates with PEs and Ps with management based mechanisms. There is no distributed signalling among PEs and Ps.

## 12 Security aspects

There is no additional security requirement other than stated in ITU-T Rec. Y.1312.

# Annex A

## Detailed description of CE and PE

### A.1 Architecture of CE participating in multiple Layer 1 VPNs (constructs from ITU-T Recs G.805 and G.8080/Y.1304)

A CE is an administrative grouping of Access Group Containers (AGC) (see ITU-T Rec. G.8080/Y.1304 Amendment 1) and Layer 1 VPN Applications. An AGC provides a location for services to a Layer 1 VPN Application. A Layer 1 VPN Application is composed of one or more Connection Users (CUs) and Customer Call Agents (CCAs) (note that the term CCA from ITU-T Rec. Y.1312 and the term Connection Requestor from ITU-T Rec. G.8080/Y.1304 Amendment 1 denote the same entity). There is one and only one AGC per Layer 1 VPN Application per CE.

From a U-Plane perspective, Figure A.1 illustrates the direct relationship that exists between Layer 1 VPN CUs and AGs. Note that $AG_2$ belongs to both $AGC_A$ and $AGC_B$ for Layer 1 VPNs A and B (this is an extension to ITU-T Rec. G.8080/Y.1304 Amendment 1). This is required to allow sharing of the U-Plane between Layer 1 VPNs.

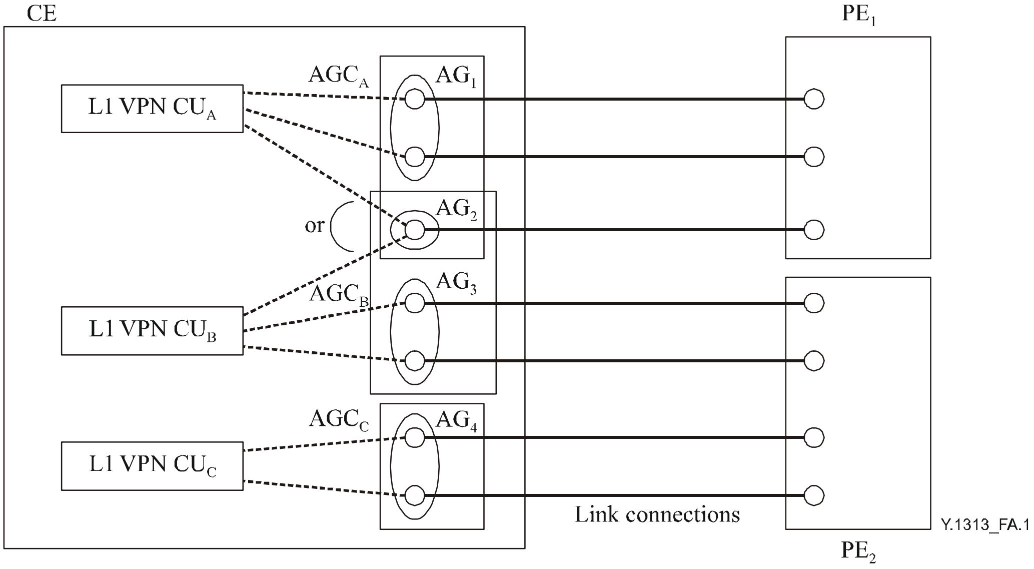


**Figure A.1/Y.1313 – Example of U-Plane architecture for the CE and the PE**

From a C-Plane perspective, Figure A.2 illustrates the relationship that exists between Layer 1 VPN CCAs and the SNPP links contained in AGCs.

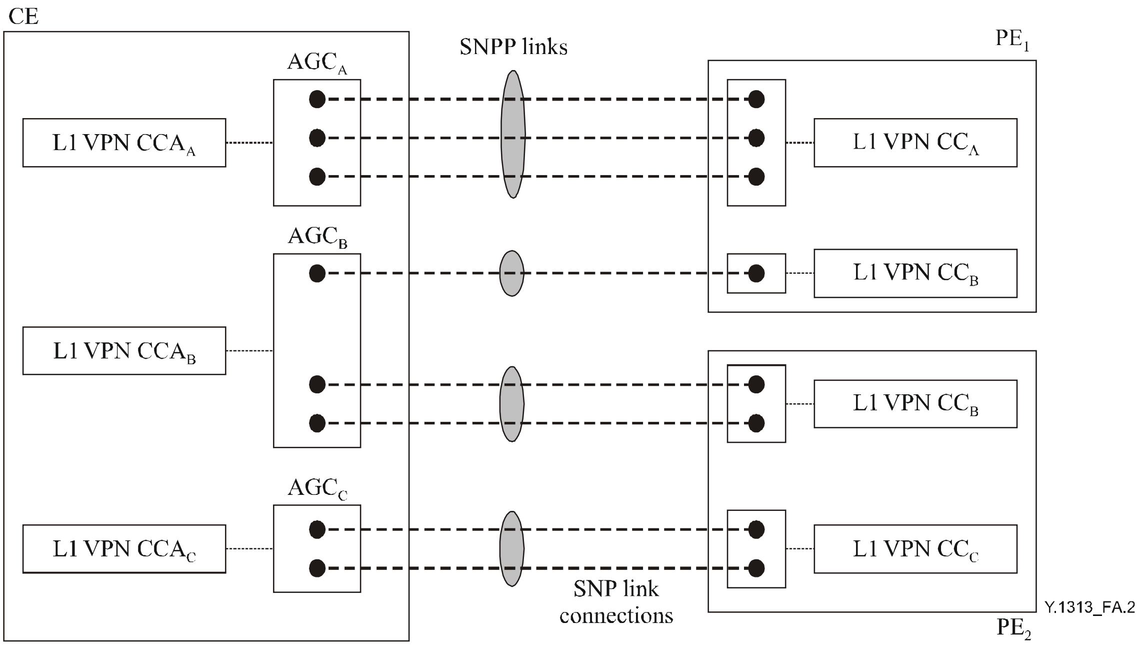


**Figure A.2/Y.1313 – Example of C-Plane architecture for the CE and the PE**

### A.2 Architecture of PE participating in multiple Layer 1 VPNs (constructs from ITU-T Recs G.805 and G.8080/Y.1304)

As it relates to the CE, the PE is an administrative grouping of link connections and SNPP links. This grouping is subject to the following two constraints:

1) link connections associated to the same AG on a CE must belong to the same PE (a U-Plane constraint);
2) the closure of all SNPP links, which contain SNP link connections that are allowed to be bound to the same link connections by configuration, must belong to the same PE (a C-Plane constraint).

Furthermore, it is assumed that the PE has explicit knowledge of which SNPP links belong to which Layer 1 VPNs. This entails that the PE has one Connection Controller (CC) per Layer 1 VPN. The PE architecture and how it relates to the CE are illustrated in Figures A.1 and A.2. In this example, L1 VPN B on the CE is dual-homed to PE$_1$ and PE$_2$. The example also assumes that the C-Plane is dedicated since there is a Connection Controller per Layer 1 VPN per PE. Other functions and properties of the PE are left unspecified.

### A.3 Architecture of CE and PE in relation with management systems

The CE and PE architecture described in the previous clause assume that the Layer 1 VPN control architecture is distributed. However, the Layer 1 VPN control architecture can also be centralized. This implies that management entities must be introduced: the customer management system (CMS) and the provider management system (PMS). Note that the CCC (Customer Centralized Controller) and PCC (Provider Centralized Controller) functions are instantiated within the CMS and PMS respectively. Furthermore, the CE and PE architecture must be extended with management interfaces. In particular, there may be a CNM (Customer Network Management) interface between customer entities and the provider management system. Furthermore, there may be a proxy control interface between the customer management system and the PE. Finally, there are management interfaces internal to the customer and the provider. The general set of control interfaces is depicted in Figure A.3.

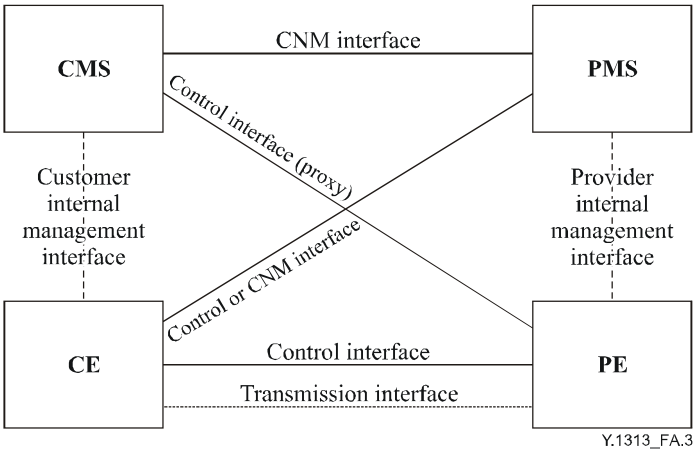

CMS
CNM interface
PMS
Control interface (proxy)
Customer internal management interface
Provider internal management interface
Control or CNM interface
CE
Control interface
Transmission interface
PE
Y.1313_FA.3

**Figure A.3/Y.1313 – Overall CE-PE interfaces, including management**

# Appendix I

## Implementation examples of existing mechanisms for Layer 1 VPN

Implementation examples of existing mechanisms that may be applied for the Layer 1 VPN functions are described as follows. Note that mechanisms described in this appendix are only examples. This Recommendation does not exclude other mechanisms to be applied for supporting L1 VPN services. Also note that mechanisms described in this appendix may need to be extended for supporting L1 VPN services.

**Table I.1/Y.1313 – Example of existing mechanisms for Layer 1 VPN**

| | | |
|---|---|---|
| Membership information maintenance | | |
| | Example of routing based mechanisms | [IETF RFC 2547 *bis*], [IETF GVPN] |
| Routing information maintenance and route computation | | |
| | Example of optical control plane routing protocols | [IETF GMPLS OSPF], [OIF Routing E-NNI 1.0] |
| | Example of virtual router based mechanisms | [IETF VR], [IETF GVPN] |
| Connection control | | |
| | Example of optical control plane signalling for UNI | [IETF GMPLS Overlay], [OIF UNI 1.0], [ITU-T G.7713.2], [ITU-T G.7713.3], [IETF RFC 3474], [IETF RFC 3475], [IETF RFC 3476] |
| | Example of optical control plane signalling for I-NNI, E-NNI | [IETF RFC 3473], [IETF RFC 3472], [ITU-T G.7713.1], [ITU-T G.7713.2], [ITU-T G.7713.3], [IETF RFC 3474], [IETF RFC 3475], [OIF Signaling E-NNI 1.0] |

**Table I.1/Y.1313 – Example of existing mechanisms for Layer 1 VPN**

| Management | | |
|---|---|---|
| | Example of CNM interface | CORBA, Web services, FTP |
| | Example of communication between the PCC and the PE/P | TMF814, SNMP, XML, TL-1 |
| | Example of policy protocols | [IETF RFC 2748] |
| | Example of auto-discovery mechanisms | [IETF LMP], [OIF UNI 1.0], [ITU-T G.7714.1] |

## BIBLIOGRAPHY

[IETF RFC 2547 *bis*] ROSEN (E.), REKHTER (Y.): BGP/MPLS IP VPNs, (draft-ietf-l3vpn-rfc2547bis-01.txt), *work in progress in IETF*.

[IETF GVPN] OULD-BRAHIM (H.), REKHTER (Y.): GVPN Services: Generalized VPN Services using BGP and GMPLS Toolkit, (draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-04.txt), *work in progress in IETF*.

[IETF GMPLS OSPF] KOMPELLA (K.), REKHTER (Y.): OSPF Extensions in Support of Generalized Multi-Protocol Label Switching, (draft-ietf-ccamp-ospf-gmpls-extensions-12.txt), *work in progress in IETF*.

[OIF Routing E-NNI 1.0] ONG (L), *et al.*: Draft OIF Specification for Intra-Carrier E-NNI Routing using OSPF (*oif2003.259*).

[IETF VR] KNIGHT (P.), OULD-BRAHIM (H.): Network based IP VPN Architecture using Virtual Routers, (draft-ietf-l3vpn-vpn-vr-01.txt), *work in progress in IETF*.

[IETF GMPLS Overlay] SWALLOW (G.), *et al.*: GMPLS UNI: RSVP-TE Support for the Overlay Model, (draft-ietf-ccamp-gmpls-overlay-04.txt), *work in progress in IETF*.

[IETF LMP] LANG (J.): Link Management Protocol (LMP), (draft-ietf-ccamp-lmp-10.txt), *work in progress in IETF*.

## SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2004