



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

1	Scope	1
2	References.....	1
2.1	Normative references.....	1
2.2	Informative references.....	2
3	Definitions	2
4	Abbreviations.....	3
5	Classification of functions	4
6	Service scenarios, service features and required functions	8
6.1	Description of functions with service features	8
6.2	Examples of service scenarios and required functions.....	9
7	Architecture classification	11
7.1	Provider network architecture	11
7.2	Customer network architecture.....	16
7.3	Management architecture	17
8	Layer 1 VPN functional architecture concepts.....	19
8.1	Architecture constructs.....	19
8.2	Resource allocation schemes	20
8.3	Private addressing.....	23
9	Layer 1 VPN functional entities architecture	24
9.1	Membership information maintenance and connectivity policy management.....	24
9.2	Routing information maintenance and route computation	25
9.3	Connection control	26
9.4	Management	26
10	Examples of functional architecture	26
10.1	Distributed provider network architecture.....	26
10.2	Hybrid provider network architecture	29
10.3	Centralized provider network architecture	32
11	Implementation examples of functional architecture	33
11.1	Overview	33
11.2	Distributed provider network architecture.....	34
11.3	Hybrid provider network architecture	38
11.4	Centralized provider network architecture	39
12	Security aspects	39

	Page
Annex A – Detailed description of CE and PE	40
A.1 Architecture of CE participating in multiple Layer 1 VPNs (constructs from ITU-T Recs G.805 and G.8080/Y.1304)	40
A.2 Architecture of PE participating in multiple Layer 1 VPNs (constructs from ITU-T Recs G.805 and G.8080/Y.1304)	41
A.3 Architecture of CE and PE in relation with management systems.....	41
Appendix I – Implementation examples of existing mechanisms for Layer 1 VPN	42
BIBLIOGRAPHY	43

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

- [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:

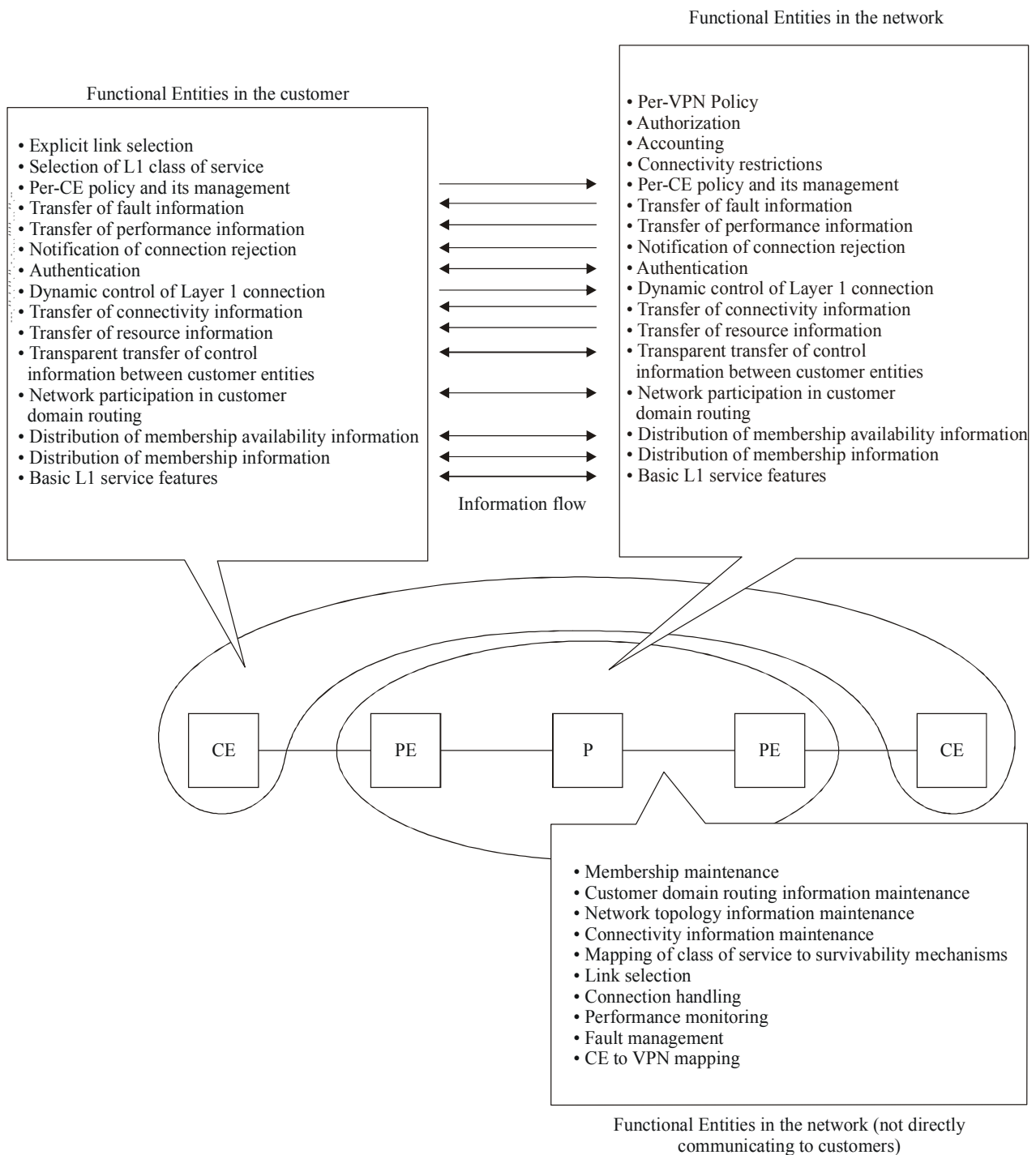
AAA	Authentication, Authorization and Accounting
BGP	Border Gateway Protocol
CCC	Customer Centralized Controller
CE	Customer Edge
CNM	Customer Network Management
COPS	Common Open Policy Service
CORBA	Common Object Request Broker Architecture
CP	Connection Point
CUG	Closed User Group
DCN	Data Communications 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.

...



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 – 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