International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2113

(01/2009)

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

Next Generation Networks – Quality of Service and performance

Ethernet QoS control for next generation networks

Recommendation ITU-T Y.2113

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.

Recommendation ITU-T Y.2113

Ethernet QoS control for next generation networks

Summary

Recommendation ITU-T Y.2113 specifies dynamic Ethernet quality of service (QoS) control for next generation networks. Specifically, it defines service definitions and general requirements, a QoS control architecture, and a set of traffic management mechanisms for Ethernet-based NGNs. Related OAM and protection and restoration mechanisms are specified by reference to other Recommendations.

Source

Recommendation ITU-T Y.2113 was approved on 23 January 2009 by ITU-T Study Group 13 (2009-2012) under Recommendation ITU-T A.8 procedures.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T Y.2113

Ethernet QoS control for next generation networks

1 Scope

This Recommendation addresses Ethernet quality of service (QoS) control for next generation networks. It specifies the following:

- Service definitions and general requirements for Ethernet-based NGNs.
- Reference model of QoS architecture for Ethernet-based NGNs.
- Traffic management mechanisms for Ethernet-based NGNs.
- Operation, administration and maintenance (OAM) mechanisms for Ethernet-based NGNs.
- Protection and restoration mechanisms for Ethernet-based NGNs.

The OAM and protection and restoration mechanisms are specified by reference to other Recommendations.

Ethernet-based NGN is broadly characterized as the employment of IP protocols for the control of Ethernet data flows. In the data link layer, data link features and interfaces defined in [b-IEEE 802.3] will not be altered.

As considered in this Recommendation, the Ethernet network encompasses not only the customer's local network but also the operator's access and core networks, which are assumed to employ Ethernet technology.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.7041] Recommendation ITU-T G.7041/Y.1303 (2005), *Generic framing procedure (GFP)*.

[ITU-T G.8001] Recommendation ITU-T G.8001/Y.1354 (2008), *Terms and definitions for Ethernet frames over transport*.

[ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.

[ITU-T G.8011] Recommendation ITU-T G.8011/Y.1307 (2004), *Ethernet over Transport – Ethernet services framework*.

[ITU-T G.8012] Recommendation ITU-T G.8012/Y.1308 (2004), *Ethernet UNI and Ethernet NNI*.

[ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2007), *Characteristics of Ethernet transport network equipment functional blocks*.

[ITU-T G.8031] Recommendation ITU-T G.8031/Y.1342 (2006), *Ethernet linear protection switching*.

[ITU-T G.8032] Recommendation ITU-T G.8032/Y.1344 (2008), *Ethernet ring protection switching*.

[ITU-T Y.1221] Recommendation ITU-T Y.1221 (2002), *Traffic control and congestion control in IP-based networks*.

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services*.

[ITU-T Y.1730] Recommendation ITU-T Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[ITU-T Y.1731] Recommendation ITU-T Y.1731 (2006), *OAM functions and mechanisms for Ethernet based networks*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2006), *Resource and admission control functions in Next Generation Networks*.

[IEEE 802.1Q] IEEE Standard 802.1Q (2005), IEEE standard for local and metropolitan area networks – *Virtual Bridged Local Area Networks*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Ethernet user to network interface (E-UNI): An interface that uses the Ethernet frame structure between a user (an end user or a customer network) and a network element of the transport network.

3.2.2 Ethernet network to network interface (E-NNI): An interface that uses the Ethernet frame structure between network elements within separate transport networks.

3.2.3 Ethernet virtual connection (EVC): An instance of an association of two or more E-UNIs. These E-UNIs are said to be "in the EVC". A given UNI can support more than one EVC via the service multiplexing attribute.

NOTE – This terminology is used in a different way as defined in [ITU-T G.8011] and [ITU-T G.8001].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AAA	Authentication, Authorization, Accounting
AR	Access Rate
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
B-Tag	Backbone VLAN Tag
BW	Bandwidth

CAC	Connection Admission Control
CBR	Constant Bit Rate
CBS	Committed Burst Size
CE	Customer Edge
CF	Coupling Flag
CIR	Committed Information Rate
CL-PS	Connectionless, Packet-Switched
CM	Colour Mode
CMTS	Cable Modem Termination System
CO-CS	Connection Oriented, Circuit-Switched
CO-PS	Connection Oriented, Packet-Switched
CoS	Class of Service
CPE	Customer Premises Equipment
C-Tag	Customer VLAN Tag
C-VID	Customer VLAN ID
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
E-AF	Ethernet Assured Forwarding
E-DF	Ethernet Default Forwarding
E-EF	Ethernet Expedited Forwarding
E-LAN	Ethernet LAN
E-LINE	Ethernet Line
E-NNI	Ethernet Network to Network Interface
E-PHB	Ethernet Per-Hop Behaviour
E-Tree	Ethernet Tree
E-UNI	Ethernet User to Network Interface
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EBS	Excess Burst Size
EIR	Excess Information Rate
EPL	Ethernet Private Line
EPLAN	Ethernet Private LAN
EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line
EVPLAN	Ethernet Virtual Private LAN
FRS	Frame Relay Service
GFP	Generic Framing Procedure

GGSN	Gateway GPRS Support Node
GMPLS	Generalized MultiProtocol Label Switching
GPRS	General Packet Radio Service
I-Tag	Backbone Service Instance Tag
ID	Identifier
IP	Internet Protocol
LDP	Label Distribution Protocol
LSP	Label Switched Path
MAC	Media Access Control
MBS	Maximum Burst Size
MPLS	MultiProtocol Label Switching
NACF	Network Attachment Control Function
NGN	Next Generation Network
nrt-VBR	non real-time Variable Bit Rate
OAM	Operation, Administration and Maintenance
OTH	Optical Transport Hierarchy
P-Tag	Provider Tag
PAE	Port Access Entity
PD-FE	Policy Decision Functional Entity
PDH	Plesiochronous Digital Hierarchy
PE-FE	Policy Enforcement Functional Entity
PE	Provider Edge
PNNI	Private Network to Network Interface
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RADIUS	Remote Authentication Dial In User Service
RARP	Reverse Address Resolution Protocol
RSVP	Resource ReserVation Protocol
S-Tag	Service VLAN Tag
SCF	Service Control Functions
SDH	Synchronous Digital Hierarchy
SGSN	Serving GPRS Support Node
SLA	Service Level Agreement
SONET	Synchronous Optical Network
TE	Traffic Engineering
TPID	Tag Protocol Identifier
TRC-FE	Transport Resource Control Functional Entity

UNI	User to Network Interface
VBR	Variable Bit Rate
VC	Virtual Connection
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network

5 Conventions

None.

6 Concept and general requirements for the Ethernet-based NGN

6.1 Definition of Ethernet-based NGN concept

The key idea of Ethernet-based NGN is to use the Ethernet frame format throughout an NGN transport network. No format conversion occurs during the end-to-end delivery of Ethernet frames. Without a change in the basic Ethernet frame format, it is required that the Ethernet header fields contain information of QoS provisioning as specified in [IEEE 802.1Q] in order to support the control and management functions of NGN. Ethernet-based NGN means the network using the Ethernet technology through any physical media, including fixed and wireless environments in the NGN transport stratum. The Ethernet-based NGN services are various services provided by network operators using Ethernet transport networks. Figure 1 illustrates the generic architecture model and services of Ethernet-based NGN. The Ethernet is a transfer medium for core transport as well as the access transport of NGN.

It is optional that non-Ethernet-based access networks (e.g., DSL) are connected to Ethernet-based core networks. However, non-Ethernet-based access network technologies are beyond the scope of this Recommendation.

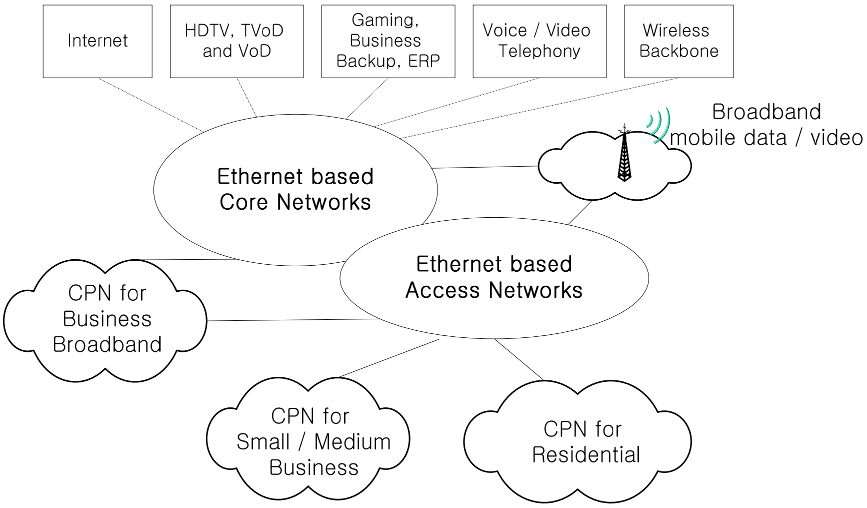

Internet
HDTV, TVoD and VoD
Gaming, Business Backup, ERP
Voice / Video Telephony
Wireless Backbone
Broadband mobile data / video
Ethernet based Core Networks
Ethernet based Access Networks
CPN for Business Broadband
CPN for Small / Medium Business
CPN for Residential

Figure 1 – Generic architecture model and services of Ethernet-based NGN

6.2 General requirements for Ethernet-based NGN service

The general requirements for the Ethernet-based NGN service fall into two categories: user equipment and network.

User equipment is required to:

- Support the same Ethernet frame format for fixed and wireless transport interfaces while various transport technologies are applied.
- Provide auto-discovery capability such as ARP/RARP.
- Provide the relevant QoS/TE requesting capability with traffic parameters according to SLA depending on the applications.
- Provide Ethernet frame tagging using IEEE 802.1Q VLAN tags for the Ethernet traffic management.

The network is required to:

- Support capabilities of OAM, protection and restoration, and load sharing.
- Support the VPN capability. The existing VLAN can be extended or changed to support the NGN core network.
- Provide an auto-configuration capability such as neighbour discovery.
- Provide access control capability based on the MAC address and/or VLAN ID including security.
- Provide the traffic contract function and QoS class mapping between access networks and core networks.
- Provide the Ethernet traffic management mechanisms to guarantee the requested QoS/TE requirements depending on the different Ethernet services.

7 QoS architecture for the Ethernet-based NGN

7.1 Introduction

It is required that the QoS architecture for Ethernet-based NGN meets the following control and management requirements:

- Flexible connection configuration and bandwidth allocation:
  - Dynamic provision for end-to-end connectivity.
  - Priority, access control, security protection.
  - TE/QoS handling for acceptable end-to-end quality.
- Various VPN services:
  - Access control, QoS and security according to VPN services.
- Integration of switching capabilities:
  - TE/QoS, routing, control processing.
  - Binding of MAC address and VLAN ID.

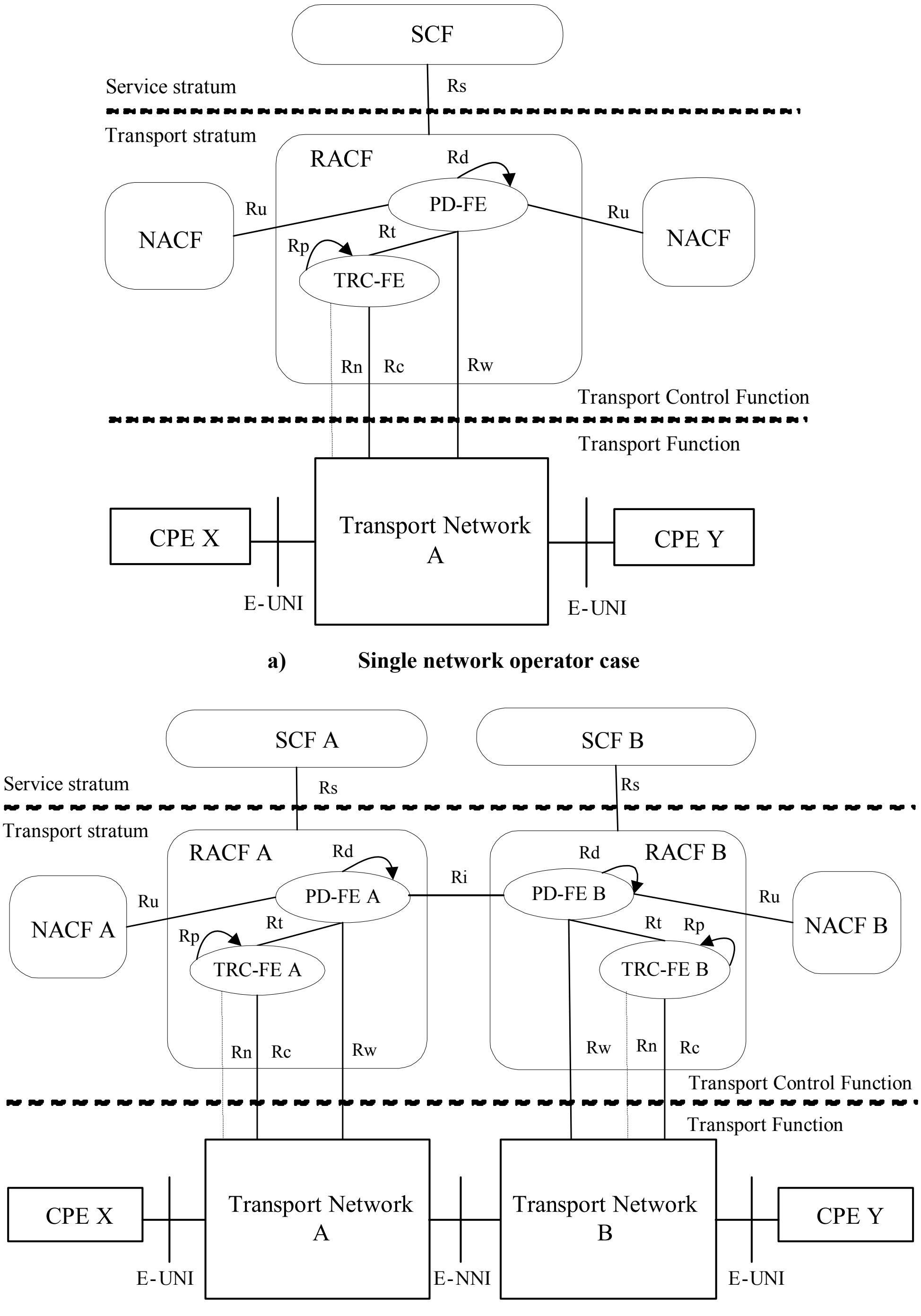
Ethernet-based NGN depends on the QoS/TE capabilities of each layer. For example, the QoS/TE capability of IP over Ethernet over SDH depends on IP QoS/TE (layer 3), Ethernet QoS/TE (layer 2), and SDH QoS/TE (layer 1) capabilities. Therefore, the QoS/TE mappings between different layer protocols are important.

7.2 Reference model

Figure 2 shows the reference model for Ethernet-based NGN by focusing on dynamic QoS control [ITU-T Y.2012], [ITU-T G.8010] and [ITU-T Y.2111]. The interface between the customer and the operator is an Ethernet user-to-network interface (E-UNI). Ethernet services are offered by concatenating a number of operator networks. The interfaces between different operator networks are Ethernet network-to-network interfaces (E-NNIs).

Figure 2-a illustrates a case where the access and core networks are managed by the same operator (i.e., are in a single administrative domain), and Figure 2-b illustrates a case where there are multiple network operators. In both Figure 2-a and Figure 2-b, it is possible that the functional entities TRC-FE and PD-FE reside in the access transport and core transport.

All reference points and functional entities specified in [ITU-T Y.2111] apply to the Ethernet-based NGN defined in this Recommendation. In particular, the Rn reference point, which is transport-technology dependent, is required to support information components such as network connectivity, transfer characteristics, link type, traffic separation, connectivity monitoring, bandwidth profile, UNI list, preservation, survivability as defined in [ITU-T G.8011]. The details of the Rn reference point specific to the Ethernet transport are for further study.



a) Single network operator case

b) Multiple network operator case

Figure 2 – Reference model of Ethernet-based NGN

The E-UNI is an Ethernet interface in both the physical layer and media access control (MAC) layer. Ethernet frames exchanged across the E-UNI are formatted as defined in [IEEE 802.1Q]. Ethernet frames are untagged or tagged with VLAN tag control information. VLAN tag control information consists of the VLAN ID and user priority bits (commonly referred to as p-bits). The frames defined in [IEEE 802.1Q], however, are inadequate to support OAM and protection of VPN services. Therefore, the Ethernet frame from the E-UNI is encapsulated in the link layer payload at the E-NNI. Frame encapsulation is further described in clause 7.3.6. Ethernet frames are transported inside the transport network using the deployed native transport technology. It is optional that the transport technology is CO-CS (connection oriented, circuit-switched), CO-PS (connection oriented, packet-switched), or CL-PS (connectionless, packet-switched). Table 1 lists some examples of the different transport technologies that are currently deployed.

Table 1 – Examples of transport technologies and services

Technology	Examples
CO-CS	SONET, SDH
CO-PS	ATM, FRS, MPLS
CL-PS	Ethernet

For CO-CS, Ethernet frames are encapsulated using the generic framing procedure (GFP) [ITU-T G.7041] frame encapsulation. Ethernet frames are then transparently transported across the circuit-switched networks. For packet-switched transport, Ethernet frames are encapsulated and forwarded using a native transport technology, e.g., ATM.

7.2.1 Bandwidth profile

Figure 3 shows an example of bandwidth profile per service attributes. The bandwidth profile applies to all of the frames per E-UNI, E-NNI, EVC, CoS, physical port or L2/L3 information. Multiple bandwidth profiles exist simultaneously at the E-UNI/E-NNI. However, for a given frame, only one bandwidth profile will apply.

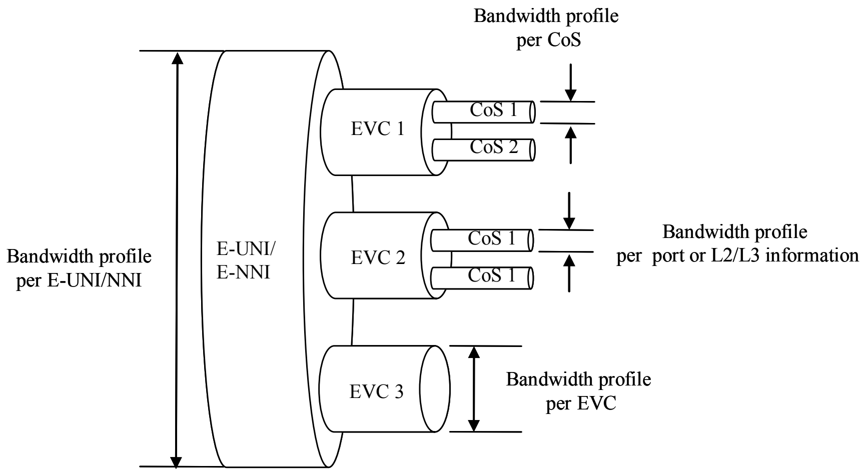


Figure 3 – Bandwidth profile per service attribute

7.2.2 Ethernet virtual connection (EVC)

The EVC extends between two E-UNIs. Across the E-UNI, one or more VLAN IDs are mapped to the same EVC. An EVC supports multiple CoSs as identified by p-bits. Service classes vary in terms of their QoS requirements. Each of those service classes is considered a separate CoS instance.

It is required that an EVC has one of four possible types with respect to class of service and bandwidth profile:

- Single-CoS EVC wherein all frames belonging to EVC are treated in the same manner and transported with equal bandwidth profile.
- Single-CoS EVC with multiple bandwidth profiles wherein frames belonging to EVC are treated in the same manner but are transported with different bandwidth profiles.
- Multi-CoS EVC with a single bandwidth profile wherein frames are treated differently according to their classes of service, even as all frames are transported with equal bandwidth profile.
- Multi-CoS EVC with multiple bandwidth profiles, wherein frames are treated differently according to their classes of service, and frames are transported with CoS-designated bandwidth profile.

In the case of single-CoS EVC with multiple bandwidth profiles, input frames from E-UNI are untagged frames that have the same priority, whereas bandwidth profiles can be assigned based on physical ports or L2/L3 information (e.g., MAC address, IP address).

7.2.3 Ethernet user to network interface (E-UNI)

E-UNI is the interface as defined in clause 3.2. A single E-UNI supports several EVCs destined for different destinations. Similar to EVC, it is required that E-UNI has one of four types with respect to class of service and bandwidth profile.

7.2.4 Ethernet network to network interface (E-NNI)

The E-NNI is the interface as defined in clause 3.2. A single E-NNI supports more than one EVC destined for different destinations. Similar to EVC, it is required that E-NNI has one of four types with respect to class of service and bandwidth profile.

It is possible that E-NNI's OAM and fault handling use policies as inputs. In such a case, protection and restoration behaviour varies depending on the policies for each connection and/or EVC.

E-NNI's OAM and fault handling include the following functions:

– Transfer of performance information.

– Transfer of fault information.

– Performance monitoring.

– Fault management.

The related information is exchanged according to the tag field of the frames. To be mapped with E-UNI classes using the IEEE 802.1Q format, it is required that E-NNI supports at least 8 classes of service.

7.3 VPN configuration

A VPN delivers a multipoint-to-multipoint Ethernet service that can span one or more metro areas and provides connectivity between multiple sites as if they were attached to the same Ethernet LAN. Unlike the current Ethernet multipoint-to-multipoint service delivered over network operator infrastructure consisting of Ethernet switches, it is possible that a VPN uses the MPLS network operator infrastructure [b-IETF RFC 2917]. From the network operator's point of view, the use of QoS routing protocols and procedures instead of the spanning tree, protocol and MPLS labels instead of VLAN IDs within the network operator infrastructure, result in significant improvements in the scalability of VPN as a service.

7.3.1 VPN reference model

Figure 4 shows the reference model of a VPN. The network operator transports the Ethernet frames between CEs belonging to the same VPN through the tunnel. The VPN creates groups of users that are separated from other network users and communicate among them as if they were attached to the private network.

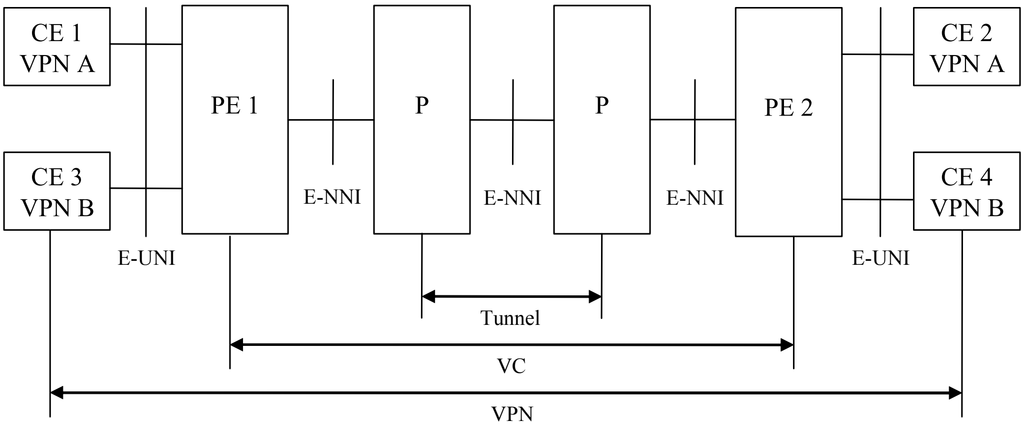


Figure 4 – Reference model of VPN

A VPN is composed of CE (customer edge), PE (provider edge) and P (provider core node). The explanation for each device is as follows:

- CE has the functionality needed on the CPE to access the services specified by the VPN.
- PE has the functionality needed on the edge of the network operator to interface with the CE.
- P is a node in the core network that does not have interfaces to customers.
- VC (virtual connection) is an identifier used to distinguish Ethernet frames transferred by a tunnel that belongs to a particular VPN. A VC label is assigned to the Ethernet frames based on VLAN ID or port ID.
- A tunnel is established in a core network for transferring Ethernet frames among the P nodes.

7.3.2 VPN configuration requirements

Typical VPN topologies include point-to-point, point-to-multipoint, multipoint-to-multipoint, mixed (e.g., partial mesh) and hierarchical. VPN configuration requirements are as follows:

- It is required that VPNs support unicast traffic. It is optional that VPNs support broadcast and multicast traffic.
- When VPN spans multiple administrative domains, it is required that the VPN service be able to act and appear as a single, homogeneous VPN from the customer point of view.
- VPN transports the encapsulated traffic of Ethernet frames. It is required that the VPN header, with the exception of the source MAC address, be preserved transparently from source to destination.
- It is recommended that the security features supported by VPN be configurable on a per-customer basis.
- It is required that QoS provisioning be supported.

7.3.3 VPN functions

The following VPN functions are required.

- Configuration between VLAN priority and MPLS CoS:

  VLAN priority bits are mapped into the corresponding MPLS CoS fields and vice versa. Such mapping is configured automatically or manually at both ingress and egress nodes based on the policy of network operators.

- Auto-discovery:

  Auto-discovery is critical to enable network operators to minimize operational costs, since it automates the creation of VPNs.

  The new PE joins a VPN when the VPN instance is configured on that PE, with one or more customer-facing ports on that PE associated with such a VPN instance. In this case, PE advertises that it is part of the VPN domain via the route reflector to other PEs joined in such a VPN instance. At this time, all appropriate PEs are "aware" of the new PE and these PE members now have all the information they need to configure the VPN with the new PE automatically.

- MAC address learning:

  MAC address learning for configuring VPN is a method of disseminating MAC addresses to discover network devices through a plurality of network switches that co-operate to enable maintaining multiple active paths between such devices. Newly discovered MAC addresses are attached to the ports of an edge switch for dissemination through the network switches. When an edge switch detects a device with a previously unknown MAC address, a MAC address information packet is generated and disseminated. The received MAC address information packet is used to update the MAC address tables in the receiving switch. Afterward, the received MAC address packet is forwarded from each receiving intermediate switch to other neighbour switches in the load balance domain.

- Full mesh tunnelling:

  Although it offers multipoint connectivity, the VPN is created with a full mesh of point-to-point pseudo-wires between the participating operator edge routers. The VPN uses an MPLS core; on the edges, it multiplexes and creates pseudo-wires to each router participating in the VPN network. As a result, a full mesh of pseudo-wires is required to support the service. Signalling for VPN relies on control sessions between edge routers for setting up and maintaining connections. Tunnel labels, making up the unidirectional tunnel label switched path (LSP), are established with link LDP or RSVP-TE signalling. The appropriate control protocol is used to perform signalling and session negotiation between tunnel endpoints.

- VPN multicast:

  The general goal of multicast is to employ a tree-like delivery channel to avoid multiple transmissions over the same physical links. The VPN multicast configuration consists of one multicast tree per VPN or one per suitable set of VPNs. It is required that all multicast applications within the VPN forward the multicast packets along the tree to all respective PEs.

7.3.4 QoS parameter mapping between E-UNI and E-NNI

During the VPN set-up, it is required that the ingress node map the QoS parameters of the E-UNI tag information into those of the E-NNI tag information.

It is required that the egress node consider the priority and CoS fields of the E-NNI tag information when queuing the frame at the VLAN bound. Figure 5 shows some examples.

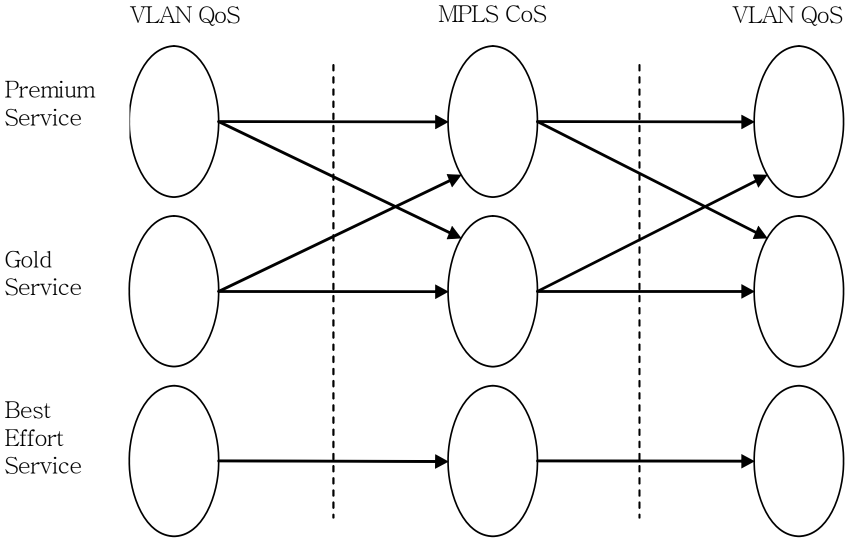


Figure 5 – Example of QoS parameter mapping

An ingress node supports the ability to carry Ethernet VPN as a best-effort service over the MPLS network [b-IETF RFC 4664] and [b-IETF RFC 4665]. The priority field of the VLAN is kept transparent between ingress node device and egress node device regardless of the QoS support of the core network.

If the VLAN field is added at the egress node, it is required that a default priority field setting of zero is supported and a configured default value is recommended. Otherwise, it is possible that the value is mapped from the CoS field of the core network.

An ingress node supports additional QoS through one or multiple CoS per VPN service. As a policy of the VPN network operator based on an agreement with the customer, the guaranteed rate is different from the Ethernet physical port rate.

Examples of the QoS mapping relationship in the VPN service include:

- The classification to CoS is based on the VLAN field regardless of the VLAN priority bits. The CoS is assigned to a specific value based on the VPN policy.
- The classification to the CoS is based on the VLAN field and priority bits.

7.3.5 VPN service models

VPN services are supported by the E-LINE (Ethernet line service), E-LAN (Ethernet LAN) and E-Tree service using EVC. A VPN ID is assigned globally and uniquely to an E-LINE, an E-LAN or an E-Tree service shared by the designated group of customers. VPN ID is associated with a specific level of CoS to deliver the same or equivalent QoS to all customers of VPN across different domains of network operators.

NOTE – E-LINE, E-LAN and E-tree services are differently defined in [ITU-T G.8011] from the viewpoint of E-UNI.

- E-LINE service:

  Point-to-point EVC between two E-UNIs can create EPL (Ethernet private line) and EVPL (Ethernet virtual private line) services using the E-LINE service type. For these services, Ethernet flow is delivered to an MPLS tunnel according to the given VLAN ID or default VLAN ID depending on the tagged or untagged port. The EPL service provides a high degree of transparency for service frames between E-UNIs. On the other hand, the EVPL service does not need full transparency for the service frames due to permission of service multiplexing at E-UNI, which allows more than one EVC to be supported at E-UNI.

Figure 6 shows an example of the E-Line service model. This figure illustrates three point-to-point EVCs: EVC1, EVC2, and EVC3. A point-to-point EVC is an EVC with exactly two E-UNIs. CE means equipment on the customer side of the E-UNI.

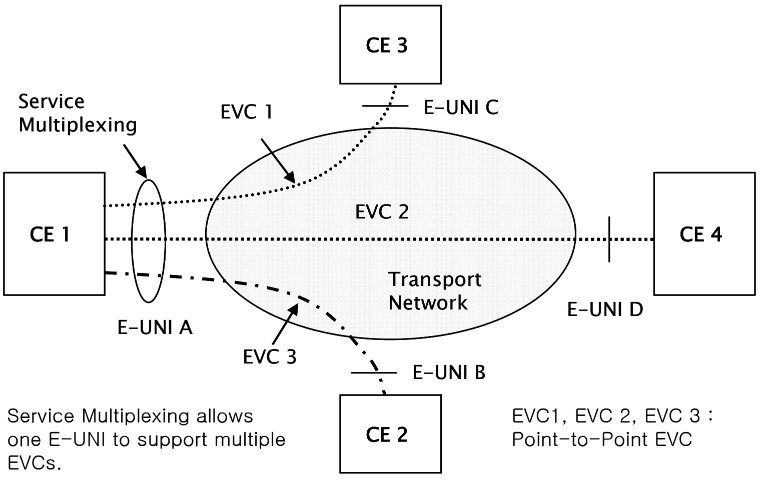

CE 3
Service Multiplexing
EVC 1
E-UNI C
CE 1
EVC 2
CE 4
Transport Network
E-UNI D
E-UNI A
EVC 3
E-UNI B
Service Multiplexing allows one E-UNI to support multiple EVCs.
CE 2
EVC1, EVC 2, EVC 3 : Point-to-Point EVC

Figure 6 – E-Line service model

- E-LAN service:

  Multipoint-to-multipoint EVC can be used to provide the E-LAN service. The E-LAN service is inherently for multipoint-to-multipoint VPN such that the MPLS multicasting function is supported [b-IETF RFC 4761] and [b-IETF RFC 4762]. For this service, a group address is set per MPLS tunnel, per VLAN, per VPN, etc.

The E-LAN service is classified by EPLAN (Ethernet private LAN) and EVPLAN (Ethernet virtual private LAN) service. EPLAN service provides dedicated connectivity for multipoint LANs. In the case of EVPLAN services, each E-UNI supports multiple VLANs, as well as both point-to-point and multipoint connections [b-MEF6]. Figure 7 shows an example of EPLAN service, providing multipoint-to-multipoint connectivity across the transport networks between a pair of non-service multiplexed E-UNIs. A multipoint-to-multipoint EVC is an EVC with more than two E-UNIs.

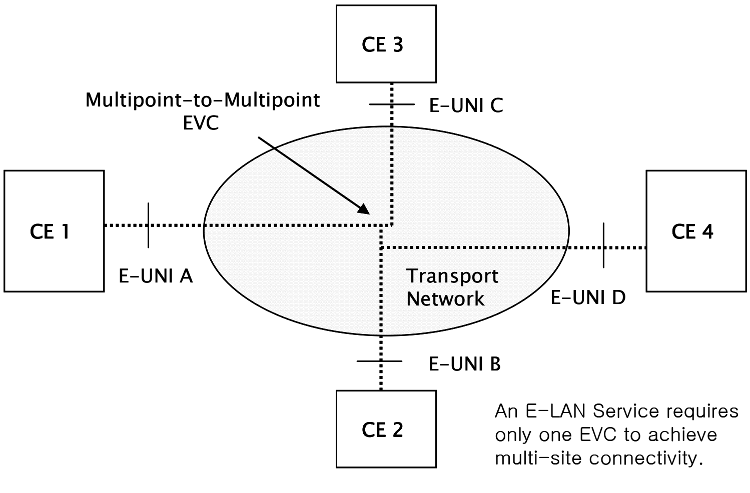

CE 3
Multipoint-to-Multipoint EVC
E-UNI C
CE 1
CE 4
E-UNI A
Transport Network
E-UNI D
E-UNI B
CE 2
An E-LAN Service requires only one EVC to achieve multi-site connectivity.

Figure 7 – E-LAN service model

- E-Tree service:

  In an E-Tree multipoint EVC, one E-UNI is designated as the roots, and all the others are designated as leaf nodes. Ingress service frames at a root are delivered to any leaf nodes in the EVC. Ingress service frames at a leaf are only delivered to the root. Leaf nodes do not send frames to each other directly. Frames sent from two leaf nodes are delivered through the root. E-Tree service is inherently a point-to-multipoint VPN which provides an MPLS multicasting function [b-IETF RFC 3353]. For this kind of service, a group address is set according to per MPLS tunnel, per VLAN, every VPN.

Figure 8 shows an example of the E-Tree service model. In this example, the point-to-multipoint EVC allows multiple leaf E-UNIs to communicate with the same root E-UNI simultaneously.

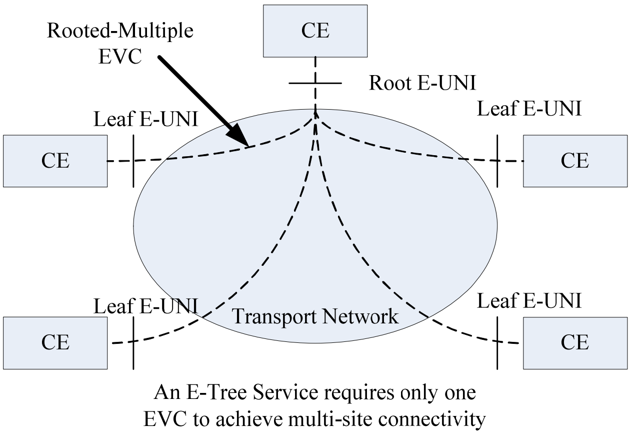


Figure 8 – E-Tree service model

7.3.6 Frame encapsulation in the VPN

To support VPN services, Ethernet frames are encapsulated in the link layer payload at the E-NNI for transport across the core networks.

Figure 9 shows the required frame encapsulation in support of VPN services. C-Tag is the customer VLAN Tag, which includes a TPID and C-VID as specified in [IEEE 802.1Q]. P-Tag could be the MPLS label or provider-specified label. The frame type at the E-UNI is one of untagged frame, priority tagged frame or tagged frame of [IEEE 802.1Q]. A frame is mapped to a tagged frame representing C-tag and the tagged frame is encapsulated in the P-tag frame at the PE. It is optional that the link header is added to the P-tag frame depending on the type of link layer.

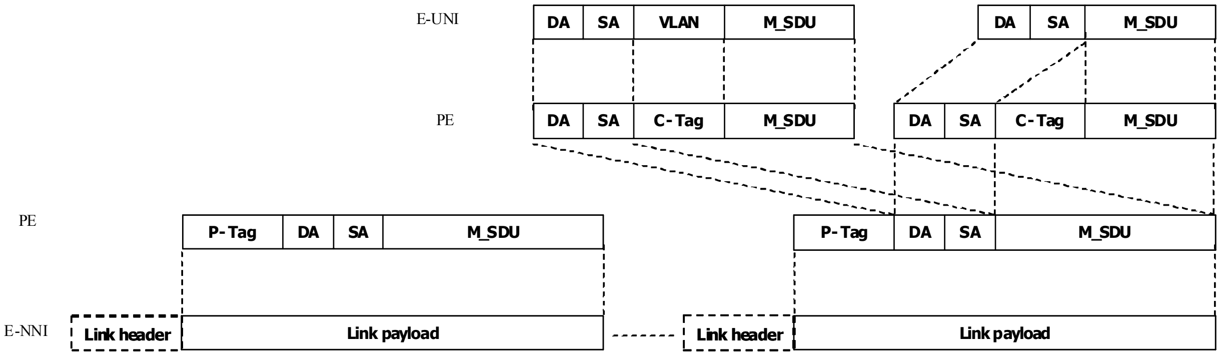


Figure 9 – Frame encapsulation in VPN

7.4 High layer switching

While the layer 3 switch performs IP-based routing, layer 4~7 switching capabilities forward packets to appropriate destinations based on the upper layer information. Unlike layer 2 or layer 3 switching, the upper layer information is utilized to make switching decisions. Through the analysis of TCP/UDP port information (HTTP, FTP, Telnet, SMTP, POP3, etc.), layer 4 switching delivers packets with the same destination IP address to different destinations in a local domain.

Furthermore, layer 4 information can be used to prioritize and queue traffic. Layer 7 switching looks inside the application layer field to make forwarding decisions. Depending on the contents, such as HTTP contents, cookie information, FTP file names and e-mail titles, traffic can be directed to different paths. The major benefits provided by layer 4~7 switching capabilities are failover of various servers and network security by preventing monopoly over network resources.

Support of layer 4~7 switching capabilities requires the binding of the Ethernet MAC address with a high layer service. Multiple Ethernet MAC addresses can be assigned to the same destination IP address and/or port number. By examining the information on the high layer, a mapping rule given by a switch operator finds a proper destination Ethernet MAC address.

7.5 Access control

Network access control makes use of the physical access characteristics to provide the means for authenticating and authorizing devices attached to a physical port and to prevent access to a such port in cases wherein the authentication and authorization process fails. Examples of ports wherein the use of authentication can be desirable include the ports of MAC bridges and the ports used to attach directly to the LAN.

It is recommended that access control be based on [b-IEEE 802.1X]. Appendix I provides further information.

8 Traffic management for Ethernet-based NGN

8.1 Overview

Users can select or request their own QoS/TE with the relevant parameters from the network operator. CAC requires the knowledge of certain parameters to operate efficiently. In particular, it is recommended that the network operator's transfer capability, the source traffic descriptor, connection admission priority and the requested QoS classes are taken into account.

A network operator's capability, a source traffic descriptor, and an associated QoS class are declared by the user at connection establishment by means of signalling or subscription.

For a given network operator's connection, the source traffic descriptor belonging to the traffic contract and all parameter values of this source traffic descriptor are the same at all standardized interfaces along the connection.

To meet QoS commitments, a conformance definition is specified at the AAA server for any given network operator's transfer capability. A conformance definition also pertains to each standardized network-to-network interface. A traffic contract applies to an Ethernet virtual flow. Therefore, the conformance definition at an interface applies to the level where the traffic contract is defined. The conformance definition also covers the reverse connection.

CAC is operator specific. Once the connection has been accepted, the value of CAC and E-UNI/E-NNI parameters are set by the network based on the network operator's policy.

8.2 Ethernet QoS services

Edge mechanisms and network forwarding classes are combined to define a set of Ethernet QoS services. Service categories are defined by specifying the traffic parameters, edge rules, network forwarding classes and other corresponding IP QoS parameters. Table 2 shows the Ethernet QoS services.

Table 2 – Ethernet QoS services

Ethernet QoS service	Traffic parameter	Edge rule	Forwarding class (Associated DiffServ PHB)	Y.1221 transfer capability	Y.1541 IP QoS class
Premium service	CIR > 0 CBS > 0 EIR = 0 EBS = 0	Drop non-conforming frames	E-EF	Dedicated bandwidth	QoS classes 0, 1, 6 and 7
Gold service	CIR > 0 CBS > 0 EIR > 0 EBS > 0	Admit non-conforming frames up to EIR. Excess frames are assigned high discard precedence	E-AF with minimum bandwidth assurances. No delay bound. Drop excess frames first in case of congestion.	Delay-sensitive statistical bandwidth	QoS classes 2, 3 and 4
Best-effort service	CIR = 0 CBS = 0 EIR > 0 (possibly equal physical rate) EBS > 0 (large)	All frames are admitted with high discard precedence	E-DF No bandwidth assurances. No delay bound. Drop first in case of congestion.	Best effort	QoS class 5 (unspecified)

The premium service is useful for those applications requiring stringent bounds on both frame loss and frame delay. The service does not allow excess frames (defined as frames that are non-conforming to CIR) into the network. It is most suitable for EPL (Ethernet private line) application as defined in [ITU-T G.8012] on SDH networks. In this case, frame discard precedence is invisible to the nodal mechanism and there is nothing to be gained from allowing frames in the network with different discard precedence.

The gold service provides some bandwidth assurances but not any delay bounds. In that respect, it is similar to the traditional frame relay service or ATM nrt-VBR service category. This service is useful for the EVPL (Ethernet virtual private line) application that requires some bandwidth assurance but is not sensitive to delay.

The best-effort service supports the other applications that are not sensitive to delay and delay variation.

As the first column of Table 2, Ethernet QoS service is recommended to be mapped into the corresponding ITU-T Recommendations, [ITU-T Y.1541] and [ITU-T Y.1221]. These parameters are consistent with those of [b-MEF6].

8.3 Ethernet traffic management functions

Figure 10 shows the architecture for Ethernet traffic management. This figure illustrates both the service and transport stratum functions.

When the service control function (SCF) receives a request for the Ethernet-based NGN services, the SCF determines the QoS requirements for the service and informs the RACF. The RACF performs policy-based transport resource control upon the request of the SCF. The RACF interacts with transport functional entities to control traffic conditioning functions in the transport layer.

The access and/or core transport functions perform traffic conditioning for QoS control based on the policy rules received from the RACF. The traffic conditioning includes traffic classification, metering, marking and dropping/shaping.

The conformance of the Ethernet frames received at E-UNI is verified using a metering function. Based on the output of the metering, it is possible that an Ethernet frame is coloured, recoloured or dropped depending on its conformance. Frames are then marked with the appropriate core forwarding class and proceed to the network.

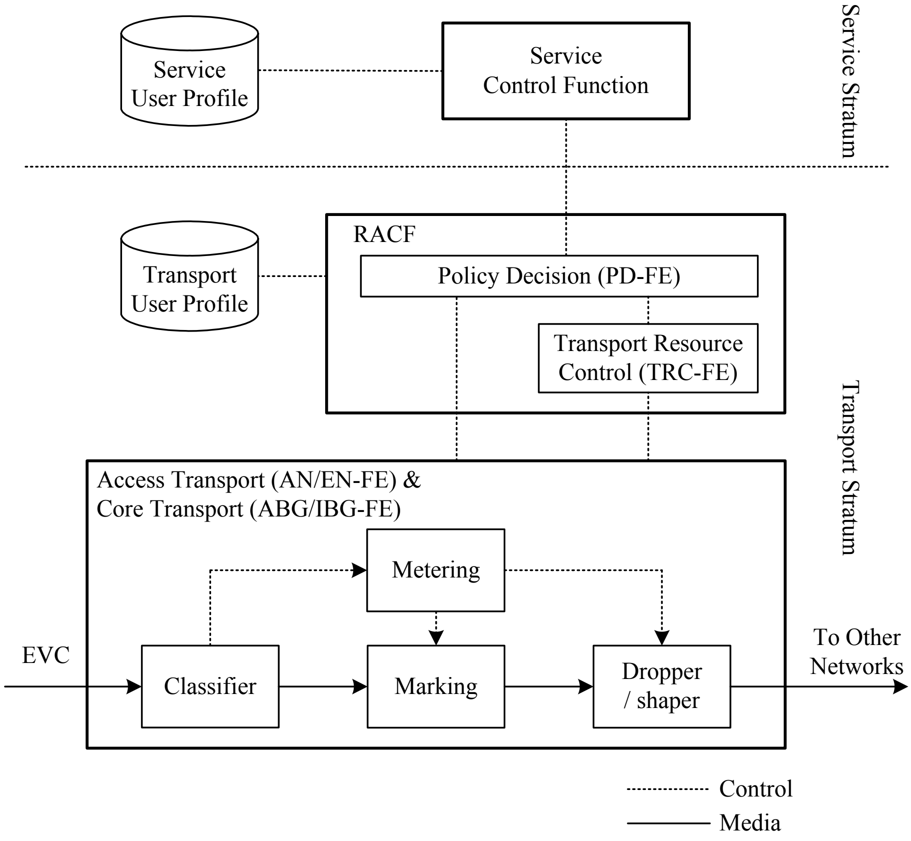


Figure 10 – Architecture for Ethernet traffic management

Traffic management mechanisms are also divided into those mechanisms implemented on the edge of the networks at the interface between the customer and the operator, and those implemented inside the network to ensure that the traffic volume does not exceed the bandwidth and to treat frames based on their performance requirements.

8.4 Traffic management mechanism for edge side

Traffic management mechanisms on the operator edge are usually concerned with ensuring that the customer submitted traffic classification adheres to a certain traffic pattern (conformance definition) and within the parameter values (traffic parameters), as agreed upon between the customer and the operator.

It is required that some actions (edge rules) are taken when the customer's traffic exceeds the assigned parameter values. Such actions usually involve dropping or marking the excess frame with a discard eligibility flag.

The main components of the edge mechanisms are collectively referred to as traffic conditioning as described in [ITU-T G.8021]. In its general form, the traffic conditioning function consists of the traffic classifier, metering, marker, dropper and shaper functions shown as in Figure 10. The following describes each of the edge functions as illustrated above.

8.4.1 Traffic classification and mapping

To identify the sequences of frames (or flows) and correlate such sequences with the traffic parameters, conformance, actions and network behaviour, traffic conditioning starts with classification.

Classification is based solely on layer 2 (Ethernet) quantities or makes use of elements of higher layers, e.g., IP. It is optional that it is also based on an EVC or the entire E-UNI.

Ethernet frames are either tagged or untagged. Tagged frames will contain the tag control information field. Both a VLAN ID and user priority bits in the field can be used for flow classification. For instance, frames with certain VLAN ID values are assigned to certain traffic parameters and network behaviour. VLAN ID values are mapped or encapsulated in LABEL and are transferred through an MPLS-based core transport network. For the case of Ethernet-based core transport networks utilizing the provider bridge and/or the provider backbone bridge, it is required that a VLAN ID be mapped to another tag (S-Tag in the provider bridge [b-IEEE 802.1ad], I-Tag or B-Tag in the provider backbone bridge [b-IEEE 802.1ah]). This mapping procedure is executed on the network edge router or access gateway by referring to the mapping table.

8.4.2 Ethernet traffic parameters and conformance definition

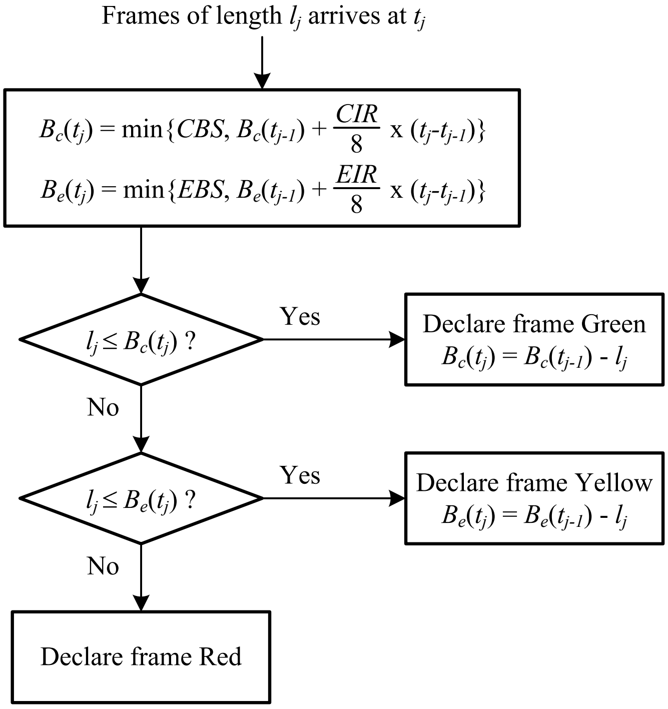
Service traffic parameters are usually associated with rate parameters as well as the corresponding measuring period. The measuring period can be expressed explicitly in seconds, i.e., rate parameters are measured over a time window of a fixed length. Alternatively, the measuring period can be stated in terms of the amount of traffic expected at a given rate.

The MEF technical specification [b-MEF10.1] defines CIR (committed information rate) and EIR (excess information rate). Related to CIR and EIR are the committed burst size (CBS) and excess burst size (EBS). Frames are accepted at the access rate (AR) as long as they are within their burst sizes. Otherwise, frames are declared to be non-conformant based on the conformance definition. There is some similarity with the FRS (frame relay service) parameters in the sense that both the CIR and EIR concepts are used. However, they differ from the FRS parameters in terms of the absence of a specified time period over which parameters are measured.

The function of the conformance definition is to determine the conformance of incoming frames to the service parameters. The conformance definition is a deterministic algorithm providing a deterministic upper bound, or a deterministic envelope, on the amount of traffic admitted to the network. A deterministic upper bound is necessary for network resource management and satisfying performance requirements.

For a sequence of ingress Ethernet frames with arrival times t_j and lengths l_j, where $j \geq 0$, the colour assigned to each frame during traffic conditioning is defined by using the algorithm shown in Figure 11 [b-MEF10.1]. For this algorithm, $B_c(t_0) = CBS$ and $B_e(t_0) = EBS$. $B_c(t)$ and $B_e(t)$ are the number of bytes in the committed and excess token buckets, respectively, at a given time t.

In addition, there are two optional parameters used to determine the behaviour of the algorithm, coupling flag (CF) and colour mode (CM) as defined in [ITU-T G.8021], but not shown in the Figure 11 for simplicity.



Frames of length l_j arrives at t_j
$B_c(t_j) = \min\{CBS, B_c(t_{j-1}) + \frac{CIR}{8} \text{ x } (t_j - t_{j-1})\}$
$B_e(t_j) = \min\{EBS, B_e(t_{j-1}) + \frac{EIR}{8} \text{ x } (t_j - t_{j-1})\}$
$l_j \leq B_c(t_j)$?
Yes
Declare frame Green
$B_c(t_j) = B_c(t_{j-1}) - l_j$
No
$l_j \leq B_e(t_j)$?
Yes
Declare frame Yellow
$B_e(t_j) = B_e(t_{j-1}) - l_j$
No
Declare frame Red

Figure 11 – Ethernet metering and marking algorithm

8.4.3 Edge rules

It is required that frames deemed non-conforming according to the conformance definition are acted upon in a certain manner. There are usually two actions associated with non-conforming frames: dropping or marking.

With dropping, non-conforming frames are not allowed to proceed beyond the edge node of the operator network. Non-conforming frames are dropped or no excess traffic is allowed in the network.

With marking, non-conforming frames are marked for discard eligibility. Discard-eligible frames are allowed in the network under the condition that no performance assurances are extended to them. Discard-eligible frames are to be dropped first when the network is in a congestion state. The volume of discard-eligible frames is usually limited, e.g., by EIR to avoid exhausting the network resources and affecting upper-layer performance negatively.

The choice between dropping and marking has a significant impact on the service offered.

8.5 Traffic management mechanisms for core side

It is required that the operator's core network is equipped with traffic management capabilities that enable satisfying the performance objectives on a frame-by-frame basis. Traffic management mechanisms inside the operator's core network are those related to transmission scheduler, buffer management and admission control.

It is recommended that traffic engineering is supported over the end-to-end transfer. Still, offering continuous traffic engineering for the different parameters of E-UNI and E-NNI is difficult. Thus, it is required that parameter mapping is done on edge routers or access gateways. Basically, traffic flows are aggregated or divided during the bridging of the different network interfaces. Traffic classification depends on the network operator's policy.

8.5.1 Ethernet per-hop behaviour (E-PHB)

Transmission scheduling and buffer management are usually referred to as nodal behaviour (in the context of the IP differentiated service, they are referred to as the per-hop behaviour (PHB)). Transmission scheduling has to do with what frame has to be transmitted first and what portion of the transmission facility has to be reserved for a particular flow or group of flows. Buffer management is concerned with the acceptance of incoming packets to a nodal buffer based on the current buffer fill and the packet-discard eligibility.

There are two main approaches for identifying the type of behaviour applied to each packet, the stateful and stateless approaches. The stateful approach is based on a connection identifier. A connection identifier determines the connection where the incoming packet belongs as well as the type of behaviour that applies to it. One example is the ATM/MPLS traffic management wherein, e.g., the MPLS label is used to define the connection and service category to which a packet belongs, e.g., CBR connection. This method requires keeping the context tables inside the node that correlates the label to its service category.

The second method is the one applied to the IP differentiated services where the packet carries in its header an indication as to what type of treatment is applied to it, e.g., priority treatment. All packets with the same bit pattern receive the same treatment from the node. This technique is perceived to be more scalable than the stateful approach.

In this clause, the differentiated service approach is extended to the Ethernet. For the case of tagged Ethernet frames, there are 3 user priority bits in the tag control information. Such bits can be used in a variety of ways to support a number of E-PHBs. Similar to differentiated service PHB, it is optional that E-PHB includes the following:

- Ethernet expedited forwarding (E-EF), which is suitable for implementing services requiring frames to be delivered with minimum delay and loss bounds. No reordering of frames is allowed.
- Ethernet assured forwarding (E-AF), which defines a number of classes with a number of discard precedences associated with each class. No reordering of frames is allowed.
- Ethernet default forwarding (E-DF), which is suitable for implementing services with no performance assurances, e.g., best effort. No reordering of frames is allowed.

Buffer management includes the provisions required to handle short- and long-term congestion. Short-term congestion is handled by buffering incoming frames during those brief periods when the frame input rate to the node exceeds the nodal bandwidth. Long-term congestion is handled by dropping the packets based on their discard eligibility. It is optional that the nodal discard algorithm includes active queue management or simple drop thresholds based on the supported applications.

8.6 Connection admission control (CAC)

The main function of connection admission control (CAC) is to limit the number of connections accepted by the network. It can limit the amount of traffic submitted to the network and consequently offers a better opportunity for satisfying the QoS requirements of the accepted connections. CAC is based on traffic parameters and QoS requirements. As mentioned earlier, traffic parameters are important because they impose a deterministic upper bound on connection traffic, thus allowing for the accurate prediction of the required resources.

8.7 Resource reservation procedure

There are two resource reservation procedures for Ethernet-based NGN service: SCF-triggered reservation and CPE-triggered reservation. Those reservation procedures are the same as those defined in [ITU-T Y.2111]:

– SCF-triggered reservation:

  The CPE can perform service QoS negotiation (such as bandwidth) through service signalling, but is unaware of QoS attributes specific to the transport. The service QoS concerns characteristics pertinent to the application. (e.g., SIP phone with SDP [b-IETF RFC 4566]/SIP QoS extensions [b-IETF RFC 3312]).

  In the SCF-triggered QoS resource reservation mechanism, the SCF sends a resource initiation request to RACF to invoke the QoS resource authorization and reservation. The RACF will push the admission control decisions into the network nodes (e.g., border gateway, edge node or access node) if the resource request is authorized and admitted.

– CPE-triggered reservation:

  The CPE supports RSVP-like or other transport signalling (e.g., GPRS session management signalling, ATM PNNI/Q.931). It is able to directly perform transport QoS negotiation throughout the transport facilities (e.g., DSLAM, CMTS, SGSN/GGSN).

  In the CPE-triggered QoS resource reservation mechanism, the CPE sends a 'QoS request' over a dedicated path-coupled QoS signalling to invoke the QoS resource reservation for a given flow. Based on the 'QoS request' from the CPE, the network border node is responsible for sending the RACF a resource decision request to pull the admission control decisions from the RACF.

Especially in multiple network domains, signalling among different service/network operators is additionally needed for exchanging QoS information.

There are two scenarios for passing the QoS information for a given service over an end-to-end path:

1) The QoS requirements for a given service can be passed over the end-to-end path through application layer signalling or through the Ri reference point.

2) The QoS requirements for a given service can be passed over the end-to-end path through path-coupled QoS signalling (e.g., RSVP-like).

Those inter-domain communications for end-to-end QoS control are based on [ITU-T Y.2111]. Appendix II describes two example scenarios.

8.8 Ethernet traffic grooming

To support the guaranteed QoS over the Ethernet, traffic grooming is required. When an access node (or an edge router) is connected to core MPLS/GMPLS nodes, it is required that the traffic grooming functionality is based on the MPLS/GMPLS traffic grooming technology for compatibility. Traffic grooming is the process of grouping Ethernet frames into virtual connections. For example, in the VPN reference model described in clause 7.3.1, PE creates groups of Ethernet frames that are transported via the same tunnel.

9 Operation, administration and maintenance for the Ethernet-based NGN

OAM functionality is important in delivering network performance and availability objectives as well as in minimizing operational costs. Offering a reliable Ethernet service that can support the requirements of a service level agreement (SLA) requires the Ethernet service to have its own OAM capabilities.

The requirements for Ethernet OAM are described in [ITU-T Y.1730] and the detailed OAM functions and mechanisms for Ethernet-based networks are defined in [ITU-T Y.1731].

10 Ethernet protection and restoration for the Ethernet-based NGN

Protection and restoration are also important to enhance network availability. As the Ethernet OAM is required, protection and restoration mechanisms at the Ethernet layer itself are also required to provide reliable Ethernet services based on SLAs. The Ethernet protection switching mechanism for the linear subnetwork connection is described in [ITU-T G.8031] and the protection switching for the ring connection is described in [ITU-T G.8032].

11 Security consideration

Security considerations are addressed in clause 7.3 (VPN configuration) and clause 7.5 (access control). Configuring VPN and activating the appropriate filtering capabilities require the relevant authentication procedures. A VPN solution has the mechanisms to activate the appropriate access control capabilities at customer request.

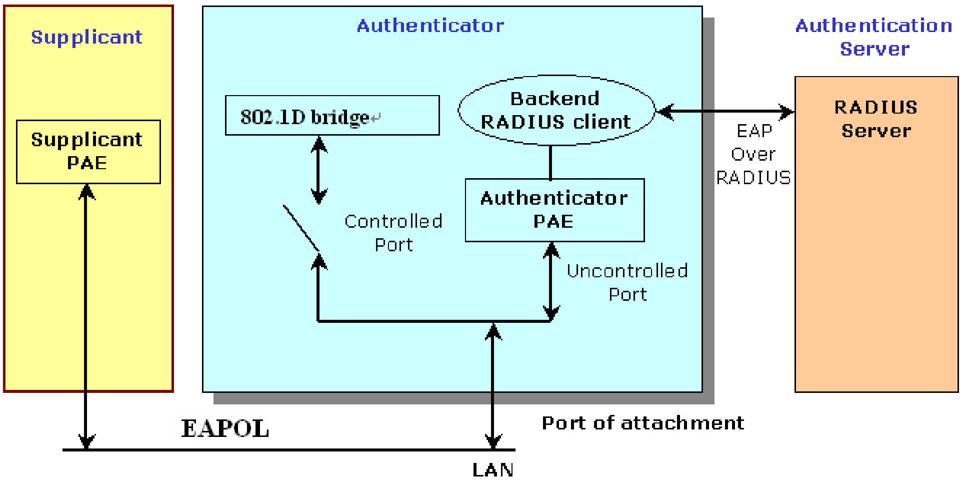
The detailed security requirements for VPN and access control are out of scope of this Recommendation.

Appendix I

Example of access control mechanism

(This appendix does not form an integral part of this Recommendation)

To access the network successfully, a supplicant takes the relevant authentication and authorization process by relying on authenticator and authentication server. Figure I.1 is an example to illustrate the relationship among the supplicant, authenticator and authentication server as well as the exchange of information among them.



Authenticator: An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.

Authentication server: An entity that provides an authentication service to an authenticator.

Network access port: A point of attachment of a system to a LAN.

Port access entity (PAE): The protocol entity associated with a port.

Supplicant: An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link.

System: A device that is attached to a LAN by one or more ports.

Figure I.1 – An example to illustrate authenticator, supplicant and authentication server roles

As shown in Figure I.1, the authenticator's controlled port is in an unauthorized state and is therefore disabled from the viewpoint of access to the services offered by the authenticator's system.

For the authentication protocol between the supplicant and the authentication server, EAP (extensible authentication protocol) [b-IETF RFC 2284] and [b-IETF RFC 3748] can be used. Over the LAN segment, EAP information is encapsulated in a LAN frame with the EAPoL (EAP over LAN) protocol, and delivered to the bridge. The authenticator acts as a RADIUS client for the authentication server.

– In the supplicant role, the port access entity (PAE) is responsible for responding to requests from an authenticator for information that will establish its credentials. The PAE performing the supplicant role in an authentication exchange is known as the supplicant PAE.

- In the authenticator role, the PAE is responsible for communication with the supplicant, and for submission of the information received from the supplicant to a suitable authentication server to enable the credentials to be checked and the consequent authorization state to be determined. The PAE performing the authenticator role in an authentication exchange is known as the authenticator PAE.
- The authentication server performs the authentication function necessary to check the credentials of the supplicant on behalf of the authenticator and indicates whether the supplicant is authorized to access the authenticator's services.

Appendix II

Example scenarios of resource reservation procedure

(This appendix does not form an integral part of this Recommendation)

This appendix provides examples of inter-domain communications for QoS control. Two means of passing the QoS information for a given service over an end-to-end path are illustrated: passing the information through the Ri reference point and passing the information through path-coupled QoS signalling. Figures II.1 and II.2 provide examples. The steps identified in the figures are described in the text below them.

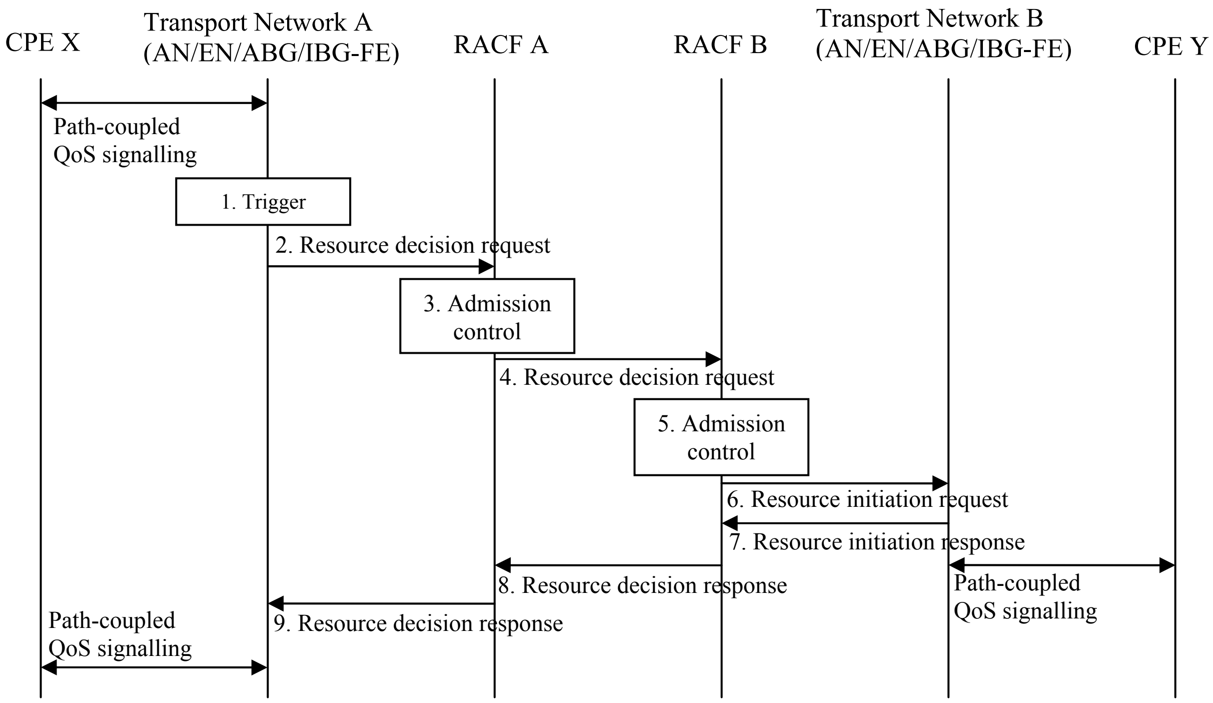


Figure II.1 – Example of inter-domain communications for QoS control through Ri reference point

Steps 1-3 in Figure II.1 correspond to the CPE-request QoS resource reservation procedure defined in [ITU-T Y.2111].

4) If it needs an additional admission decision from another RACF domain, an RDR (resource decision request) is triggered by RACF A, QoS requirements for the requested service are passed through Ri reference point.

5) On receipt of the RDR from RACF A, RACF B makes an admission decision. The decision procedures correspond to the SCF-requested QoS reservation procedure defined in [ITU-T Y.2111].

6) RACF B sends a RIR (resource initiation request) to install the final admission decisions in the transport network B. The RIR from RACF B requests the admission decisions to be enforced immediately (i.e., RIR (reservation + commitment)).

7) Transport network B installs (and enforces) the admission decisions sent from the RACF B and sends a RIP (resource initiation response) back to the RACF B. After sending RIP, a resource reservation indication message is transferred to CPE Y through path-coupled QoS signalling.

8-9) RACF B and RACF A send RDRs (resource decision response) back to the requester.

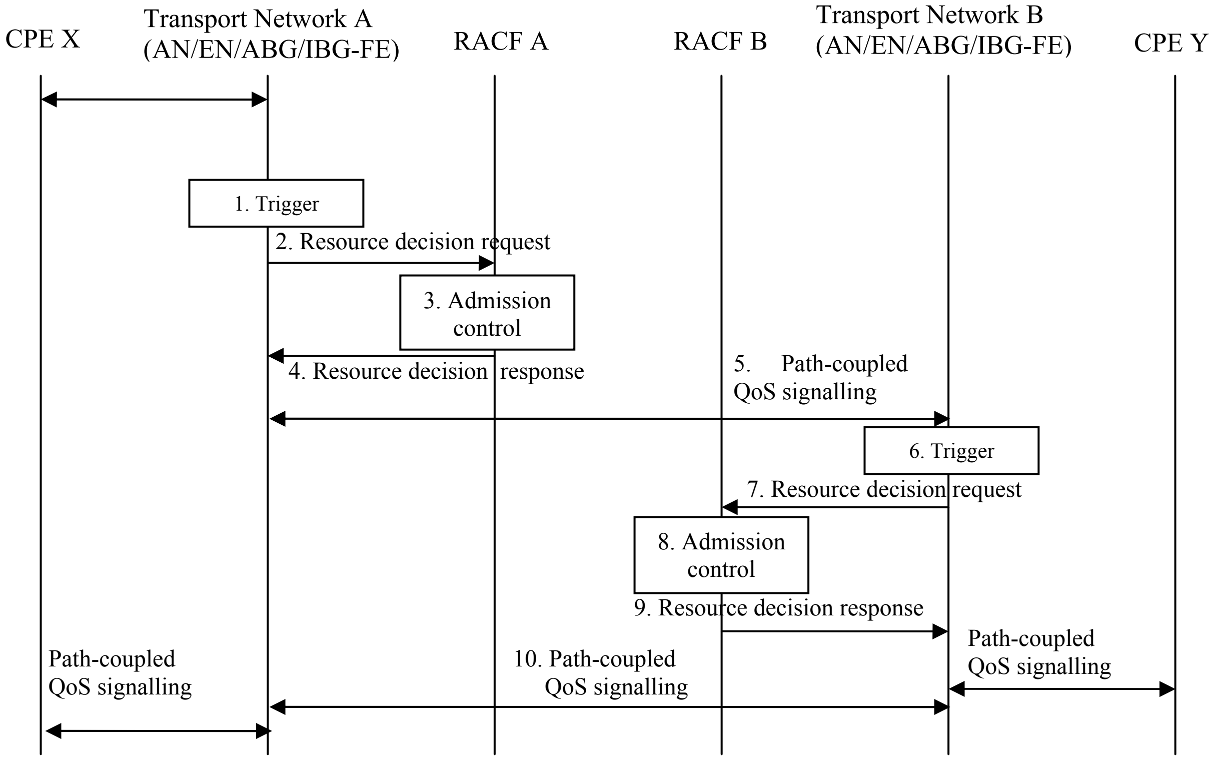

CPE X
Transport Network A (AN/EN/ABG/IBG-FE)
RACF A
RACF B
Transport Network B (AN/EN/ABG/IBG-FE)
CPE Y
1. Trigger
2. Resource decision request
3. Admission control
4. Resource decision response
5. Path-coupled QoS signalling
6. Trigger
7. Resource decision request
8. Admission control
9. Resource decision response
Path-coupled QoS signalling
10. Path-coupled QoS signalling
Path-coupled QoS signalling

Figure II.2 – Example of inter-domain communications for QoS control through path-coupled QoS signalling

Steps 1-4 in Figure II.2 correspond to the CPE-request QoS resource reservation procedure defined in [ITU-T Y.2111].

5) Transport network A and transport network B exchange QoS requirements through path-coupled QoS signalling. An RDR is triggered by a request indicated through the QoS signalling from transport network A. RACFs of each network domain work independently.

Steps 6-9 in Figure II.2 correspond to the CPE-request QoS resource reservation procedure defined in [ITU-T Y.2111] with the exception of the resource reservation indication message transferred to CPE Y through path-coupled QoS signalling.

10) Transport network A and transport network B exchange the result of resource reservation through path-coupled QoS signalling. This result of resource reservation is further transferred to CPE X through path-coupled QoS signalling.

Bibliography

[b-IETF RFC 2284] IETF RFC 2284 (1998), *PPP Extensible Authentication Protocol (EAP).*

[b-IETF RFC 2917] IETF RFC 2917 (2000), *A core MPLS IP VPN architecture.*

[b-IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture.*

[b-IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*

[b-IETF RFC 3353] IETF RFC 3353 (2002), *Overview of IP Multicast in a Multi-Protocol Label Switching (MPLS) environment.*

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP).*

[b-IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol.*

[b-IETF RFC 4664] IETF RFC 4664 (2006), *Framework for Layer 2 Virtual Private Networks (L2VPNs).*

[b-IETF RFC 4665] IETF RFC 4665 (2006), *Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks.*

[b-IETF RFC 4761] IETF RFC 4761 (2007), *Virtual Private LAN Service (VPLS) using BGP for Auto-Discovery and Signaling.*

[b-IETF RFC 4762] IETF RFC 4762 (2007), *Virtual Private LAN Service (VPLS) using Label Distribution Protocol (LDP) signaling.*

[b-IEEE 802.1ad] IEEE Standard 802.1ad (2005), IEEE Standard for Local and metropolitan area networks – *Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges.*

[b-IEEE 802.1ah] IEEE Standard 802.1ah (2008), IEEE Standard for Local and metropolitan area networks – *Virtual Bridged Local Area Networks – Amendment 6: Provider Backbone Bridges.*

[b-IEEE 802.1D] IEEE Standard 802.1D (1998), IEEE Standard for Local and metropolitan area networks – *Media Access Control (MAC) Bridges.*

[b-IEEE 802.1S] IEEE Standard 802.1S (2002), Amendment 3: IEEE Standard for Local and metropolitan area networks – *Multiple Spanning Trees.*

[b-IEEE 802.1X] IEEE Standard 802.1X (2001), IEEE Standard for Local and metropolitan area networks – *Port-based network access control.*

[b-IEEE 802.3] IEEE Standard 802.3 (2005), *Information technology – Local and metropolitan area networks – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.*

[b-MEF6] *Technical Specification MEF 6 (2004), Ethernet Services Definition Phase I.*

[b-MEF10.1] *Technical Specification MEF 10.1 (2006), Ethernet Services Attributes Phase 2.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	Telecommunication management, including TMN and network maintenance
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, open system communications and security
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, 2009