International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1292

(09/2008)

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

Internet protocol aspects – Architecture, access, network capabilities and resource management

Customizable IP networks (CIP): Framework for the requirements and capabilities related to the customization of IP service networks by customers

Recommendation ITU-T Y.1292

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.1292

Customizable IP networks (CIP): Framework for the requirements and capabilities related to the customization of IP service networks by customers

Summary

Recommendation ITU-T Y.1292 describes the framework for requirements and capabilities to enable the customization of IP networks and related IP service and IP transfer capability to meet the customer's needs. Such a framework includes the service requirements and functional requirements and capabilities as well as the architectural considerations.

In addition, this Recommendation identifies the application scenarios and service procedures applicable to the context of customization using the capabilities made available to and/or performed by the customer of IP services.

Source

Recommendation ITU-T Y.1292 was approved on 12 September 2008 by ITU-T Study Group 13 (2005-2008) 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

Introduction

Recommendation ITU-T Y.1292 describes the framework for requirements and capabilities to enable the customization of IP networks and related IP service and IP transfer capability to meet the customer's needs (see Recommendations ITU-T Y.1001 and ITU-T Y.1241).

The framework provided in this Recommendation includes an architectural model, high-level service requirements and functional capabilities. In addition, this Recommendation identifies the application scenarios and service procedures applicable to the context of customization using the capabilities made available to and/or performed by the customer of IP services.

In general, customization refers to the degree of manageability or controllability as exercised by the customer via a suitable agent. Such agent-based architecture is based on principles similar to those described in Recommendations ITU-T X.160 and ITU-T Y.130.

Recommendation ITU-T Y.1292

Customizable IP networks (CIP): Framework for the requirements and capabilities related to the customization of IP service networks by customers

1 Scope

This Recommendation covers the following:

- General overview and description of concepts related to the customization of IP services and related IP network aspects.
- General model of a customizable IP network from the end user's perspective.
- Definition of and requirements for the service capabilities offered to an end user for customization purposes.
- Functional capabilities that can be controlled by the end user of a customizable IP network.

In addition, Appendix I provides a description of application scenarios and service procedures used by the end user of a customizable IP network.

Note that the scope is restricted to IP networks when IP layer networks as defined in [ITU-T G.809] and operation within the NGN transport stratum as defined in [ITU-T Y.2011] are considered.

The detailed mechanisms for supporting the capabilities of a customizable IP network are not covered by the scope of this Recommendation.

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.809] Recommendation ITU-T G.809 (2003), *Functional architecture of connectionless layer networks*.
<http://www.itu.int/rec/T-REC-G.809>

[ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.
<http://www.itu.int/rec/T-REC-M.60>

[ITU-T M.3050.x] Recommendations ITU-T M.3050.x-series (2007), *Enhanced Telecom Operations Map (eTOM)*.
<http://www.itu.int/rec/T-REC-M>

[ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (2006), *Principles for the Management of Next Generation Networks*.
<http://www.itu.int/rec/T-REC-M.3060>

[ITU-T Y.1001] Recommendation ITU-T Y.1001 (2000), *IP framework – A framework for convergence of telecommunications network and IP network technologies*.
<http://www.itu.int/rec/T-REC-Y.1001>

[ITU-T Y.1241] Recommendation ITU-T Y.1241 (2001), *Support of IP-based services using IP transfer capabilities*.
<http://www.itu.int/rec/T-REC-Y.1241>

[ITU-T Y.1311] Recommendation ITU-T Y.1311 (2002), *Network-based VPNs – Generic architecture and service requirements*.
<http://www.itu.int/rec/T-REC-Y.1311>

[ITU-T Y.1711] Recommendation ITU-T Y.1711 (2004), *Operation & Maintenance mechanism for MPLS networks*.
<http://www.itu.int/rec/T-REC-Y.1711>

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.
<http://www.itu.int/rec/T-REC-Y.2011>

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 customer [ITU-T M.3050.x]: The customer buys products and services from the enterprise or receives free offers or services. A customer may be a person or a business.

3.1.2 IP service [ITU-T Y.1001]: A data transmission service in which the data that is transferred across the interface between the user and provider is in the form of IP (Internet protocol) packets (sometimes called datagrams).

NOTE – The IP (network) service includes the service provided using the IP transfer capability.

3.1.3 IP transfer capability [ITU-T Y.1241]: IP transfer capability is defined as the set of network capabilities provided by the IP layer. It may be characterized by the traffic contract as well as the performance attributes supported by the control and management functions of the underlying protocol layers.

3.1.4 service level agreement [ITU-T Y.1241]: Service level agreement (SLA) is a negotiated agreement between a customer and the service provider regarding the levels of service characteristics and associated set of metrics. The content of an SLA varies depending on the service offering and includes the attributes required for the negotiated agreement.

3.1.5 end user (user) [ITU-T M.3050.x]: The end user is the actual user of the products or services offered by the enterprise. The end user consumes the product or service.

NOTE – Typically, the (end) user is a person or a machine delegated by a customer to use the services and/or facilities of a telecommunication network.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 customize: This involves ensuring the suitability to the individual requirements of a customer.

3.2.2 customizable: This refers to the capability of being customized.

3.2.3 customizable IP network (CIP): This is an IP network that is capable of being customized in accordance with and by the capabilities specified within this Recommendation.

3.2.4 customization: This refers to the result of being customized.

3.2.5 manageable: This refers to the capability of being managed.

3.2.6 manageability: This pertains to the characteristic of being manageable.

3.2.7 CIP provider: The provider using a customizable IP network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA Authentication, Authorization and Accounting
CBR Constant Bit Rate
CDR Charging Data Record
CIP Customizable Internet Protocol network
CIPA Customizable Internet Protocol network Agent
CoS Class of Service
CPE Customer Premises Equipment
C-Plane Control Plane
DIB Directory Information Base
DNS Domain Name Service
eTOM Enhanced Telecom Operations Map
FTP File Transfer Protocol
HTTP HyperText Transfer Protocol
IP Internet Protocol
M-Plane Management Plane
MPLS Multi-Protocol Label Switching
P2P Point-to-Point
P2MP Point-to-Multipoint
PABX Private Automatic Branch Exchange
PDA Personal Digital Assistant
PKI Public Key Infrastructure
QoS Quality of Service
QUA Quality of Service User Agent
RFID Radio Frequency Identifier
RGW Residential Gateway
SIP Session Initiation Protocol
SLA Service Level Agreement
SLS Service Level Specification
SOAP Simple Object Access Protocol
UNI User-to-Network Interface
U-Plane User Plane
UPC Usage Parameter Control

URI Uniform Resource Identifier

URL Uniform Resource Locator

VBR Variable Bit Rate

VNF Virtual Networking Function

VPN Virtual Private Network

VTR Video Tape Recorder

XML eXtensible Markup Language

5 Conventions

In this Recommendation, words such as manage and control (and derivatives thereof) are used in the general English dictionary sense rather than in the specific sense of the M-series or Q-series Recommendations. When specific usage in the sense of the M-series or Q-series Recommendations is required, specific indications are made.

6 Overview

6.1 Service aspects

The main objective of a CIP network is to provide customers with the ability to manage and control certain aspects of the IP service they have subscribed to and the related IP network technology facilitating the IP service.

A certain degree of autonomy on the part of the customer and/or individual end user (within the customer organization) is desirable. For example, a customer will find it advantageous to be able to:

– Select the set of end users, which may be human, terminal equipment or applications permitted to use the IP service within the given customer organization.

– Create and customize services and network configurations (e.g., virtual private networks (VPNs)) with the relevant network resources provided by the customizable IP (CIP) provider to the customer.

– Select, control and/or manage various features of the services. For example, the customer can negotiate the service level agreements (SLAs) offered by the CIP provider related to QoS and network performance objectives, as well as the security requirements and capabilities.

In general, various degrees or levels of customization capabilities can be offered to the customer depending on the level of sophistication of the available customization capabilities.

NOTE 1 – When the customer is an organization, several end users of this organization can be connected to the CIP network. In particular, several end users can be connected to the CIP network using the same UNI (user-to-network interface) as defined and provided by the CIP provider, i.e., at the interface deemed to demarcate the end of the CIP provider's jurisdiction and the beginning of the end user's jurisdiction, and within the scope of the customer in question.

NOTE 2 – This Recommendation follows the general principles established in [ITU-T Y.1311], as applicable, although the scope is not restricted to VPN situations.

6.2 General customization model

Figure 1 illustrates the customization model applicable to a CIP network.

Acting on behalf of its own organization and/or on behalf of the end users within the customer organization, the customer interacts with the CIP provider to achieve the desired customizations. The customer interacts with the CIP provider through the CIP agent.

The customer may also delegate some customization responsibilities to its end users within the bounds of the privilege allocated to such end users. This is indicated by the broken arrows.

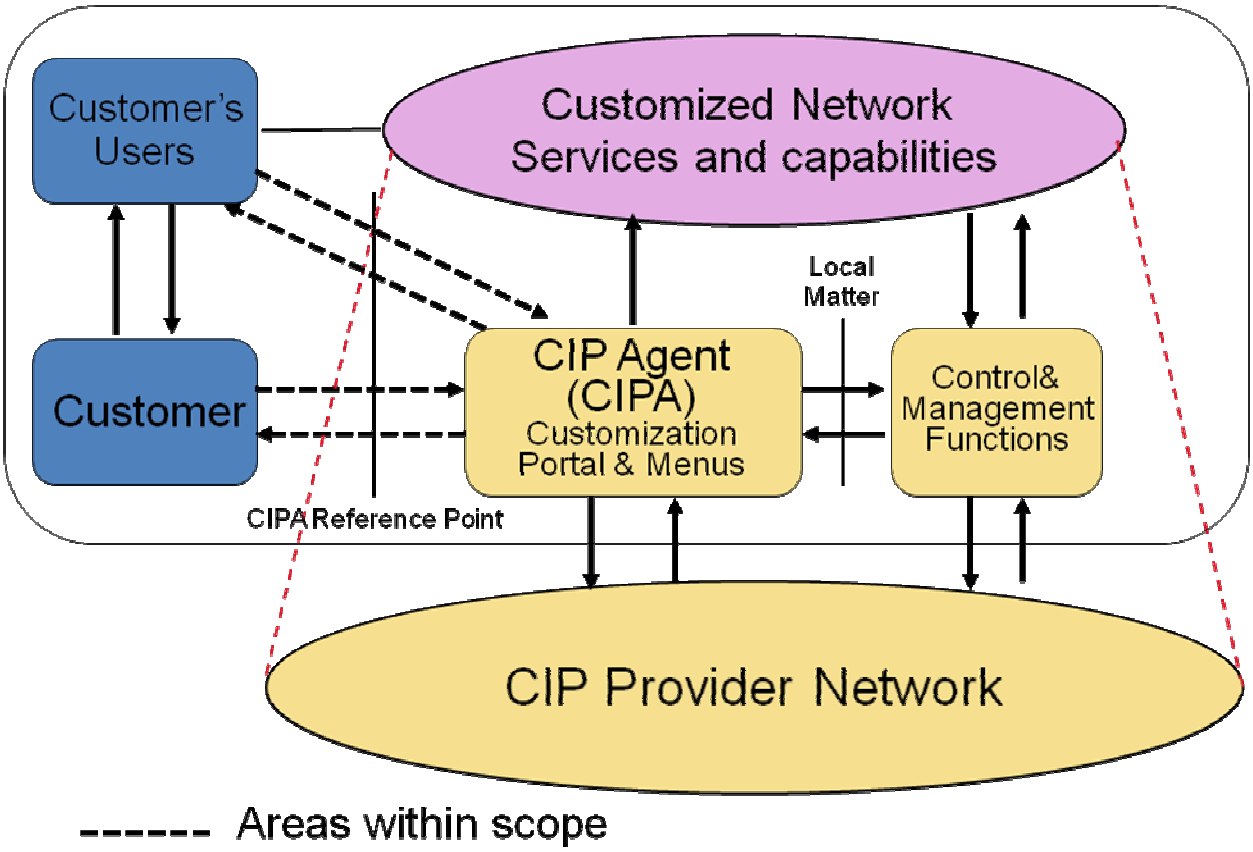


Figure 1 – General customization model

The agent concept shown in Figure 1 is similar to the principles described in [b-ITU-T X.160] and [b-ITU-T Y.130].

The control and management functions used by the CIP agent may consist of a number of appropriate systems, such as the following:

– Systems based on the NGN management principles specified in [ITU-T M.3060].

– Systems based on the eTOM business framework specified in [ITU-T M.3050.x].

The linkage between the CIP agent and such systems is out of scope of this Recommendation and may be subject to local considerations as described in [b-ITU-T X.160].

6.3 Service level agreements (SLAs)

The CIP provider supplies its customers (and related end users) with IP network connectivity services based on the negotiated SLAs [ITU-T Y.1241]. An SLA specifies the customer/end user requirements that the CIP provider is committed to.

An SLA defines the level of the quality of services to be provided, setting performance objectives to be achieved by the CIP provider. It also defines the procedures and reports that must be provided to track and ensure compliance with the negotiated SLA.

For given types of applications requiring more than best-effort types of SLA, the customer (and related end users) can optionally negotiate SLAs with performance requirements such as bandwidth, delay and loss performance.

An SLA can ensure the performance and availability of the CIP network to the customer and its end users. Reliability and availability are the key objectives that the CIP provider may have to fulfil in order to support a negotiated SLA. The capabilities defined in a given negotiated SLA may be activated on demand (as a result of an end user's request) or provided at the subscription time. Depending on the SLA negotiated with the customer, the CIP provider may have to control and manage the corresponding resources in the underlying CIP network.

6.4 Menu-based network customization capabilities

6.4.1 Introduction

The capabilities provided by the CIP provider allow the customers (and even end users within the customer organization) to have different levels of control and management over the relevant network resources of the customizable network. Customer and end-user access to network capabilities are provided by a set of menus (e.g., available via a web portal). Depending on the service contract, such menus can allow the further specification of SLA parameters.

Network capabilities can be negotiated through a menu system that can exhibit individual CIP features related to the network itself and/or services, as well as their combinations. Network features can include storage resources, bandwidth and processing time. Service resources include relevant resources required for the support of distance learning, telecommuting, electronic commerce, telemedicine and online entertainment. Other features, such as controlling/managing a group of end users forming a VPN, are accessible. In addition, some features can relate to associated supported technologies and service architectures such as resources related to databases, secure networks, the Internet or Java.

The detailed mechanisms for the support of customization and related management and/or control mechanisms are out of the scope of this Recommendation.

6.4.2 Levels of resource manageability

One feature of customization is the ability to select the degree of resource manageability required. Table 1 introduces the concept of resource manageability levels. Note that the levels described in Table 1 are only examples of resource manageability levels that can be offered by a CIP provider.

Table 1 – Levels of resource manageability

Level	Description	Features	Remarks
0	No manageability	No monitoring, no resource control	• No mechanism to detect network faults and congestion • No mechanism to control network resources
1	Overall network resource manageability	Overall monitoring, no resource control	• Notify the overall network fault and resource status by CIP provider • No resource control by the customer
2	Group-level resource manageability	Group-level resource monitoring and control	• Notify the group-level network fault and resource status by CIP provider • Customer managing the group-level resources
3	Individual resource manageability	Individual-level resource monitoring and control	• Notify the individual network fault and resource status for end-to-end connectivity • End user managing the end-to-end resources

Manageability level 2 ("group-level resource manageability") corresponds to the case where network resources are to be manageable on the basis of end-user groups. A typical case is VPN where the corresponding network resources are shared between end users.

A given network resource is considered as a single entity of manageability which can be dedicated to an individual end user (level 3) or shared between a group of end users (level 2).

NOTE – The resource parameters and their corresponding granularity are implementation-specific and are therefore out of the scope of this Recommendation.

6.5 Customer expectations

Customization capabilities are provided by the CIP provider to assist the customer in fulfilling its service expectations.

The customer may wish to negotiate performance parameters to ensure corresponding performance objectives such as the following:

– Availability (e.g., 99.999%).

– Response time (e.g., less than 5 ms to download a 1 Megabyte file).

– Service-blocking probability, including network access blocking.

– Service priority and QoS/CoS parameters.

6.6 Network capability requirements

The degree of customization and manageability offered to the customer depends on capabilities, called network capabilities, supported and provided by the CIP provider. This clause identifies network capabilities that can be used in the context of this Recommendation.

6.6.1 General network capabilities

The capabilities to be provided by the CIP network provider include support for the following:

– Creating/updating/deleting end-user profiles, including the end-user name, number, services subscribed to, etc.

– Advertisement/solicitation of name, address and number.

– Allocation of network addresses and address filtering.

– Authorization/authentication to identify the end user (e.g., query for end-user identifier, password, certification).

– Troubleshooting of network access problems.

– End-to-end transparency between end users.

– Name/number/service portability, navigation, name notification and name database management.

– Accounting of the end user's service utilizations for billing.

6.6.2 Network capabilities related to performance parameters

Network capabilities can optionally include support for the customer to dimension, manage, control and monitor network performance parameters. The following are examples of parameters that can be considered relevant in this context:

– Packet error rate, packet loss rate.

– Round trip delay, one-way delay and delay variance.

– Availability (e.g., system uptime, mean time to failure, mean time to repair).

– Peak bandwidth, available bandwidth and minimum bandwidth.

– Round trip delay of location identification for mobility.

– Access blocking probability and service completion probability.

– Traffic-related statistics (e.g., number of packets to be received or transmitted, number of packets discarded or received in error).

6.6.3 VPN-related network capabilities

CIP provider capabilities include support for the capabilities outlined in [ITU-T Y.1311], such as the following:

– Means to enable the customer to define VPN membership.

– Accommodation of customer-defined VPN address schemes.

– Means for a single customer site to belong concurrently to more than one VPN.

– Means for the customer to define VPN topologies (ranging from hub-and-spoke, partial mesh to full mesh, for example).

– Support for fixed and mobile end users.

– Support for a wide range of routing protocols between the customer's premises routers and CIP provider's edge routers.

– Means for supporting a variety of an end user's traffic (QoS) requirements as defined by the end user.

– Means for supporting different modes of communication such as any-to-any (1:1), multicast (1:N, M:N) and broadcast (1:All).

– Means to enable the customer to easily add, remove or change devices, sites, routes, traffic, etc.

– Means to enable the customer to define SLAs per VPN and/or per VPN site and/or per VPN route.

7 Functional capabilities

7.1 Overview

This clause provides a description of functional capabilities that can be considered to support the network capability requirements identified in clause 6.6. The functional capabilities are described according to end user perspectives and CIP provider perspectives. The functional capabilities provided by the CIP provider allow the customer (and end users within the customer organization) to customize its own IP network.

7.2 Naming, addressing and identification capabilities

An end user can be identified by his/her name, address and/or number. The physical attachment point, such as corresponding to a MAC address, can also be used to identify the end user. Binding mechanisms among the name, address, number and physical attachment point are required to identify the end user. If an end user moves, connectivity should be maintained. This implies handling the binding between the end-user permanent IP address (as home address) and end-user temporary IP address (as care-of-address). The temporary care-of-address identifies the IP address of the visited location while the permanent IP address identifies the end user.

If end users announce their names to the CIP provider, the CIP provider identifies their names with address and location information allowing them to be reachable via their names. The domain name service (DNS) functions should allow some form of end user-identification. Real-time address translation and dynamic mapping between address and domain name server are required to support mobility. The following requirements for naming and addressing are necessary to support customizable IP services:

• End user is identified by name, address and/or number.

• Dynamic update and automatic configuration of the name service database are executed at the request of the customer.

- Translations between private naming/addressing and global naming/addressing for end-to-end connectivity may be required while end users use their own private naming/addressing dedicated at a specific region or group. When the end user moves to another location, the corresponding registration servers are notified of the new end user's location.

7.3 End-user grouping capability

End-user grouping is mainly used for multicast and VPN services. The CIP provider is required to support proper registration and membership distribution mechanisms in order to provide end-user grouping capability. The grouping capability is recommended to allow for the identification of end-user groups. End users may actively select, join or leave a given end-user group.

7.4 Application clustering capability

Clustering is a common term for providing a service over multiple servers to increase fault tolerance and/or to support load sharing. Clustering can be used for large-scale and mission-critical applications that do not allow any downtime. Each server within the cluster aims at maintaining the same information and performs administrative tasks such as load-balancing, server failure determination and failover duty assignment. The end user can trigger application clustering by allocating multiple servers (e.g., computers) into a corresponding dedicated cluster.

7.5 Information navigation and query capabilities

In the customizable IP network, various types of multimedia information may be associated with information content to allow fast and efficient navigation for end users. Multimedia information and applications available in the network are recommended to be accessed at a minimum by username and password.

The database containing the multimedia information may be searched and sorted with the relevant directory structure.

For information navigation and query capabilities, a set of descriptors describing various types of multimedia information and identifying its contents is used. The description of "information data" provides the means to deliver audiovisual data as objects with certain relations in time and space.

To aid in information acquisition, short descriptions for raw information contents are essential. In principle, any type of information data may be retrieved by means of any type of data query. A search engine may be necessary to match the data query and information description. To help information acquisition, information processing and a storage platform may also be required (e.g., servers for messaging, retrieval and distribution).

End users can activate the information navigation and query capabilities under the following cases:

- Changing information contents and types of data.
- Searching recursively to get detailed information.
- Maintaining the history of information navigation and queries, etc.

7.6 Auto-discovery and auto-configuration capabilities

Auto-discovery and auto-configuration capabilities are technologies that enable the CIP network to be customized quickly to the environments that they should manage. Deploying new services at a rapid pace necessitates implementing the discovery methodologies in an extensible manner such that newly discovered capabilities can be added step-by-step to the IP network. End users are able to configure their own network environments (e.g., VPN) by utilizing auto-discovery and auto-configuration.

The CIP network is recommended to support the auto-discovery capability that, in particular, dynamically conveys the location information of the end user, consistent with and respecting privacy requirements. Auto-discovery capability can be useful for achieving service scalability. The following are its advantages:

- Reduces downtime by eliminating the process of identifying the IP address and manually adding it in the backup unit.
- Enhances safety by removing erroneous IP configurations.
- Increases security by monitoring devices on the network.
- Diminishes the complexity when modifying firmware and/or hardware equipment configuration.

7.7 Information access control and security capabilities

End users may sometimes require the use of network paths with an appropriate level of security. Securing data traffic requires constructing a secure channel to end user's home (residential) networks. Access control and cryptographic functions are to be supported during registration and activation. IP-based VPN services can be used for providing security with an appropriate policy. The set of administrative policies determines both connectivity and QoS for VPN customers. End users can activate and deactivate access control with security associations.

The packet filtering capability can provide reasonable protection and access control at the user-to-network interface; it can be applied to various gateway routers or intermediate network equipment between end users and the network. The packet filtering and security functions can be combined with specific protocols such as SIP, ITU-T H.323, FTP, etc.

7.8 End-to-end transparency capability

One of the critical requirements is the support for seamless handover. End-to-end transparency is recommended to be maintained during handover since applications should run independently of the supporting infrastructure. The CIP provider's network is recommended to support the following three types of end-to-end transparency:

- Location transparency

  With distributed computing technology, end users can gain access from anywhere regardless of the actual physical location of such servers.
- Network transparency

  The application server executes the corresponding control process independently of specific network types and end-user terminals.
- Protocol transparency

  Protocol transparency is achieved by providing a standardized user-to-network interface, realizing independent service control processes, shielding complex network technical details from the service provision platform, and developing open communication network interfaces.

The three types of transparency may be chosen by the end user. If the end user requires end-to-end transparency, the CIP provider is recommended to check whether such end-to-end transparency can be supported. The CIP provider may have to restrict other functions, such as NAT or disguised traffic, that can disrupt the transparencies. In this case, there is a need to verify which functions disrupt location, network and protocol transparencies.

7.9 Connection configuration capability

The connection configuration capability allows the specification as to who is allowed to communicate with whom (e.g., end user, information service broker, information broker). There are three basic connection configurations: point-to-point, multicast and broadcast.

Point-to-point connections may provide unidirectional and bidirectional, as well as symmetric and asymmetric, paths. For point-to-point connections, the CIP network can support the following features:

- Establishment, modification or release at the request of two participating end users
- Establishment with unicast addressing/naming capability.

A broadcast connection may provide unidirectional communication between one end user and other end users. This connection is one-to-many (all) during a particular initiated session. A multicast connection is the one-to-many relationship continued for the duration of a given initiated session. In this connection, one end user is the root, and the other end users are leaves. The root can send one copy of each packet and address it to the group of leaves wishing to receive it. End users can establish their own network configuration depending on their private resources and service/applications. End users may try to optimize their private communication configuration considering the communication cost and performance.

7.10 Routing and forwarding control capabilities

Proper routing paths between the source and the destination are decided according to the traffic contract and overall network traffic condition. The routing paths between the source and the destination are selected by end users, e.g., best effort, VPNs, managed IP facilities. Based on the end users identified routing selection, future routings can occur based on a definite routing policy. For connectionless transfer, the router forwards the IP packets with their respective QoS information and end user requirements along a selected routing link.

The routing algorithm can be classified according to routing decision processes that are generally applied to end-to-end or hop-by-hop connections. For network scalability and robustness, some combinations of routing decision processes may be used for specific connections or flows. The following are the routing requirements in customizable networks:

- Capability to support QoS-enabled paths

  QoS-enabled paths are needed to support the end user's specific requirements (mobility, VPN, security, policy, QoS level, etc.).
- Capability to provide alternative paths

  To cope with failure of a routing path, alternative routing paths should be provided.
- Capability to exchange routing information for interconnecting situations

  Negotiate and select the QoS parameters to support end-to-end QoS requirements.
- Capability to support scalable routing

  A trade-off between the amounts of routing database information required in the CIP network elements and the size of the CIP network.
- Capability to support broadcast routing

  The CIP network is able to copy packets, thereby allowing sources to send packets to all receivers.
- Capability to support multicast routing

  The CIP network is able to build packet distribution trees that allow sources to send packets to all receivers bound to the multicast spanning tree. The multicast tree is built according to network policies.

7.11 Alternative path selection and multi-homing capabilities

To deliver reliable service, the end user may require a set of procedures to provide protection for the traffic carried on different paths and to support the selection of his/her physical/logical interface. To support such requirements, alternative path selection and multi-homing capabilities are essential.

The alternative path selection capability guarantees seamless service by avoiding service deterioration in case of network faults. For the selection of the backup path, the CIP network maintains route information along the same original path and proceeds to set up the alternative path. The following are requirements for supporting alternative path selection capability (end users can select alternative path and multi-homing capabilities based on their preferences):

- Alternative path discovery

  Depending upon the prior agreements made between the end user and the carrier, when a network fault occurs, end-user traffic may be automatically routed to an alternative path.
- Multi-homing

  Providing multi-homing capability has some advantages, one of which is redundancy. This is similar to the alternative path effect. Entities such as end users, hosts, routers and subnets should be able to be insulated from certain failure modes within one or more network providers. A network with this capability is recommended to accommodate continuities in connectivity during failures. Another advantage is better performance. Through multi-homing, a network entity should be able to protect itself from performance deterioration. Multi-homing provides multiple interfaces on the end-to-end path.

7.12 Mobility control and management capabilities

While most end users are moving, their connectivity should be controllable at any time. Efficient mobility control and management procedures are recommended to be developed in combination with security procedures. Mobile end users and terminals should be able to update their location database dynamically. This way, a mobile host is able to maintain and use the same IP address as it changes its point of attachment to the CIP network. The relevant registration protocol is used to authenticate the mobile IP end users. The location resolution and seamless handover procedures are enforced while IP end users or terminals are in motion. Supporting mobility control and management requires the following capabilities (end users can choose some capabilities during handover):

- Capability to allow a mobile node to be reachable by having a permanent address:
  - Address management function.
  - Registration function.
- Capability to know where a mobile node is:
  - Network information advertising/detecting function.
  - Registration function.
  - Paging function.
- Seamless handover capability.
- Capability to allocate proper resources during handover.
- Capability to support inter-domain mobility.
- Capability to find the optimal routing path.
- Capability to support AAA and security.

7.13 Traffic measurement and usage parameter control capabilities

Usage parameter control (UPC) refers to the set of actions taken by the CIP network to monitor and control traffic. The operation of UPC involves checking whether or not input traffic conforms to the QoS objectives of a compliant connection. Note, however, that excessive policing actions on a connection may have side effects on the overall network performance deterioration. Therefore, safety margins should be engineered to limit the effect of UPC. Conforming traffic refers to the contracted performance guarantee. Traffic exceeding the conformance limit will receive appropriate treatment. The forwarding process can further be associated with service priority and service reliability parameters.

The flow control of UPC guarantees that sources act as agreed upon during the call setup phase, after a call is accepted and a decision is made to penalize or not to penalize the traffic or connection when such arrival triggers a traffic overflow or violation. Actions (e.g., tagging or discarding) are taken if a source does not conform to its contract. Violation of the contract may occur in case of malfunctioning equipment, malicious end users or traffic delay.

The customizable network should directly support traffic measurement and usage parameter control functions. End users may request permission to observe the results of traffic measurements and UPC functions when they experience performance deterioration. Likewise, end users can negotiate the UPC parameters with the CIP provider. The end user can control the QoS level based on these UPC parameters.

7.14 SLA negotiation capabilities

The customizable network should be reliable and seamless to satisfy the negotiated SLAs. End users may also choose their service profiles and performance characteristics. The CIP provider is required to negotiate and agree with the end user on the technical details of specific instances of the service products being offered. The QoS parameters may be the same as those offered or customized to a specific service instance. There are always two SLAs, one for each direction. The SLA specification requires extensive monitoring of the available infrastructure.

The end user can dynamically negotiate SLAs with the CIP provider and change the SLAs to the maximum extent supported by the CIP provider.

7.15 End-to-end QoS provision and priority assignment capabilities

To enable the applications to work to the satisfaction of end users, performance guarantees are required for the resources they use. In particular, end-to-end QoS provision is necessary for many applications, e.g., upper bound for packet loss and maximum transmission delay in real-time audio streaming applications.

The end user can optionally select end-to-end QoS. In this case, the CIP provider is recommended to guarantee end-to-end QoS as a contract with an end user.

7.16 Information storage and directory processing capabilities

Directories play an important role in providing information access across networks. Directories are involved in many operations requiring access to information such as end user preferences, patient information, student records and public records.

From the CIP provider's perspective, the capability to manage both end-user profiles (e.g., phone number, address and subscribed service lists) and network/service profiles (e.g., network configuration, topology and server lists) is required. If the CIP provider grants an end user the capability to manage his/her profile, the end user can manage personal information such as password, friends' address lists, etc.

The CIP provider may provide information storage services for clients. Grid networks are an application environment that can provide these services in a secure, flexible and dynamic manner [b-Foster].

End users may enlist the help of the CIP provider to configure their own storage and directory environments.

7.17 Segment OAM and end-to-end OAM capabilities

The network requirements for both segment and end-to-end OAM capability have increasingly become pivotal in maintaining SLA contracts. To construct segment and end-to-end OAM flows from the perspective of an end system, MPLS OAM and MPLS ping/trace may be applicable [ITU-T Y.1711].

The end user can activate the OAM flows regardless of whether or not the SLA contracts are satisfied.

7.18 Virtual private network configuration capability

For customizable IP networks, policy-based control functions for providing VPN configuration individually and dynamically are necessary. VPN can be decomposed in multiple sub-VPNs, e.g., dedicated for voice, for on-demand streaming data, secure information, etc.

To provide service-dependent routing/forwarding features for VPNs, the CIP network supports virtual networking.

End users can configure their own virtual private network. Providing intelligent and dynamic VPN configurations require the following functions in the customizable network:

- For dynamic reconfiguration in a VPN node, intelligent features will be required to select tunnel(s) for each end-system that should be connected to VPN.
- Firewall policies can be chosen to ensure a high degree of security that controls incoming/outgoing unauthorized packets.
- For QoS-capable VPNs, providing tailored communication services that can be differentiated in terms of performance, monitoring, accounting, security and privacy is important. For example, the ingress node in the CIP network can perform aggregate flow scheduling based on multiple individual flows within VPN.
- Hierarchical mobility management (e.g., micro/macro mobility) may be necessary for mobility provision among VPN groups.
- The ingress nodes of a VPN provide dynamic configuration filtering rules, with levels of granularity ranging from a single node to an entire VPN.

7.19 Billing and charging capabilities

The billing and charging capabilities are based on the collecting of charging parameters. The charging parameters can be agreed by customers/end users during the SLA negotiation. The following parameters may be considered:

- Connection mode.
- Connection establishment and release time.
- QoS class and priority.
- Traffic parameters including constant bit rate (CBR) and variable bit rate (VBR).
- Charging data records (CDRs) which include the number of packets to be delivered, tagged and discarded.

7.20 Client/server management and agent management capabilities

Client/server management is required to support the scalable and efficient deployment of services. The following features can be supported in the customizable network:

- Service portal acting as a broker for services with the ability to manage complex service relationships.
- Separation of service control from service transport, thereby allowing the control of multiple and heterogeneous networks using a common control plane and providing a path to simpler network devices.
- Support for multiple network technologies achieved by abstracting the service QoS requirements from the underlying technology.
- Scalable and flexible architecture enabling plug and play (e.g., dynamic registration of new services through agent collaboration).
- End user mobility enhancement, i.e., end users can access the system from multiple customer premises equipment (CPEs) as CPE agents collaborate with the service portal agent to provide the location information of the end user.
- Distributed software entities (agents) that can cooperate in support of the trading model for the service supply chain.

The CIP network allows end users to get client/agent/server management upon the demand of the end user. The following end users of the CIP network can be considered: service providers and service clients (clients of the service providers). If a service provider requires agent management for its clients, the CIP network supports the agents of the service provider. These agents are located at appropriate places over the CIP network, acting as service providers to clients. If the service client requires agent management, the CIP network provides a client to perform tasks as an agent. This agent plays two roles: as a server of a service end user and a client of a service provider. Once their specific tasks are executed, clients will release the agent resources of the CIP network.

8 Security considerations

To ensure the secure use of a customizable IP network, the following items need to be considered:

- Authentication: This is required to verify the claimed identity.
- Authorization: This enables certain actions after the authentication. In particular, authorization ensures that only authorized persons or devices are allowed to access the CIP network elements, services and applications.
- Confidentiality: Data should not be made available to unauthorized entities.
- Integrity: This ensures that data is not modified in transition.
- Non-repudiation: Non-repudiation requirements provide undeniable proof of shipment and/or receipt of data to prevent the sender from disavowing a legitimate message or the recipient from denying receipt.
- Communication security: This function ensures that information flows only between authorized end points.
- Availability: This function ensures that there is no denial of authorized access to the CIP network elements, services, applications, etc.
- Privacy: This function ensures the right of individuals to control or influence what information related to them may be collected and stored, and by whom, and to whom that information may be disclosed.

In terms of mobility, there are inherent security risks. To be able to use the customizable IP network while avoiding the security risks associated with mobility requires identifying specific threats. The following lists the weak points and potential solutions related to mobility:

- Using binding updates: The binding update in mobile IP solutions may be used to redirect routing of information from legitimate sources to destinations without the permission and knowledge of the sender. If not used carefully, it can cause some detrimental results in the case of mobile communications.
  - Stealing data: If a rogue end user knows a mobile node's permanent address, he/she can send a binding update to a correspondent node or a database maintaining the binding update to change the route for the original mobile node's data into his/hers.
  - Reflection and flooding attacks: When a sender and a destination are communicating that the sender sends a packet to the destination is perfectly acceptable; this usually results in the destination replying back to the sender. If the sender sends to the destination a packet that causes the destination to reply to another person, however, a reflection attack is said to occur. The attacker can flood another person's link using the reflection attack.
  - Man-in-the-middle attacks are attacks on the binding update: This attack can be used on the communication path between two nodes by an attacker. An obvious method is to change the contents of a packet to cause some results that were not intended by the original sender of the packet. When the attacker is located on the path between a mobile node and a correspondent node, he/she can modify the content of the binding update, thereby possibly bringing about a reflection attack or hijacking an ongoing connection between mobile and correspondent nodes.
- Attacks using packet header information: The packet includes destination information. Therefore, if an attacker is communicating with a mobile node, he/she may put another address in the header information field, thus causing the mobile node to forward the packets to another node and possibly causing reflection or flooding attack.

As additional requirements on security, the following points for enhancing security are introduced as follows:

- Securing communication between the mobile node and the correspondent node: Messages between a mobile node and a correspondent node are required for binding cache and binding update list management, especially in mobility management. The binding update acts as a redirection request. Therefore, a correspondent node should trust the mobile node to be able to accept this request.
  - Message integrity: An attacker should not be able to modify the contents of the binding update message as well as the binding acknowledgment message.
  - Avoiding the denial of service attack: To avoid this attack, correspondent nodes must ensure that they do not maintain the active attachment state per mobile node until the binding update is accepted.
- Securing messages in the database for the binding update: The same attacks on the binding update to correspondent nodes are relevant when a mobile node is communicating with its binding update database. Database impersonation could be detrimental to the mobile and correspondent nodes. As such, the mobile node's communication should be secured using authentication.

Appendix I

Service procedures and applications scenarios

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

This appendix describes some of the service procedures for customizable IP services and applications. The application scenarios for the described customizable IP services are as follows:

- Customizable personal directory services.
- Customizable access control services.
- Customizable end-to-end QoS services.
- End-user customizable location monitoring services.
- Customizable home networking services.
- Client networking services with QoS and security.

I.1 Customizable personal directory services

A customizable personal directory service is a service intended to provide end users with access to various personal directory-related information. Directory databases are repositories for information on network-based entities, e.g., applications, files, printers and people. In customer-managed IP network environments, the end user has his/her customized directory database in the network; even if the end user moves to a different location, he/she can access the directory anytime. Using query procedures with the directory service, the end user can also get some directory information of other end users such as an end user's telephone number as well as some location information.

I.1.1 Objectives of customizable personal directory services

One of the main objectives of supporting personal directory services in customizable networks is to have a customized personal directory for the management of end-user data. For each end user, a personal set of data is stored in the CIP network. Such end-user profiles should be accessible from every location in the network around which the end user can move. Another objective is to enable CIP providers to build specialized directory services into their applications.

I.1.2 Functional model for customizable personal directory services

Figure I.1 shows the functional model for the customizable personal directory services. This model includes agents and managers as well as a logical database to support directory services as follows:

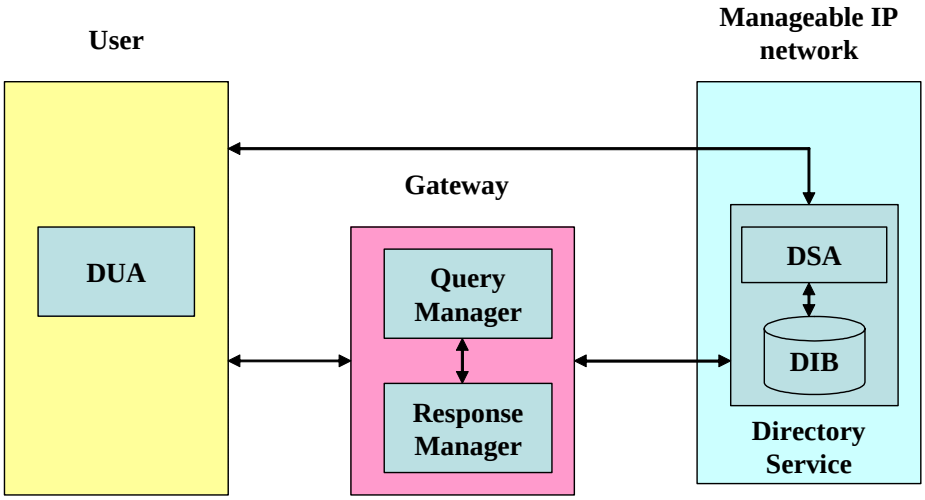
- Directory user agent (DUA) and directory service agent (DSA)

  The directory service is described as a distributed client server system. This is characterized by a number of hosts (servers, DSA) providing directory services to other hosts (end users, DUA).
- Directory information base (DIB)

  As a single, logical, global directory database, DIB stores information on directory objects such as end-user profile, location data, etc.
- Query manager and response manager

  The query manager and response manager are responsible for processing the query and response messages between DUA and DSA.

The end user can directly access his/her own directory service to update and manage directory information for customized directory services.



Note) DUA: Directory User Agent, DSA: Directory System Agent
DIB: Directory Information Base - user profile, location data etc

Figure I.1 – Functional model for customizable personal directory services

Personal directory services offer the following functionalities:

- Creation and deletion of end-user information in a distributed database maintained in the network.
- Downloading and removal of information.
- Modifications of information in the end-user management database.
- Retrieval of information contents from any location.
- Retrieval of object identifiers for end users.
- Reconfiguration of end-user information when the end user changes the home site (e.g., virtual home environment).

I.1.3 Service scenarios and procedures for customizable personal directory services

In general, a directory service should provide the following four types of service:

- Mapping name → number or address

  For example, the name of an object may be mapped onto its network address. Note that this is exactly the service provided by a phone book or through telephone inquiries.
- Mapping number or address → set of names

  This service is equivalent to a "yellow pages" function.
- Mapping object → set of names

  A set of objects is identified by one single name.
- Secure communication

  Authentication as well as mechanisms for electronic signatures are provided.

In customizable personal directory services, the following scenarios are considered:

- End user's access to his/her own directory.
- Retrieval of information from a directory.

The service procedures for accessing the end user's own directory are shown in Figure I.2. The end users directly communicate with their own directory in a customizable IP network. Once the authentication procedure is completed, the end users can modify and get their own end-user information from the directory. The directory also contains the end user's location information; such information is updated as the end user moves on to another location.

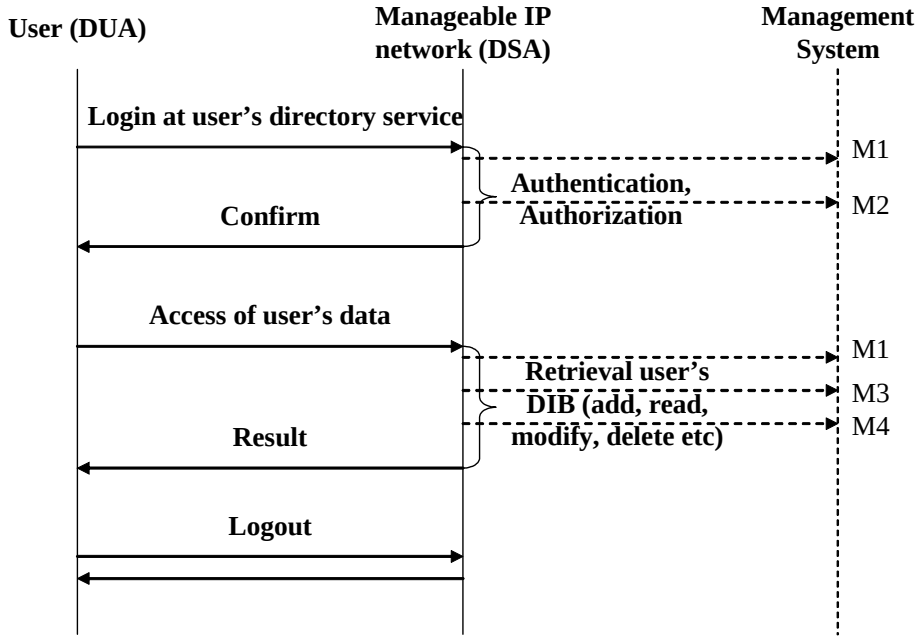


Figure I.2 – Message flow for accessing the end user's own directory

The following are some of the possible fault management events that may be sent to the management system:

M1 Directory service unavailable due to a communication or database problem.

M2 Authentication failure; this event may be reported when fraud is suspected, e.g., based on a repeated pattern of failed login attempts within a relatively short period of time.

M3 Unauthorized end user; the following are two common cases:

- End-user information in the message does not match the end-user information for the existing authorization. This event is also important in fraud detection.
- The end user does not have sufficient authority to retrieve, modify or delete requested information.

M4 Unable to update the database in case of modify and delete operations.

The service procedures for the retrieval of directory information are shown in Figure I.3. The end user sends a search query to the gateway with information to be searched (e.g., name). The query manager within the gateway selects the appropriate directory service system in the CIP network and sends the information request to the designated directory service system. After the retrieval of DIB information, the response manager in the gateway returns a response with the corresponding information (address, number, etc.) to the end user.

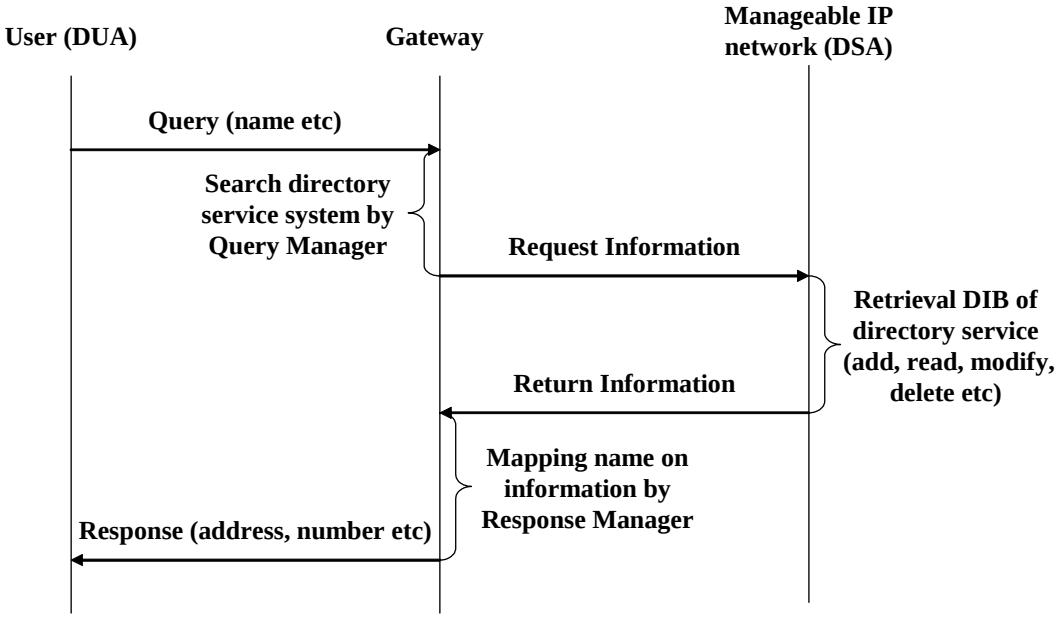


Figure I.3 – Message flow for the retrieval of information in a directory

I.2 Customizable access control services

Customizable access control provides the end user with some controllability while accessing his/her own service profiles and transport capabilities (e.g., VPN).

I.2.1 Objectives of customizable access control services

Allowing for a profile-driven access control mechanism for traffic aggregates is one of the key features of customizable IP networks. This is because end-user applications involve data with different content and bandwidth/QoS requirements.

I.2.2 Functional model for customizable access control services

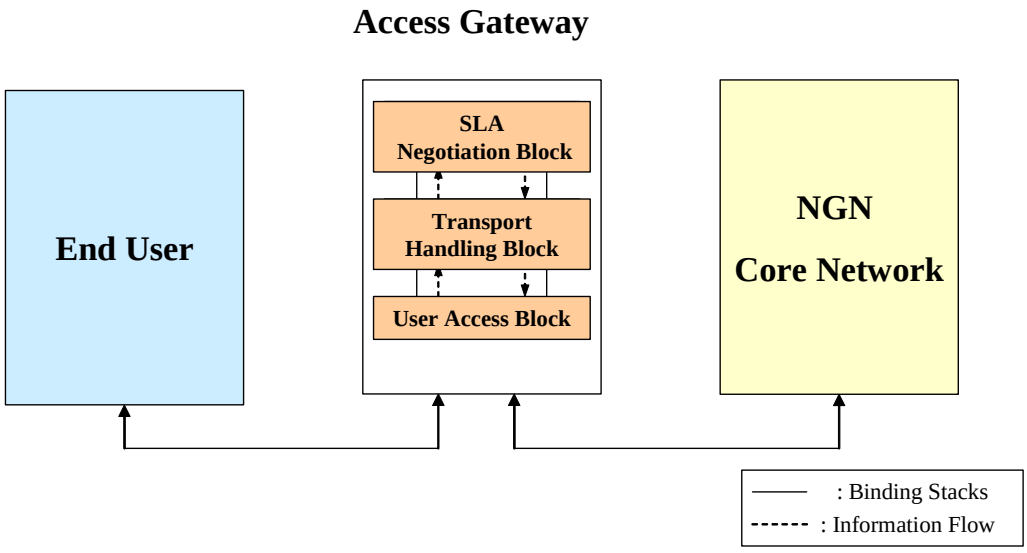


Figure I.4 – Functional model for customizable access control services

Figure I.4 shows the functional model for customizable access control services. In particular, access gateway functions that enable provisioned access control to end users are identified. Access gateway functions consist of three major functional blocks described as follows:

- User access block

  The user access block is where the end user's information request is logged first. Information deemed critical in managing the network is translated into a standard object format and forwarded to the transport handling block.

- Transport handling block

  The transport handling block provides communications paths between the end-user access block and the SLA negotiation block. All information forwarded from the end-user access block is utilized by the transport handling block, which provides common data storage such that new access control information can be easily inserted into the access handling environment. Note that this is one of the key concepts in customizable access from the end users' viewpoint, i.e., the enforcement of service level agreements must be robust and reliable.

- SLA negotiation block

  The SLA negotiation block supports the functionalities for handling SLA negotiation requests between the end user and the CIP provider based on the end user's profile for access control. Charging and billing procedures also form an important part of the functionality of the SLA negotiation block, which acts as the "front-end" for user-network communication and completes the binding for direct communication with the end user. Once this is done, the established session is updated, and a tag for billing and accounting processes is kept.

The SLA negotiation block needs only to update its internal records and communicate the change in request to the CIP provider; an entirely new session establishment is unnecessary. Billing information is passed on to the end user once its session is completed.

I.2.3 Service procedures for customizable access control services

- Negotiation of service profile information

  Dynamic negotiation on service profile information occurs in the SLA negotiation block to which end users are linked. Therefore, access to the CIP network can be partitioned dynamically using the functional blocks of the access gateway for customizable access control.

- Service procedures for customizable access by the end user

  Figure I.5 shows an example of the flow diagram for the end user-driven access control. The end user sends a request to the access gateway using service provision requests, with the end-user access block looking up the CIP network conditioning database and passing the request on to the transport handling block and finally to the SLA negotiation block. The SLA negotiation block must provide application multiplexing. There should also be a provision to accommodate changes in the end users' service level agreements dynamically in an ongoing established session as well as to admit the end-user profile during roaming. Session requirements are negotiated with the CIP provider while a set of default requested objects is maintained in the internal database. Based on the end user's requests, the access gateway opens a session with the CIP provider and negotiates with the CIP provider on the directory, access control and security.

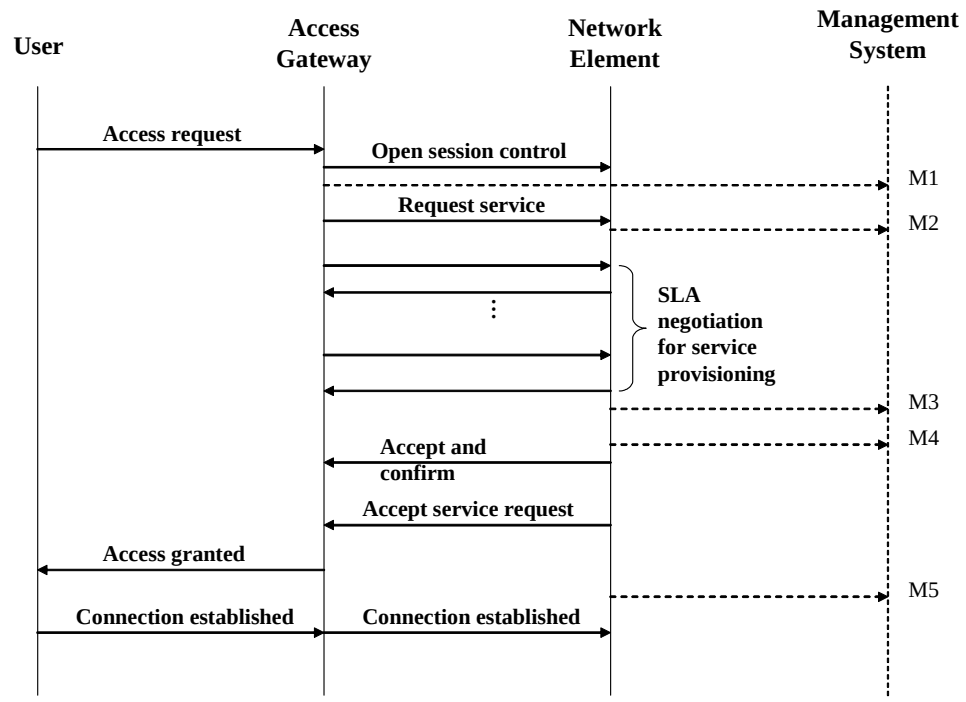


Figure I.5 – Example flow diagram for customizable access control services

For example, during session initiation, SLA negotiation and connection establishment, fault management events may be sent to the management system. The potential fault scenarios are as follows:

M1 Session initiation failure.

M2 Service request processing failure.

M3 SLA negotiation failure: SLA negotiation failure may occur as a result of fault in the service layer or transport layer in a rather complex message flow between a number of CIP network elements such as access gateway, bandwidth managers and policy managers. Therefore, further investigation is required regarding the breakdown of this event.

M4 SLA provision failure on the access gateway

M5 Connection establishment failure: The significance of this event is the determination of the management requirement for the connection (or connections) associated with a session.

- Billing and accounting procedures

  The SLA negotiation block updates its reference database after the session is initiated and starts the system log module once the session is initiated. This is required for billing and accounting purposes. In particular, the logs are important for the collection and distribution of the end user's preferences, application requirements, CIP network device capabilities on the CIP provider side, and availing of the accounting policy information from the network operator. Once successful connection with the CIP provider is realized upon the authentication and verification of the end-user profile, the end-user access block is notified; the end user then starts receiving his/her service requests.

- Support for mobility and seamless connectivity based on customizable access control

  Since the customizable access control scheme provides gateway access using IP addresses, supporting the cross network policy management for mobile end users during roaming is equally important. Such functional components provide the required policies governing end

users accessing third-party networks and crossing geographical boundaries. It keeps in constant contact with other cross-network location registers of the geographically dispersed but interconnected networks, exchanging accounting, service feature profiles and control data for local and roaming subscribers. Within an established session, the SLA negotiation block updates its internal database and starts negotiating with the CIP provider in case of a change in the end user's service requests or profile without creating a new session or disrupting the flow in the established one. If the CIP provider does not entertain this new request, the SLA negotiation block notifies the end user of the unavailability of resources while continuing to service the earlier request. The end user has the choice to either go along with or terminate the ongoing session. After the end user has terminated the session, the SLA negotiation block makes a final write to its internal database regarding the session statistics and makes note of the accounting tag before releasing the session and passing on the information to the end-user access block and finally to the end user.

I.3 Customizable end-to-end QoS services

I.3.1 Objectives of customizable end-to-end QoS service

Customizable end-to-end QoS service intends to provide end users with QoS access and control to satisfy the support for multiple-type services. The end user negotiates with the CIP provider on how to get network resources for end-to-end QoS and handle faults and bottlenecks that may hinder end-to-end QoS. Specifically, the end user is able to negotiate with the CIP provider on service level provision.

Target objectives of the customizable, end-to-end QoS service include:

- Provide the end user with control of QoS parameters.
- Provide the end user with the status of end-to-end QoS.
- Allow the CIP provider to support various end-to-end QoS requests.
- Allow the CIP provider to manage QoS in a non-homogeneous QoS network.

Customizable, end-to-end QoS services offer the following requirements:

- Creation, modification and removal of customizable, end-to-end QoS service profiles.
- Notifying the end user of the negotiation on customizable, end-to-end QoS services dynamically.
- Monitoring the network and ascertaining whether end-to-end QoS can be satisfied.
- Provision of a network to satisfy end-to-end QoS based on the service profile.

I.3.2 Functional model and procedure for customizable end-to-end QoS service

This clause describes the functional model for accessing and managing end-to-end QoS service. Figure I.6 shows the functional model for the customizable end-to-end QoS service. This model includes a service managing block that is responsible for handling end-user requests and data, and an agent that negotiates on the provision with the CIP provider to satisfy end-to-end QoS.

- Customizable end-to-end QoS end-user agent (QUA)

  QUA consists of the request functional block and negotiation functional block. The request manager receives the end user's request and verifies whether the request is valid within the network resources across the CIP network. The negotiation manager receives notifications from the customizable end-to-end QoS network manager (QNM), determines whether the end user's end-to-end QoS request is guaranteed, and re-negotiates with the end user regarding the handling of end-to-end QoS exceptions, if any.

- Customizable end-to-end QoS network manager (QNM)

  QNM receives instructions from QUA. Bandwidth, delay, jitter, packet loss and other QoS guarantee mechanisms are then notified. QoS request mismatches are resolved during negotiations with the CIP network according to the nominal values of end-user requests pertaining to the allocation and increment of bandwidth, change of QoS mechanisms, tuning of QoS parameters to network-supported provision, rerouting and protection, etc.

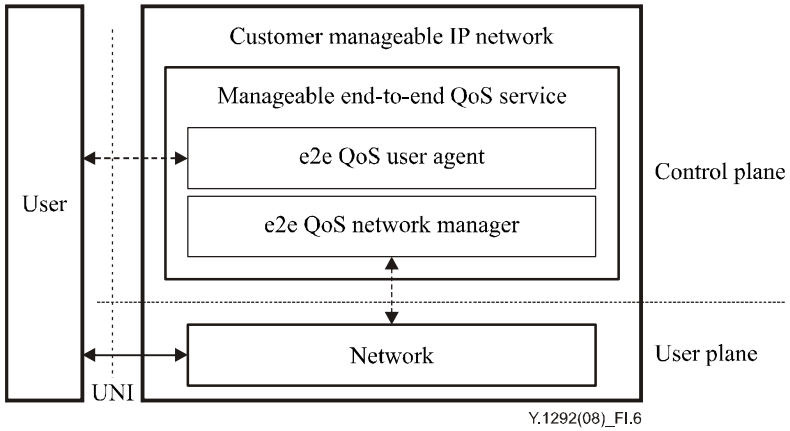


Figure I.6 – Functional model for the customizable end-to-end QoS service

In the procedures for the customizable end-to-end QoS service, the end user creates and registers customizable end-to-end QoS service with his/her initial requirements for end-to-end QoS. The end-to-end QoS end-user agent (QUA) can poll or obtain notification regarding QoS performance from an access node and an edge router of the CIP network. Bandwidth, delay, jitter and packet loss are the basic parameters for the customizable QoS performance. When the end-to-end QoS performance falls below the threshold level requested by the end user, QUA takes appropriate actions based on its stored default values to recover from such service level deterioration. If QUA is unable to negotiate with the CIP provider, the end user can re-negotiate the required QoS to request the guarantee of appropriate QoS levels.

The interface between the end user and the customizable end-to-end QoS function provides messages to:

- Create and delete the QoS profile in the customizable end-to-end QoS function.
- Notify the end user of the deterioration in the QoS level.
- Make a compromise between the end user and QoS function when the end user's requests cannot be satisfied.

The interface between the customizable end-to-end QoS function and CIP network provides messages to:

- Notify QoS performance change for the customizable end-to-end QoS function.
- Take QoS action on the CIP network.

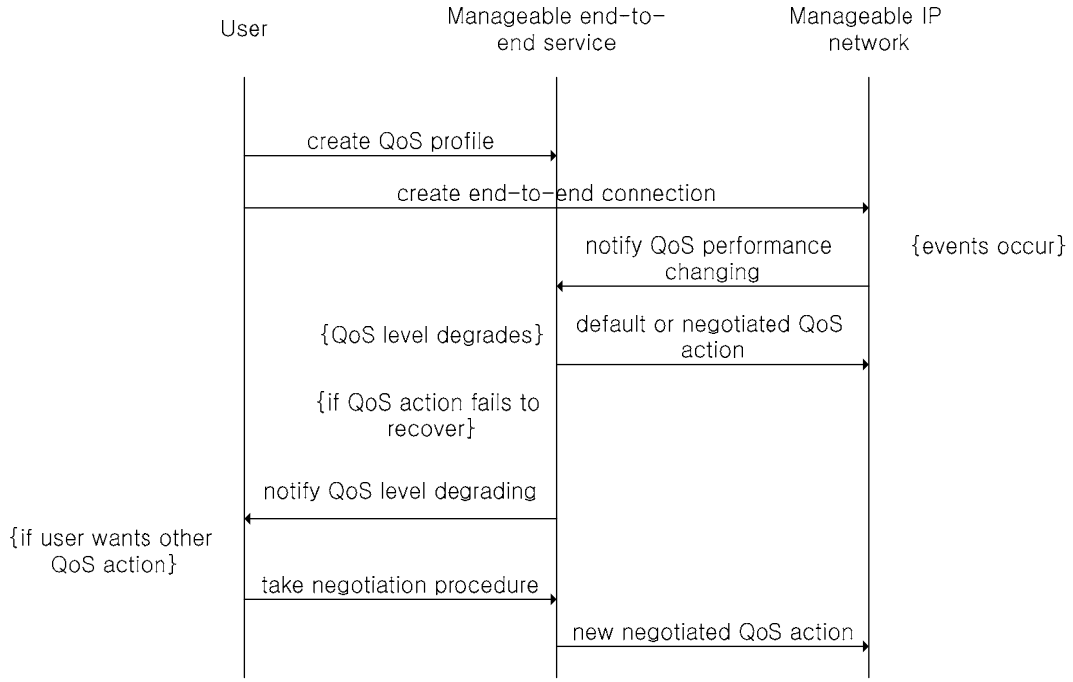


Figure I.7 – Message flows for the customizable end-to-end QoS service scenario

I.3.3 Service scenario of customizable end-to-end QoS service

An end user requests the CIP provider for an end-to-end connection with his/her QoS requirements. If QoS deteriorates, the customizable end-to-end QoS service will consider the following actions:

- Provide more network resources or reroute for end-to-end connection.
- Re-negotiate QoS parameters for end-to-end connection with the end user.

When the CIP network does not consist of homogeneous equipment to satisfy the same QoS level, the customizable end-to-end QoS service should know the different capabilities and select the appropriate QoS mechanism.

The following three scenarios are considered:

- Scenario 1 (selection of TE capability)

  Suppose an end user wants a specific bandwidth guaranteed for peer-to-peer connection, such as the VoIP network. First, the end user sends his/her connection request to the CIP network. The CIP network then receives this request and checks the status of available resources. Afterward, the CIP network responds to the end user with two options: best-effort delivery with admission control and guaranteed delivery available end-to-end communication path.

- Scenario 2 (priority assignment with cost option)

  In this scenario, the end-to-end QoS service offers priority scheduling. In case of congestion on the end-to-end path, higher priority may be selected. When the status of the path becomes normal, the priority provision returns to the normal condition to save cost.

- Scenario 3 (re-negotiation of TE capability)

  When QoS deteriorates, and all options are not applicable, end users are notified accordingly, and re-negotiation is held with the end user on how to satisfy end-to-end QoS.

I.4 End-user customizable location monitoring services

The end-user customizable location monitoring service is a service that enables the management and monitoring of end users' location information anytime, anywhere and regardless of the access technology they are using (fixed, wireless).

I.4.1 Objectives of the end-user customizable location monitoring service

The main objective of the end-user customizable location monitoring service is that an end user retrieves other end users' location information from a location information functional database. In many cases, end users are interested in communicating with a given set of their interested peers. Another objective is to provide basic information support to other services, such as emergency services.

I.4.2 Functional model for the end-user customizable location monitoring services

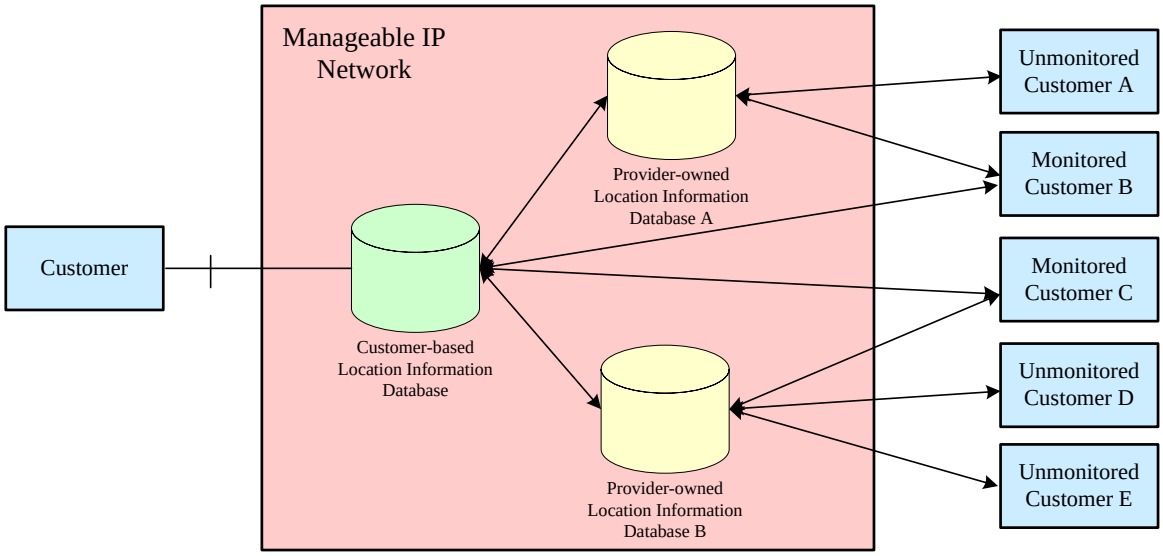


Figure I.8 – Functional model for the end-user customizable location monitoring service

The following functions are required to support the end-user customizable location monitoring service:

- Functions required on the end-user side
  - Requests regarding other end users' locations as sent to the customizable IP network.
  - Managing monitored end users' location information.
- Functions required on the CIP network side
  - Managing their respective end users' location information.
  - Responding to end-user location requests

As depicted in Figure I.8, two types of functional databases are required to support the end-user customizable location monitoring service: one is a CIP provider-owned location information database with the location information of CIP network end users. This database is an origin network location information database such as home location register/visitor location register, domain name system and home agent/foreign agent binding cache. Another is a customer-based location information database containing processed location information of customer end users. This database consists of various location information such as GPS location information and location information combined with other end-user information such as availability and connectivity.

- CIP provider-owned location information database

  This functional block is used to maintain and manage the location information of all CIP network end users.

- Customer-based location information database

  This functional block is used to request for, update, add and delete end-user location information to/from the CIP provider-owned location information database of the other end user.

I.4.3 Service scenarios of end-user customizable location monitoring services

An end user is interested in knowing the location information of its peers. In this scenario, security issues such as authentication, authorization and accounting are not covered by the scope of this Recommendation.

The following two scenarios are identified:

- End-user-to-end-user-based location information database to the CIP provider-owned location information database

  This scenario is a single-mode operation. An end user requests the other end user's location information once. If the end user-based location information database does not have the other location information, a request is issued to the CIP provider-owned location information database.

- End-user-to-end user-based location information database to monitored end user

  This scenario is a continuous-mode operation. An end user requests for the other end user's location information periodically. After the single-mode operation, the end user-based location information database contains the monitored end user's location information. Therefore, the end user-based location information database issues a request to the monitored end user directly.

In these two scenarios, the end-user-based location information database may not need to share its network resources directly with an end user. This is because the CIP provider-owned location information may be owned by the CIP provider. The CIP provider-owned location information database should manage all their respective end users' location information.

The first scenario is a single-mode operation scenario whose service procedure is shown in Figure I.9. In this scenario, an end user requests for the other end user's location information from the end-user-based location information database with a single-mode start message. In the case where the end-user-based location information database does not have the corresponding requested end user's information, a request is issued to the CIP provider-owned location information database to such effect. After receiving the request message, the provider-owned location information database responds by sending location information to the end-user-based location information database. This information is processed by the end-user-based location information database; such processed information is then provided to the requesting end user.

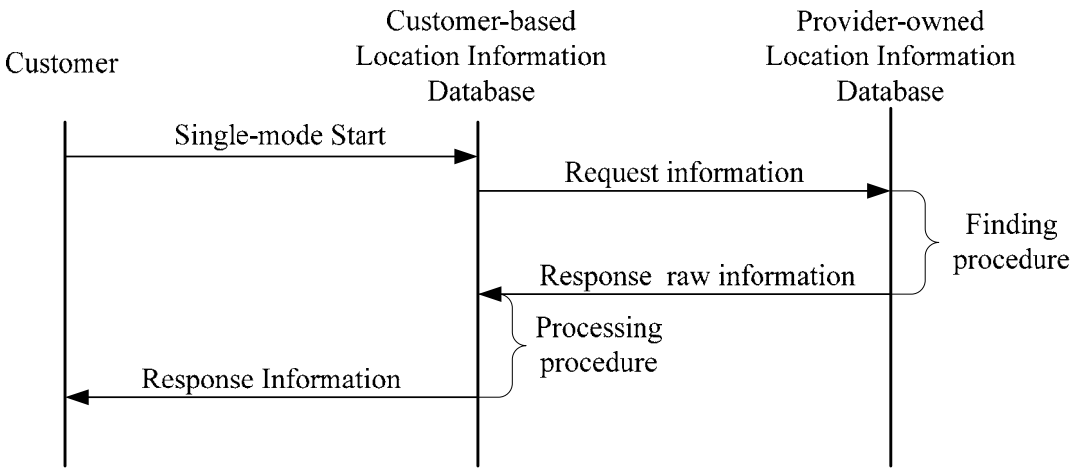


Figure I.9 – Service procedure for the single-mode operation service scenario

The second scenario is a continuous-mode operation scenario whose service procedure is shown in Figure I.10. In this scenario, an end user requests for monitored end user's location information from the information database with a continuous-mode start message. The first operation is almost the same as the single-mode operation service scenario. Note, however, that the end user-based location information database continuously adds other monitored end users to the end-user list. The end-user-based location information database periodically provides the processed information to the end user. If the end-user-based location information database receives a stop message, however, this process stops; the end-user-based location database then deletes the monitored end user's information from its list.

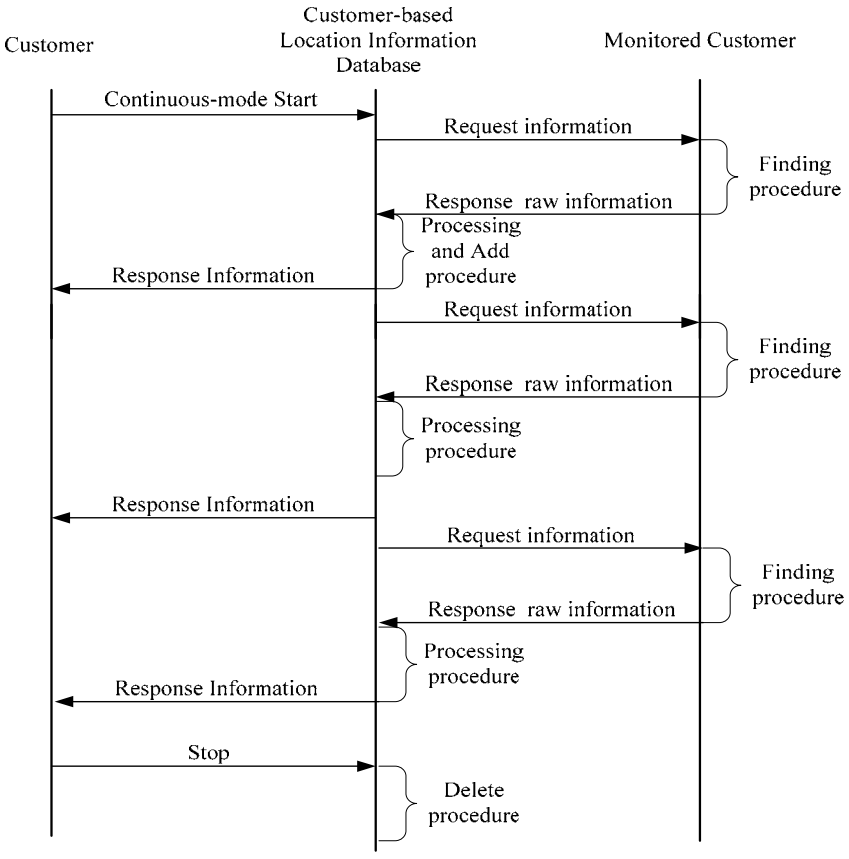


Figure I.10 – Service procedure of continuous-mode operation service scenario

I.5 Customizable home networking services

I.5.1 Objectives of the customizable home networking service

Home networking services can be defined as those providing home automation services, home entertainment services, security services and Internet service to the home. Home automation services are used to control lighting, appliances and climate control at home. Home entertainment services enable the end user to access audio, video and television services at home. Home networking services may also be extended to support the interconnection among various devices with radio frequency identifier (RFID) tags and increase the scale of network connections in comparison with the home networking services.

I.5.2 Functional model for the customizable home networking service

There are two modes of operation for home networking services: one is the local service access inside the home or within the home area network, which starts service invocation from inside the home and remote service access from external networks.

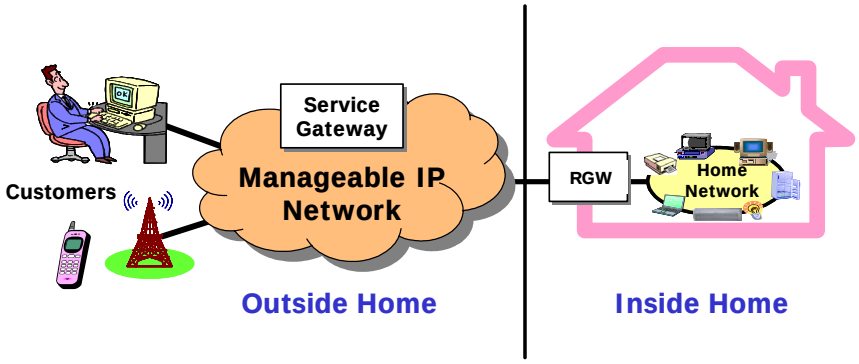


Figure I.11 – Architecture for the home networking service in the customizable IP network

As shown in Figure I.11, service gateway functions within the customizable IP network act as the portal to allow remote access and control from the external network to the home network. The service gateway enables the remote end user to manage home networking services and devices via the residential gateway. The following functions and capabilities are provided by the service gateway to support home networking services:

– End-user authentication and authorization.
– Service management.
– Service usage measurement.
– Secure connection/session establishment.
– Firewall function to protect against possible threats.
– Home directory service function that collects and presents instances of home equipment, equipment services and contents to the end user.
– Remote control function.
– Remote configuration, management function.
– Web service-based interface to have access and control.
– Policy decision function to manage QoS.

A residential gateway is a device that interconnects various home networking devices and acts as a mediator between the end user and service gateway. The residential gateway allows intelligent end user services to be created and managed within the home network as well. The details of the residential gateway functions are not addressed in this Recommendation, however.

I.5.3 Service scenario and procedures for customizable home networking services

Figure I.12 shows an example of information flows of the home networking service to enable an end user to "turn on the lights" from a remote site. SIP, HTTP and SOAP are assumed to be available for use in delivering control messages to communicate between gateways and home devices. The following procedures show the information flows required for a "turn on the lights" home networking service:

1) A remote end user is trying to log on to the service gateway to have access to home networking services.
2) If the end user is successfully authenticated and authorized, then the service gateway returns an OK message to the end user.
3) The end user sends a control message such as "turn on the light on the following device in the living room" to the service gateway.
4) The service gateway then requests for a session establishment between the service gateway and residential gateway and home device to forward the control message.
5) Once the session is successfully established, the service gateway sends to the home device the control message "turn on the light on the following device in the living room" via the residential gateway.
6) The response from the home device is acknowledged.
7) The OK control message is delivered back to the end user.
8) The end user logs off to quit the home networking service.
9) The session is terminated between the service gateway and residential gateway and home device.
10) The session between the end user and service gateway is ended.

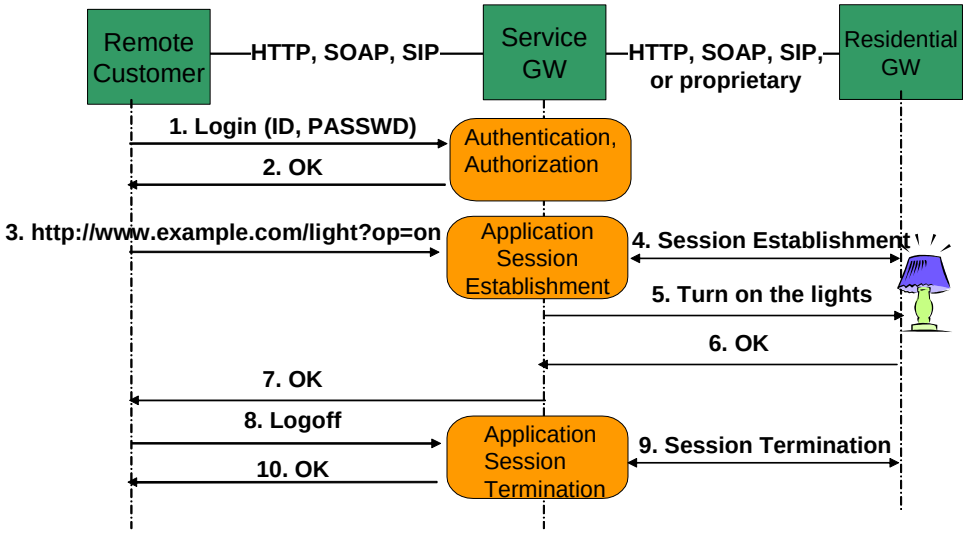


Figure I.12 – Example of information flows of the home networking service

I.6 Client networking services with QoS and security

I.6.1 Objectives of the client networking service with QoS and security

The customizable IP network supports functions to control QoS and security capabilities simultaneously or partly as requested by end users. The CIP network expects a secured path to be associated strictly with QoS provision for different types of services; hence the need to classify networking service features in QoS and security.

An example of a client networking service with QoS and security is to provide authentication mechanisms at the level of aggregates of packets such as channels or flows such that these checks need not be done on individual packets. This suggests an architecture wherein authentication and other resource management decisions are initially processed to minimize the cost of subsequent decisions. Consequently, multilayered architecture to provide QoS and security procedures may be needed as shown in Figure I.13.

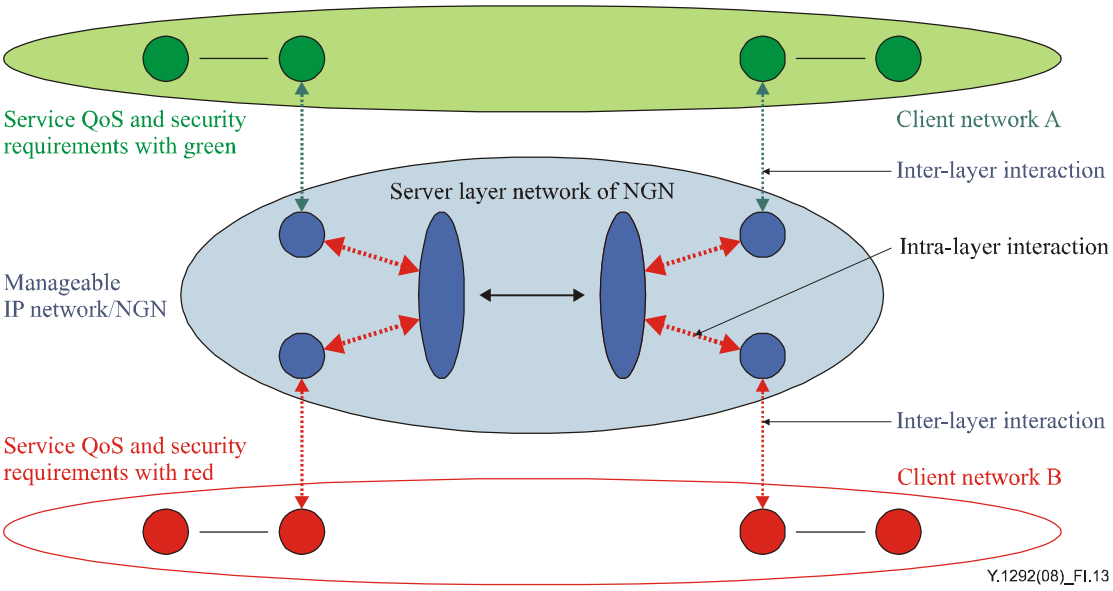


Figure I.13 – Example architecture for the client networking service with QoS and security

I.6.2 Overlay model for client networking services with QoS and security

Figure I.14 shows the overlay model for client networking services with QoS and security. In particular, an example of overlay virtual networking is presented. Virtual networking is applied to the model based on independently multi-layered architecture wherein incoming packets are classified at the edge and packets for the secured QoS service are forwarded to policy-based overlay networks; thus providing secured networking and QoS managed functions through admission control and other control mechanisms. Based on the functional architecture, a networking feature is necessary to adopt QoS and security features efficiently.

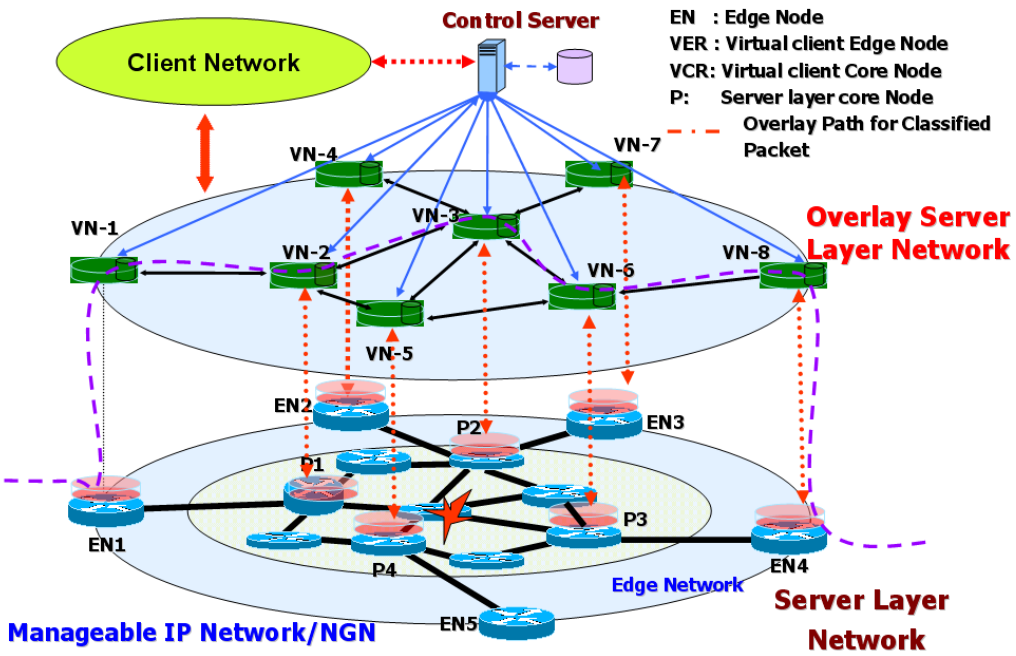


Figure I.14 – Overlay model for client networking services with QoS and security

An example of the routing management algorithms of the overlay model is presented in Figure I.15. This figure shows the procedure for virtual networking function (VNF) table construction. Control information is classified according to the incoming end-user information, with the control server making its own networking table in procedures c, d and e. The multiple virtual networking tables according to security level and required QoS level are applied to perform the routing functions over the overlay network. The primary goal of VNF provision on the overlay network is to provide multiple secured QoS paths at each level. The VNF routing function is performed independently of other VNF domains in the network.

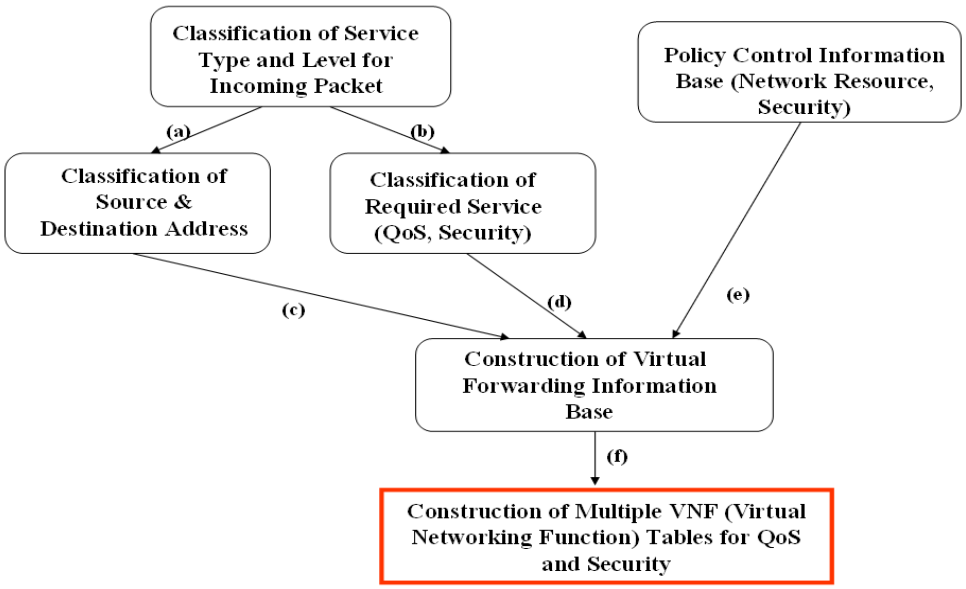


Figure I.15 – Examples of table construction of virtual networking function in the overlay model

To make a forwarding information base from information on routing and policies, advanced control mechanisms are required to supply multilayered virtual client networking associated with end-user customizable networking features.

Appendix II

Example of functional architecture and service creation scenario for end-user customizable VPN services

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

VPN will be one of the most promising services in NGN according to the rapid increase in VPN service demands. The framework for the dynamic creation of VPN service based on intelligent/active networking will promote a variety of VPN application services. In a network based on service negotiation, a node with intelligent/active features is able to represent a solution to manage the entire volume of different requests coming from consumers.

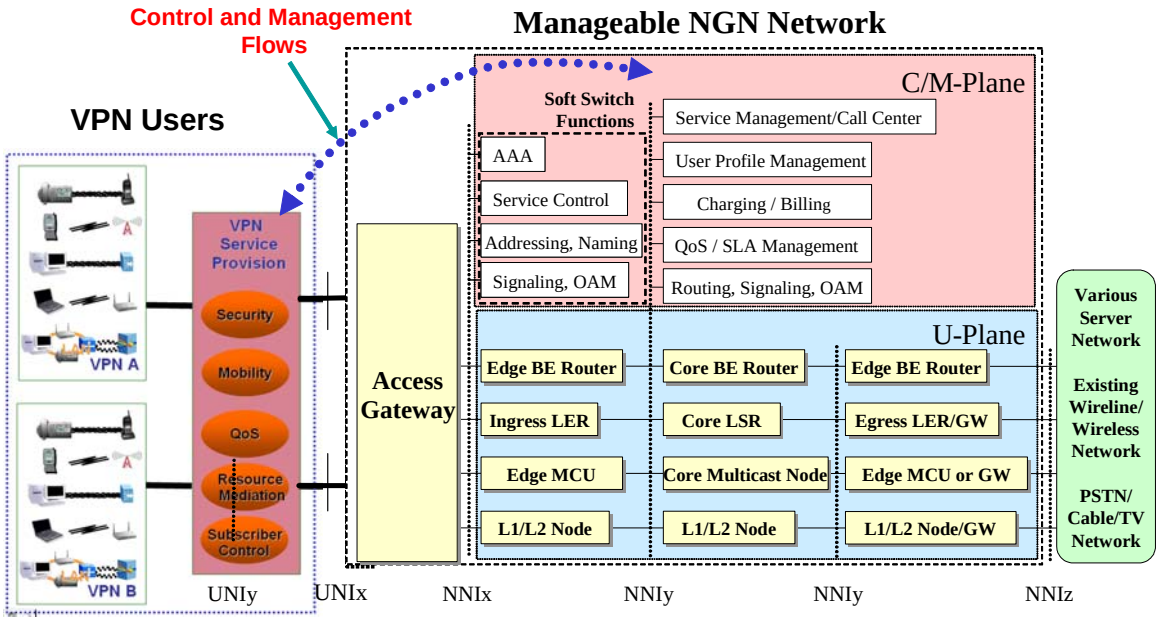


Figure II.1 – Example of the functional architecture for end-user customizable VPN services

Security is definitely one of the key issues in VPN scenarios. An intelligent and active feature in VPN networking will assume an important role to provide flexible means for customizing services appropriately. The intelligent/active features for security in VPNs are exploited for adaptive secure routing and service capability. In particular, the security capability of VPN is negotiated with the C/M-plane of the IP network; its service level will be assigned to VPN end users.

As shown in Figure II.1, the control and management functions of the customizable IP network represented in a control flow between a service provision module of VPNs and the C/M-plane module of the customizable IP network are established to deliver networking service capabilities from/to VPNs. The C/M-plane of the CIP network will need to be characterized to provide the above-mentioned networking capabilities to VPNs.

In addition to the above-mentioned features, the following capabilities are characterized to provide intelligent/active VPN services in the CIP network:

- Mobility.
- Static/dynamic QoS provision.
- Resource mediation for VPN services.
- Subscriber control on VPNs' service capabilities.

- Security negotiation/provision.

From a functional standpoint in the intelligent VPN of the IP network, VPN is an active flow activated by appropriately customizing additional intelligent/active features in a VPN access node. This is achieved via one underlying program and their injected programs, each associated with one of the intelligent/active VPN functions. The activation process is appropriately invoked vis-a-vis external topology, internal topology and the routing table of VPNs (with multiple virtual routing tables). By applying these parameters, a number of different VPNs are characterized by their own topology and management strategy.

Figure II.2 shows an example of the functional architecture for implementing a customizable VPN. If VPNs are considered to be interconnected at different operators, implementation architecture for a customizable VPN may be as illustrated in Figure II.2. For example, the customizable VPN service requires the following three functions: service mediator, SLA mediator and access mediator.

- Service mediator function
  - AAA.
  - Presentation.
  - Subscription.
- SLA mediator function
  - Dynamic negotiation and re-negotiation of SLA.
  - Synchronization with other SLA mediator.
  - Communication with resource manager in the customizable IP network.
- Access mediator function
  - AAA.
  - Directory transactions.
  - Preference list handling.
  - Service menu.
  - End-user profile processing.
  - Terminal types and mapping.

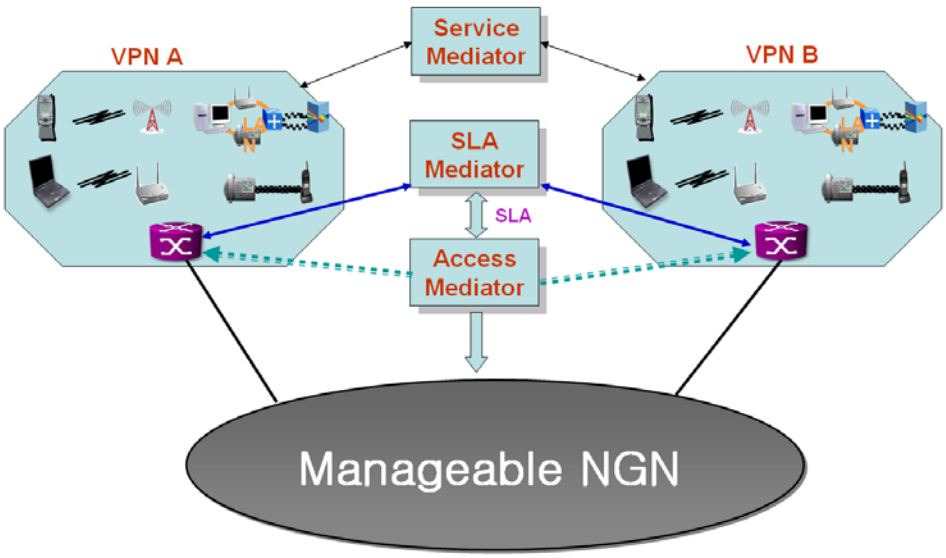


Figure II.2 – Example of the implementation scenario for end-user customizable VPN

Bibliography

[b-ITU-T H.323] Recommendation ITU-T H.323 (in force), *Packet-based multimedia communications systems*.
<http://www.itu.int/rec/T-REC-H.323>

[b-ITU-T X.160] Recommendation ITU-T X.160 (1996), *Architecture for customer network management service for public data networks*.
<http://www.itu.int/rec/T-REC-X.160>

[b-ITU-T Y.130] Recommendation ITU-T Y.130 (2000), *Information communication architecture*.
<http://www.itu.int/rec/T-REC-Y.130>

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)*.
<http://www.ietf.org/rfc/rfc959.txt>

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.
<http://www.ietf.org/rfc/rfc959.txt>

[b-Foster] Foster I. (2003), *The Grid: Computing Without Bounds*, Scientific American Magazine, April, pp. 60-67.

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, 2010