International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2215

(06/2009)

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

Next Generation Networks – Service aspects: Service capabilities and service architecture

---

Requirements and framework for the support of VPN services in NGN, including the mobile environment

Recommendation ITU-T Y.2215

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
IPTV over NGN	Y.1900–Y.1999
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
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2215

Requirements and framework for the support of VPN services in NGN, including the mobile environment

Summary

Recommendation ITU-T Y.2215 specifies service requirements and framework for the support of VPN services in NGN, including the mobile environment.

Source

Recommendation ITU-T Y.2215 was approved on 29 June 2009 by ITU-T Study Group 13 (2009-2012) under Recommendation ITU-T A.8 procedures.

Keywords

Functions, mobile, next generation network, service requirements, virtual private network.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T Y.2215

Requirements and framework for the support of VPN services in NGN, including the mobile environment

1 Scope

This Recommendation identifies service requirements and functional framework for the support of VPN services in NGN, including the mobile environment.

The provision of VPN services in NGN, including the mobile environment, covers the support of mobility management functions across different fixed and wireless network domains as well as at different network levels including intra-access network, inter-access network, and inter-network levels [ITU-T Q.1706]. This includes mobility support at the NGN service stratum and the NGN transport stratum [b-ITU-T Y.2011].

The detailed definition of mobility management-related functions and architecture is outside 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 Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

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

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

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[ITU-T Y.2236] Recommendation ITU-T Y.2236 (2009), *Framework for NGN support of multicast-based services*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 access network [b-ITU-T Q.1742.1]: Network that connects access technologies (such as a Radio Access Network) to the core network.

3.1.3 accounting [b-ITU-T Y.2233]: The process of collecting and analysing NGN service and NGN resource usage metrics for the purposes of capacity and trend analysis, cost allocation, auditing, and billing, etc. Accounting management requires that resource consumption be measured, rated, assigned, and communicated between appropriate business entities.

3.1.4 billing [b-ITU-T Y.2233]: The process after rating in which the NGN transactions of NGN event usage are compiled and bills are produced.

3.1.5 charging [b-ITU-T Y.2233]: Function within the NGN network and the associated OCS/BD components whereby information related to a chargeable event is collected, formatted, transferred and evaluated in order to make it possible to determine usage for which the charged party may be billed (offline charging) or the subscriber's account balance may be debited (online charging).

3.1.6 mobility [ITU-T Q.1706]: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.1.7 mobility management [ITU-T Q.1706]: The set of functions used to provide mobility. These functions include authentication, authorization, location updating, paging, download of user information and more.

3.1.8 personal mobility [ITU-T Q.1706] and [ITU-T Y.2201]: This is the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

3.1.9 quality of service (QoS) [b-ITU-T G.1000]: The collective effect of service performances, which determine the degree of satisfaction of a user of the service.

3.1.10 service continuity [ITU-T Y.2201]: The ability for a moving object to maintain ongoing service over including current states, such as user's network environment and session for a service.

3.1.11 service level agreement [b-ITU-T G.8081]: A contract between two parties such as a service provider and a customer. It defines the services available to the customer, and the grade of service of those services as offered to the customer. It also usually describes the service guarantee and potential penalties in case of service degradation or failure.

3.1.12 terminal mobility [ITU-T Q.1706] and [ITU-T Y.2201]: This is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. The ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 virtual private network (VPN): A VPN is a communication network, built over public and/or private network resources, used to support controlled and secure communications within a group of users as if they were on a private network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ANI	Application-to-Network Interface
CE	Customer Equipment
CPE	Customer Premises Equipment

GRE	Generic Routing Encapsulation
GTP	GPRS Tunnelling Protocol
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
L2TP	L2 Tunnelling Protocol
LAN	Local Area Network
mGRE	multipoint Generic Routing Encapsulation
MPLS	MultiProtocol Label Switching
NACF	Network Attachment Control Functions
NGN	Next Generation Network
NNI	Network-to-Network Interface
PD-FE	Policy Decision Functional Entity
PE	Provider Equipment
PE-FE	Policy Enforcement Functional Entity
QoS	Quality of Service
RACF	Resource and Admission Control Functions
SA	Security Association
SCF	Service Control Functions
SLA	Service Level Agreement
TRC-FE	Transport Resource Control Functional Entity
UNI	User-to-Network Interface
VPN	Virtual Private Network

5 Conventions

None.

6 Introduction

The support of virtual private network (VPN) services in NGN including mobile environment allows multipoint controlled and secured communication services using NGN resources for the exchange of multimedia streams within a group of service users.

Types of VPN services in NGN include:

– Site-to-site VPNs that link branch offices, suppliers, partners, customers, and communities of interest;

– Access VPNs that accommodate mobile workers and telecommuters allowing them to securely access their corporate network from outside the office;

– Multiservice VPNs that support multimedia communications with end-to-end QoS provision.

Appendix I provides scenarios for enhanced applications and services supported via the use of VPN services.

This Recommendation builds upon the NGN capabilities specified in [ITU-T Y.2201].

7 Service requirements

This clause addresses the requirements for VPN services when provided in NGN, including the mobile environment.

7.1 General requirements

For the support of VPN services [ITU-T Y.1311], NGN is required to provide:

- support for fixed and mobile users;
- means for users to specify VPN membership;
- accommodation of user-defined VPN addressing schemes;
- transparency to user data;
- means for single customer site to belong concurrently to more than one VPN;
- provision of arbitrary user-defined VPN topologies (ranging, for example, from hub-and-spoke, partial mesh to full mesh);
- provision for multiprotocol support;
- provision of multi-homed user sites;
- provision of standards-based interfaces (independent of user's device supplier);
- support for wide range of routing protocols between CE and PE routers [ITU-T Y.1311];
- means to support a variety of user's traffic (QoS) requirements as defined by the user, or negotiated/renegotiated (e.g., between the user and the provider);
- means to support different modes of communication: one-to-one, one-to-many, many-to-one and many-to-many;
- means to offer, support and maintain agreed levels of service (e.g., via service level agreements);
- means to meet user's security requirements (e.g., in terms of different security levels);
- provision of VPN members with secure dynamic access to VPN (e.g., via dial-up);
- provision of appropriate VPN management services in the areas of configuration, SLAs and QoS, security, fault, performance, accounting, mobility and multicast;
- accommodation for growth of a given VPN or a number of VPNs;
- means of ensuring service and transport level compatibility among VPN members (e.g., tunnelling, codecs).

7.2 Configuration management

NGN is required to provide:

- configuration capabilities for VPN members at both the service and the transport level (e.g., dynamic creation and modification of VPNs, according to specific application requirements and/or user requirements);
- consistency and coherence verification of user configuration information;
- ability to easily change topology;
- ability to easily add, remove or modify VPN-related devices, sites, routes, etc.;

– ability to accommodate growth requirements for VPN related devices, sites, routes, traffic, etc.

7.3 Service level agreements and quality of service

NGN is required to support mechanisms for negotiating service level agreements (SLAs) with the (fixed or mobile) subscriber/user (e.g., per VPN, per VPN site, per VPN connection).

SLAs include:

– service level objectives, e.g.:
  - bandwidth (e.g., tunnel bandwidth);
  - QoS parameters (e.g., packet loss rate, latency);
  - availability;
  - reliability;
  - security;
  - priority;

– service monitoring objectives:
  - QoS monitoring;
  - flow tracking;
  - reporting.

NGN is required to provide mechanisms to ensure QoS support as required by SLAs. These mechanisms include VPN-related resource and admission control mechanisms such as:

– priority management (e.g., per VPN, per VPN site, per VPN connection);

– traffic class differentiation;

– QoS signalling;

– performance measurement;

– overload/congestion control.

7.4 Security

NGN is required to support mechanisms for:

– controlling (fixed or mobile) user access to the VPN via access control mechanisms (identification, authentication and authorization of (fixed or mobile) users accessing the VPN);

– ensuring the privacy of data being transported by the VPN;

– secure key distribution;

– secure and efficient SLA negotiation;

– security policies to satisfy users and/or providers' security requirements (e.g., to adjust the configuration of VPN users or VPN groups, to reflect trust relationships).

7.5 Fault management

NGN is recommended to provide:

– information to the VPN customer in the event of service disruption and restoration;

– dynamic VPN recovery, non-disruptive and not perceived by the VPN users;

– provision of relevant VPN incident reports and summaries.

7.6 Performance management

NGN is recommended to support:

- maintenance of VPN performance consistent with SLAs;
- provision of VPN performance information, including statistics;
- ability to demonstrate performance to VPN customer;
- prediction of VPN trends, likely problems and/or recommendations in relation to current SLAs, traffic patterns, QoS, etc.

7.7 Accounting

NGN is required to support:

- provision of accounting information to VPN customer/users;
- customized breakdown of VPN accounting information;
- correlation of accounting to QoS and/or SLAs;
- correlation of accounting to VPN performance and fault management information.

7.8 Mobility

NGN is required to support:

- nomadism for personal (i.e., VPN user) and terminal (i.e., VPN user terminal) mobility.

NGN is recommended to support:

- service continuity [ITU-T Q.1706] for terminal mobility.

In particular, NGN is required to support:

- service continuity for terminal mobility in case of VPN voice services.

7.9 Multicast

NGN is recommended to support:

- multicast capabilities within a VPN, e.g., to support specific applications such as linear TV within a VPN.

If multicast capabilities are supported, NGN is required to support:

- creation, operation and release of multicast groups within a VPN;
- mechanisms to manage multicast connections within a VPN (i.e., all multicast trees within that VPN);
- mechanisms allowing VPN members to join and leave multicast groups within a VPN.

8 VPN framework architecture

This clause identifies the new functions and extensions/modifications of the various functions of the NGN functional architecture [ITU-T Y.2012] in order to support VPN services in NGN, including the mobile environment.

Figure 1 shows the VPN framework architecture based on the NGN functional architecture [ITU-T Y.2012] for the provision of VPN services in NGN, including the mobile environment.

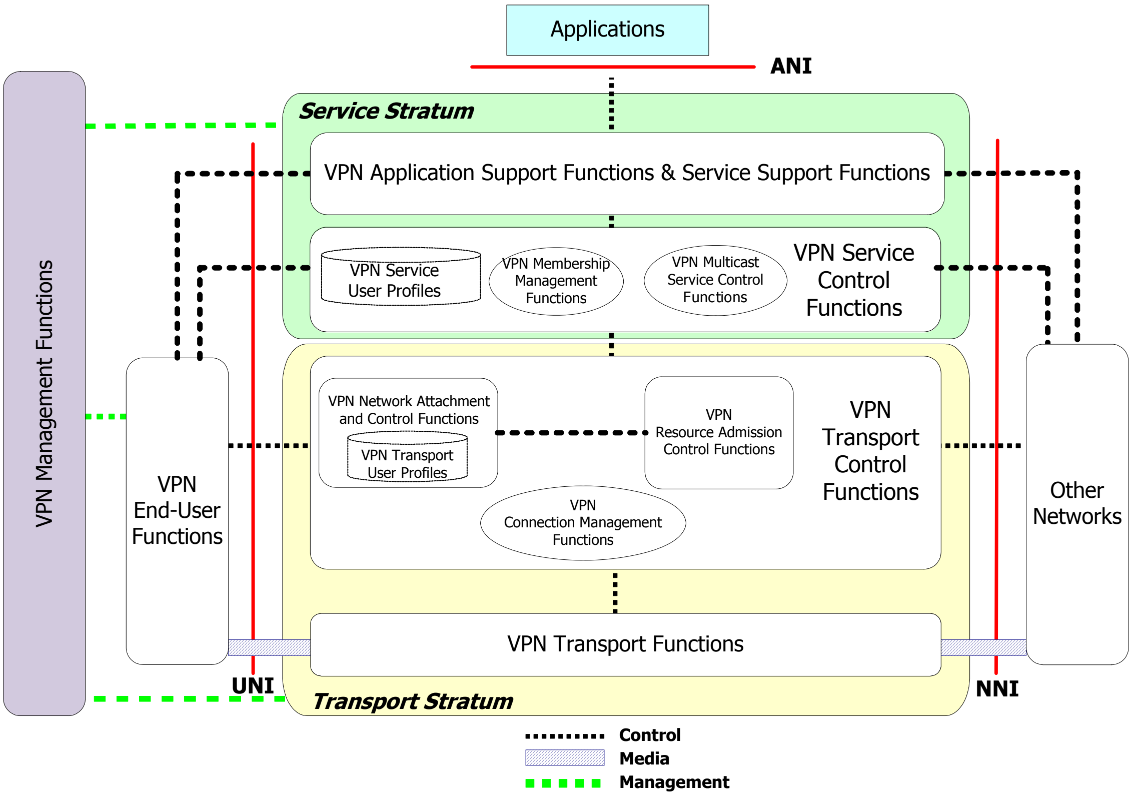
Applications
ANI
Service Stratum
VPN Application Support Functions & Service Support Functions
VPN Service User Profiles
VPN Membership Management Functions
VPN Multicast Service Control Functions
VPN Service Control Functions
VPN Management Functions
VPN End-User Functions
VPN Network Attachment and Control Functions
VPN Transport User Profiles
VPN Resource Admission Control Functions
VPN Transport Control Functions
VPN Connection Management Functions
Other Networks
VPN Transport Functions
UNI
NNI
Transport Stratum
Control
Media
Management

Figure 1 – VPN framework architecture based on [ITU-T Y.2012]

8.1 VPN functions at the service stratum

The service stratum provides the VPN service level functions which include VPN application support and service support functions and VPN service control functions.

8.1.1 VPN application support and service support

The VPN application support and service support functions work in conjunction with the VPN service control functions to provide VPN end-users and VPN applications with the capabilities they request.

VPN application interactions with the VPN application support and service support functions are handled through the ANI reference point.

8.1.2 VPN service control

The VPN service control functions (including VPN membership management and VPN multicast service control functions) provide service control functions for VPN applications including interaction with service user profiles. VPN service control functions provide the capabilities to:

– register VPN members;

– authenticate and authorize VPN members;

– select data encryption methods, and key exchanges, if required;

– negotiate QoS and SLA;

– perform mobility management;

– perform session control among VPN members;

– perform VPN membership management, as described in clause 8.1.2.1;

– perform VPN multicast service control within a VPN, as described in clause 8.1.2.2.

8.1.2.1 VPN membership management

The VPN membership management functions provide support for:

- creation, maintenance and release of VPNs;
- joining and leaving VPNs;
- partitioning of a VPN into multiple VPN groups (including VPN multicast groups).

The VPN membership management functions interact with multicast group membership management functions [ITU-T Y.2236] for VPN multicast group membership management.

8.1.2.2 VPN multicast service control

The VPN multicast service control functions use multicast service control functions [ITU-T Y.2236] to control VPN multicast groups.

8.2 VPN functions at the transport stratum

8.2.1 VPN transport control

The VPN transport control functions provide VPN resource and admission control functions, VPN network attachment control functions and VPN connection management functions.

8.2.1.1 VPN resource and admission control

Resource and admission control functions for VPNs provide VPN resource management to support QoS (including resource reservation) and VPN admission control in the transport stratum.

VPN resource management includes: intra-VPN resource calculation, VPN path selection, mapping of VPN network topology to transport resources, maintenance of VPN membership information, policy management.

VPN admission control involves checking authorizations based on user profiles, SLAs, operator specific policy rules, service priority, and resource availability within access and core transport networks.

8.2.1.2 VPN network attachment control

The VPN network attachment control functions provide registration of VPN users at the access level and initialization of VPN end-user functions for accessing VPN services.

The VPN network attachment control functions provide VPN network-level identification and VPN user authentication and authorization (based on VPN user profiles).

The VPN network attachment control functions also manage the VPN related IP address space, authenticate VPN access connections, and announce to VPN users the contact point(s) of VPN related functions in the NGN service stratum.

The VPN network attachment control functions also provide VPN configuration based on VPN user profiles (e.g., QoS related profile information).

The VPN network attachment control functions provide support for VPN transport user profile, which takes the form of a functional database including VPN user's information and other VPN user related control data.

8.2.1.3 VPN connection management

The VPN connection management functions provide management of VPN connections (tunnel management). The VPN connection management functions include the VPN multicast connection management functions.

8.2.1.3.1 VPN multicast connection management

The VPN multicast connection management functions use multicast connection management functions [ITU-T Y.2236] to control VPN multicast connections (i.e., all multicast trees within a VPN).

8.2.2 VPN transport

The VPN transport functions provide transport level functions (e.g., VPN traffic forwarding).

8.3 VPN end-user functions

The VPN end-user functions provide support for:

– SLAs and QoS levels, enabling various VPN traffic engineering mechanisms such as service priority control, packet filtering, traffic classification, rate limiting, resource reservation and admission control at the transport stratum;

– VPN join/leave;

– VPN group join/leave (including VPN multicast groups);

– VPN security providing support for VPN end-user traffic encryption/decryption, VPN end-user authentication and other VPN end-user security features, such as access control and security assurance control.

8.4 VPN management functions

These functions are out of scope of this Recommendation.

9 Security

Security of VPN services in NGN, including the mobile environment, is required to satisfy both NGN security requirements as contained in [ITU-T Y.2701] and VPN specific security requirements as described in clause 7.

Appendix I

Scenarios of VPN services in NGN, including the mobile environment

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

This appendix describes scenarios of VPN services in NGN, including the mobile environment.

I.1 Virtual corporate office

Figure I.1 illustrates a VPN scenario called "virtual corporate office" where a "hub-and-spoke" topology model is used, i.e., a model in which the corporate resources are supported in a central head office site (corresponding to the "hub"), with a number of mobile workers or branch offices (corresponding to the "spokes") connected to the head office site using VPN tunnels provided by the NGN.

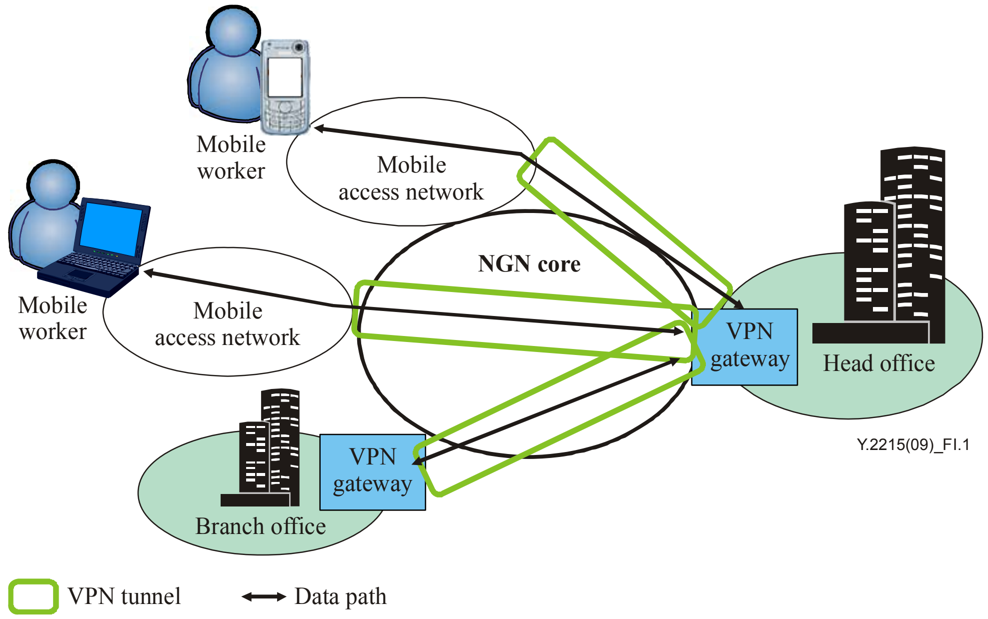

Figure I.1 – Virtual corporate office scenario – "hub-and-spoke" model

Figure I.2 shows another virtual corporate office scenario where a "spoke-to-spoke" topology model is used. This model provides the ability to use temporary VPN tunnels, e.g., between mobile worker terminals and branch office sites.

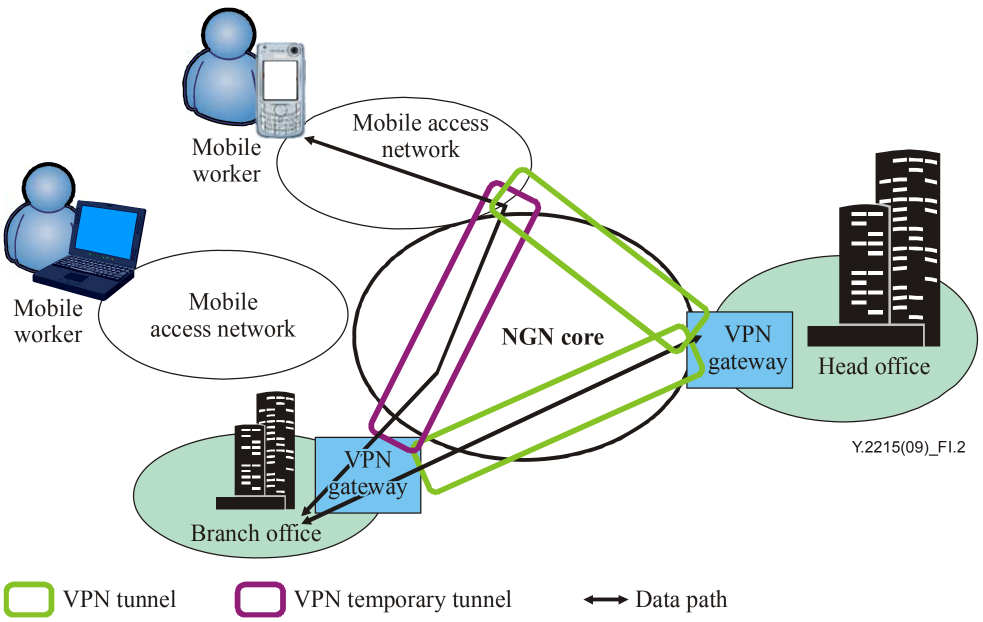

Figure I.2 – Virtual corporate office scenario – "spoke-to-spoke model"

The two models above can be used to provide multiservice VPNs.

Multiservice VPNs allow to deliver multimedia applications with an end-to-end quality of service. They require that the VPN support appropriate QoS mechanisms (for voice, video and data), so that real-time voice and video traffic flows are properly classified and prioritized to support applications efficiently.

Multiservice VPNs support different networking capabilities in order to support VPN user requirements in terms of services, QoS and security.

Multiservice VPNs can support flexible virtual network topologies (e.g., built on a per application basis).

I.2 Personal end-to-end VPN

Figure I.3 illustrates a "personal end-to-end VPN" scenario in which end-to-end VPN tunnels are used between VPN user terminals. This scenario does not require specific capabilities from the NGN apart from allowing the end-to-end tunnels to be carried through the NGN.

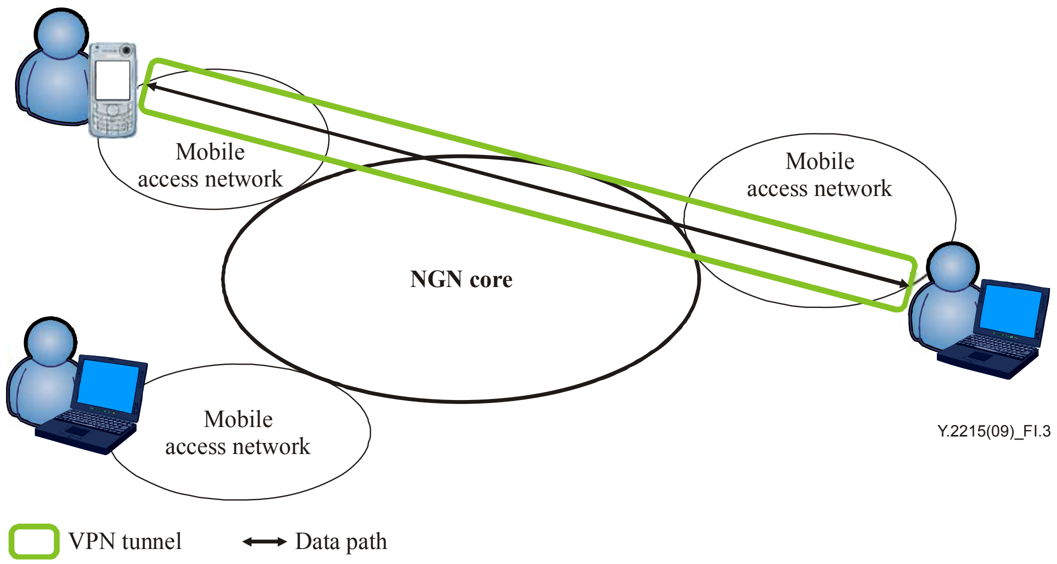

Figure I.3 – Personal end-to-end VPN scenario

I.3 Community-based VPN

Figure I.4 shows a community-based VPN scenario. This scenario consists in using VPNs and groups within those VPNs to form communities (e.g., similar to web-based communities) which the users can join or leave. VPN users using community-based VPN services can make use of different types of terminals, for instance, personal computers, laptops, mobile devices, etc.

Community-based VPNs allow to form different community groups. Community groups are groups of VPN users who are members of the same community, thus having access to the same set of services and applications provided within that community.

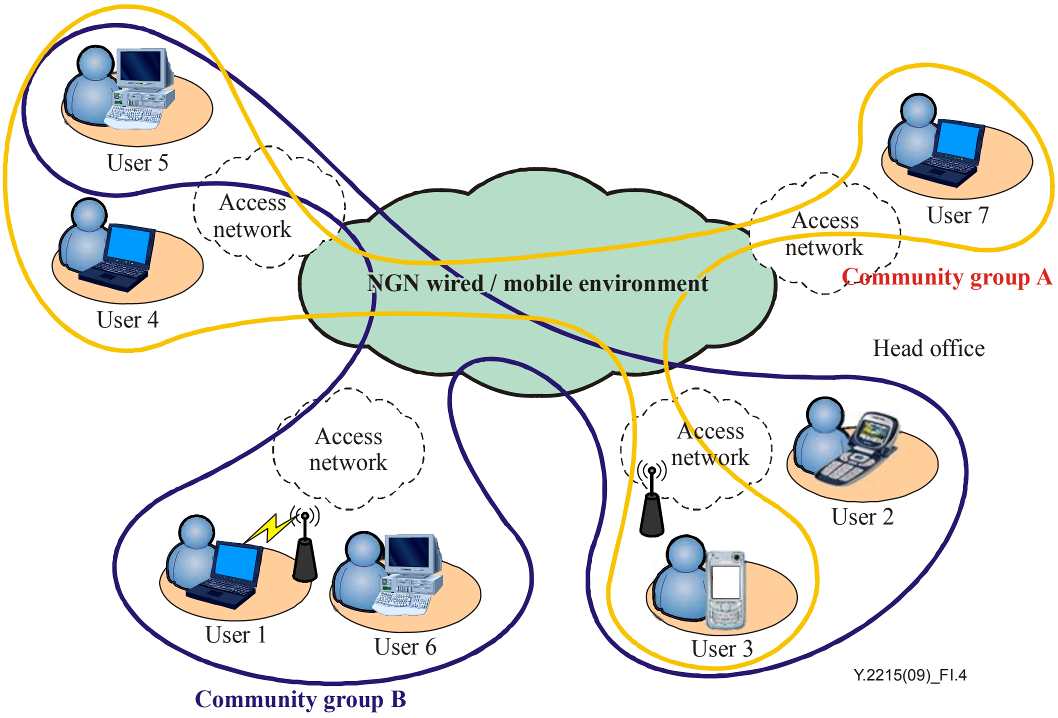

Figure I.4 – Community-based VPN scenario

Community-based VPNs provide management of community groups related-user information as well as other community groups characteristics, for example in the area of security, QoS and applications provided to the community group users.

Bibliography

[b-ITU-T G.1000] Recommendation ITU-T G.1000 (2001), *Communications Quality of Service: A framework and definitions*.

[b-ITU-T G.8081] Recommendation ITU-T G.8081/Y.1353 (2008), *Terms and definitions for Automatically Switched Optical Networks (ASON)*.

[b-ITU-T Q.1742.1] Recommendation ITU-T Q.1742.1 (2002), *IMT-2000 references to ANSI-41 evolved core network with cdma2000 access network.*

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[b-ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN.*

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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009