International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2601

(12/2006)

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

Next Generation Networks

Fundamental characteristics and requirements of future packet based networks

ITU-T Recommendation Y.2601

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

ITU-T Recommendation Y.2601

Fundamental characteristics and requirements of future packet based networks

Summary

This Recommendation provides fundamental characteristics of a future packet based network (FPBN). This Recommendation provides user plane, control plane and management plane requirements for the architecture of an FPBN comprised of transport stratum packet based path layer networks as defined in [G.805], [G.809], [X.200] and [Y.2011].

Source

ITU-T Recommendation Y.2601 was approved on 14 December 2006 by ITU-T Study Group 13 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, 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

			Page
1	Scope		1
2	References		1
3	Definitions		1
4	Abbreviations		2
5	Future packet based networks		3
6	Fundamental characteristics		3
7	Requirements		4
	7.1	Addressing requirements	4
	7.2	Control related requirements	4
	7.3	QoS related requirements	4
	7.4	Network performance management (PM) related requirements	5
	7.5	Protection related requirements	5
	7.6	Payload related requirements	5
	7.7	Operations, administration and maintenance (OAM) related requirements	5
	7.8	Security related requirements	6
	7.9	Control plane requirements	6
	7.10	Management plane requirements	6
	7.11	Basic transport stratum service requirements	6
	7.12	Enhanced transport stratum service requirements	6
Appendix I – Some problems with current packet based networks			7
	I.1	Issues facing network operators	7
BIBLIOGRAPHY			9

ITU-T Recommendation Y.2601

Fundamental characteristics and requirements of future packet based networks

1 Scope

This Recommendation provides fundamental characteristics of a future packet based network (FPBN). This Recommendation provides user plane, control plane and management plane requirements for the architecture of an FPBN comprised of transport stratum packet based path layer networks as defined in [G.805], [G.809], [X.200] and [Y.2011].

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.

[G.805] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

[G.809] ITU-T Recommendation G.809 (2003), *Functional architecture of connectionless layer networks*.

[X.200] ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

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

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

3 Definitions

This Recommendation uses and defines the following terms:

3.1 absolute QoS: See [Y.2111].

3.2 access group: See [G.805].

3.3 address: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.4 connection: See [G.805].

3.5 control plane: See [Y.2011].

3.6 flow: See [G.809].

3.7 flow domain: See [G.809].

3.8 identifier: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects).

NOTE – Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private identifiers are normally not disclosed to third parties).

3.9 user plane: A classification for objects whose principal function is to provide transfer of end-user information: user information may be user-to-user content, or private user-to-user data.

3.10 importance: Importance is the survivability of a given packet compared to all other packets when the network has insufficient resources to service all the traffic.

NOTE – The importance of a given packet is independent of the delay requirements (urgency) of that packet.

3.11 management plane: See [Y.2011].

3.12 off-path: Off-path in a connection-oriented network means it is using a separate trail. Off-path in a connectionless network means it is using a separate server layer trail.

3.13 relative QoS: See [Y.2111].

3.14 subnetwork: See [G.805].

3.15 trail: See [G.805].

3.16 urgency: Urgency is how fast a packet must get processed in order to meet the requested QoS requirements.

NOTE – The urgency of a packet is conveyed in terms of the performance (delay) it requires and a packet's urgency is independent of the survivability (importance) of that packet.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

ATM	Asynchronous Transfer Mode
CAPEX	Capital Expenditure
cl-ps	Connectionless packet switched
co-cs	Connection-oriented circuit switched
co-ps	Connection-oriented packet switched
DoS	Denial of Service
FPBN	Future Packet Based Network
FR	Frame Relay
IP	Internet Protocol
mp-t-mp	Multipoint-to-multipoint
MTU	Maximum Transmission Unit
OAM	Operations, Administration and Maintenance
OPEX	Operational Expenditure
PHB	Per-Hop Behaviour
PM	Performance Management
PSTN	Public Switched Telephone Network
p-t-mp	Point-to-multipoint
p-t-p	Point-to-point
QoS	Quality of Service

SLA Service Level Agreement

SLS Service Level Specification

VPN Virtual Private Network

5 Future packet based networks

Future Packet Based Networks (FPBNs) provide the topmost layer(s) of the transport stratum as defined in [Y.2011].

Further ITU-T Recommendations and other ITU-T documents are expected to provide more detailed requirements, architecture and protocols based on the FPBN fundamental characteristics and requirements within this Recommendation.

6 Fundamental characteristics

This clause provides objectives for an FPBN in terms of the fundamental characteristics. The main objectives are provided below.

An FPBN is expected to:

- Provide both connectionless (cl-ps) and connection-oriented (co-ps) services for multiple client types.
- Efficiently support point-to-point (p-t-p) and point-to-multipoint (p-t-mp) services.
- Support at least absolute quality of service (QoS) in the co-ps mode (if a co-ps mode is provided).
- Interwork and coexist with current cl-ps and co-ps packet networks.
- Support arbitrary network topologies and be able to expand bandwidth, topology, number-of-customers and number-of-services incrementally.
- Detect, and recover from, facility and equipment failures and performance degradation as appropriate to the requirements of the service.
- Offer the appropriate operations, administration and maintenance (OAM) functions for each plane.
- Completely secure the internal control and management plane traffic from external attack and ensure that it remains secure and stable under situations of extreme stress.
- Secure the management plane to prevent access to control and management functions by unauthorized users.
- Be able to accommodate new traffic types.
- Support mechanisms to allow statistical multiplexing for efficiency.
- Support lawful interception of FPBN services. The requirements for lawful interception in NGN are described in other ITU-T Recommendations.
- Support accounting functions by being able to monitor at least network utilization and performance parameters.
- Provide the ability to distinguish between urgency (delay) and importance (survivability).
- Support services that require in-order delivery of packets.
- Provide harmonized and consistent means of referring to user plane access points.
- Provide traffic user plane defect detection and handling (OAM) that is not reliant on the control and/or management planes and is not a function of the nature of the client being transported.

- Support mechanisms to harmonize trail or connection setup and teardown with OAM activation and deactivation.
- Support mechanisms to avoid traffic impact during reconfiguration.
- Attempt to keep traffic flowing while recovering from failures.
- Only deliver traffic from the intended source/ingress to the intended destination(s)/egress(es) except under extremely rare multiple failure conditions.
- Support emergency services.
- Be scalable and reliable.
- Support mechanisms to maintain the separation between user traffic flows as appropriate for the FPBN service that is being provided.

Additionally, an FPBN:

- Should efficiently support multipoint-to-multipoint (mp-t-mp) services.
- Should allow a smooth migration from current cl-ps and co-ps packet networks.
- Should support logical separation of control, management and user planes.
- Should support off-path control and management planes.

7 Requirements

This clause provides requirements based on the objectives provided in clause 6.

7.1 Addressing requirements

This clause provides addressing related requirements for an FPBN. These requirements apply to the network, not necessarily to the user packet itself.

An FPBN is expected to support:

- The identification of a packet's source and its destination within the FPBN in the cl-ps mode.
- The identification of a connection's source within the FPBN in the co-ps mode at the connection's destination.

Additionally, an FPBN:

- Should support FPBN addressing that is disjoint from any client addressing.

7.2 Control related requirements

This clause provides control related requirements for an FPBN.

An FPBN is expected to support:

- Mechanisms to safeguard against persistent (i.e., looping) traffic units in the cl-ps mode.
- Mechanisms to safeguard against co-ps connections containing forwarding loops.
- Mechanisms to ensure the integrity of the control information (e.g., header checksum).

Additionally, an FPBN:

- Should facilitate the in-order delivery of the traffic unit.

7.3 QoS related requirements

This clause provides QoS related requirements for an FPBN.

An FPBN:

- May support queuing priority, which can be implicit or explicit.

- May support discard priority, which can be implicit or explicit.

7.4 Network performance management (PM) related requirements

This clause provides PM related requirements for an FPBN.

An FPBN is expected to:

- Suspend any network performance measurements (for both directions of the trail or connection) if either direction of a bidirectional trail or connection enters the unavailable state.
- Support network performance monitoring (PM) including availability, packet loss, delay and jitter between any two points in the network.

Additionally, an FPBN:

- Should provide logging of FPBN utilization as appropriate for the FPBN services that are supported.
- May provide utilization information on links and nodes.

7.5 Protection related requirements

This clause provides protection related requirements for an FPBN.

An FPBN:

- May support mechanisms to recover from equipment or facility failures.

7.6 Payload related requirements

This clause provides payload related requirements for an FPBN.

An FPBN is expected to:

- Deliver packets in-sequence for the connection-oriented mode of operation.

Additionally, an FPBN:

- May support mechanisms for dynamically discovering the maximum transmission unit (MTU) of a path or connection across an FPBN.
- May support mechanisms to enable the in-sequence delivery of packets for the connectionless mode of operation.
- May support mechanisms to ensure the integrity of the adapted information.

7.7 Operations, administration and maintenance (OAM) related requirements

This clause provides OAM related requirements for an FPBN.

An FPBN is expected to support:

- Simple OAM mechanisms to detect and handle defects.
- OAM mechanisms that are agnostic about the client layer that the FPBN is carrying (i.e., management of the server layer is independent of the client that is being transported).
- OAM defect detection and handling in the traffic user plane.
- OAM defect detection and handling (e.g., defect indication to the trail termination) on a unidirectional basis in the traffic user plane in the co-ps mode.
- The appropriate consequent actions (after defect detection) at a trail termination sink (e.g., suppression of client traffic, defect indication to the client and defect indication to the trail termination source) for co-ps and co-cs clients.

7.8 Security related requirements

This clause provides security related requirements for an FPBN. The intent is to protect against and detect unauthorized end stations but not unauthorized users on authorized end stations.

An FPBN is expected to provide:

- Mechanisms to protect the control plane communications from security threats.
- Mechanisms to protect the management plane communications from security threats.

7.9 Control plane requirements

This clause provides control plane related requirements for an FPBN.

An FPBN is expected to:

- Support a control plane that is independent of any particular client layer control plane.
- Support an unambiguous and reliable means of distinguishing control plane packets from user plane packets and management plane packets.
- Allocate resources to control plane packets such that user plane traffic, regardless of the amount, cannot cause control functions to become inoperative.
- Detect and recover from control plane failures and degradation as appropriate to the requirements of the service.

7.10 Management plane requirements

This clause provides management plane related requirements for an FPBN.

An FPBN is expected to:

- Support a management plane that is independent of any particular client layer management plane.
- Support an unambiguous and reliable means of distinguishing management plane packets from user plane packets and control plane packets.
- Allocate resources to the management plane packets such that user plane traffic, regardless of the amount, cannot cause management functions to become inoperative.

7.11 Basic transport stratum service requirements

This clause provides basic transport stratum service requirements for an FPBN.

An FPBN is expected to support:

- Point-to-point transport stratum services without adaptation.
- Point-to-point transport stratum services including adaptation functions.
- Point-to-multipoint transport stratum services including adaptation functions.

7.12 Enhanced transport stratum service requirements

This clause provides enhanced transport stratum service requirements for the FPBN.

An FPBN is expected to support:

- Connection-oriented transport stratum services with absolute QoS assurance.
- Transport stratum services with relative QoS.

Additionally, an FPBN:

- Should support multipoint-to-multipoint transport stratum services including adaptation functions.

Appendix I

Some problems with current packet based networks

Network operators are now facing a major turning point in the evolution of their many and various service-dedicated network platforms (such as PSTN, ATM, FR, Internet backbone, IP VPN, etc.) towards simpler, more converged connectionless and connection-oriented common service networks. Such a network is expected to be robust, carrier-scale, and flexible, while at the same time optimizing both capital expenditures (CAPEX) and operational expenditures (OPEX).

I.1 Issues facing network operators

Current cl-ps networks have the advantage that they provide a relatively simple operational model, and the disadvantage that they are unable to provide hard end-to-end QoS guarantees in a cost-effective way. Current co-ps networks have the advantage that they can provide guaranteed performance, but possibly at a relatively higher operational complexity. Operators therefore expect that both cl-ps and co-ps modes be supported in order to be able to provide all the services that their customers require.

I.1.1 Support for different traffic types

Network operators expect a scalable architecture that:

- Enables the provision and guarantee of service level specifications (SLS).
- Is 'designed for uncertainty'.
- Provides for different traffic types and their associated service differentiation mechanisms.

Further, in order to provide such QoS based services, a network is expected to provide a mechanism (virtual or otherwise), which provides for the logical separation of different traffic classes associated with different traffic.

I.1.2 Protecting the control and management planes for user plane traffic

Network operators expect that their control and management infrastructure be protected from user traffic. See I.1.5 for an additional discussion of security. Thus, a network architecture is expected to provide the capability to separate the various planes in a particular mode (e.g., cl-ps, co-ps, or co-cs). An example is the separation of data plane from control plane in the SS7 architecture.

I.1.3 Guaranteeing and charging for service level agreements (SLAs)

As broadband access penetration increases and new applications emerge, the question of how to deliver QoS based services, along with the mechanisms for charging for these services has become increasingly important. To this end (and at the very least), network operators will want to:

- Guarantee fair access to shared resources in the access network.
- Control load distribution to avoid focused overload in the core.
- Support hard guarantees to customers.
- Support pricing of different classes.

Any QoS architecture is expected to provide for these functions. It is important to note that in general, the QoS functions described above are characterized by their end-to-end behaviour. However, while QoS architectures such as the IETF's differentiated services (DS) architecture [b-RFC 2475] define an end-to-end QoS model, the DS model itself is described in terms of per-hop behaviours (PHBs) and edge traffic conditioning, and network operators may feel that the DS model is insufficient to provide the required end-to-end QoS guarantees.

I.1.4 The need to ensure emergency services get through and are maintained

Network operators are expected to ensure that emergency services (e.g., 112 and 911 emergency calls) are established and are not dropped under conditions of resource shortfall. A related problem in current QoS approaches is the inability to distinguish between urgency and importance.

I.1.5 Provide adequate security

Network operators expect their infrastructure to be secure. However, architectures that carry control and management plane information in-band in a shared user plane, such as in IP networks, can offer greater potential for attacks against an operator's network infrastructure. Such attacks include classical security attacks (hijacking, privacy, non-repudiation, etc.), as well as attacks on network availability (e.g., denial of service (DoS) attacks).

I.1.6 Identification, location and remediation of faults (OAM)

Clearly, network operators will expect to have the ability to rapidly detect, locate, and remediate network faults (preferably proactively, i.e., before the customer notices). However, certain architectural choices can make such rapid fault remediation difficult or impossible. For example, consider the case of IP networks, where control and management information is carried in-band. In this case, it can be difficult or impossible to rapidly locate, diagnose, and repair certain classes of faults (in particular, those faults which have the property that the fault itself prevents fault detection, location, or repair).

I.1.7 Performance monitoring

Network operators also expect to have the ability to monitor the performance of their networks and the services they provide. The same architectural choices that can cause fault remediation to be difficult (or impossible) can cause similar problems for performance monitoring.

BIBLIOGRAPHY

[b-RFC 2475] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

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, 2007