International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2616

(08/2014)

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

Next Generation Networks – Packet-based Networks

Interworking mechanisms in public packet telecom data networks

Recommendation ITU-T Y.2616

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
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	**Y.2600–Y.2699**
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.2616

Interworking mechanisms in public packet telecom data networks

Summary

Constituting a hierarchical packet data network which can meet requirements of future packet based networks (FPBN), public packet telecom data networks (PTDN) provide efficient interworking mechanisms with other packet data networks (PDN), e.g., IP networks and other PTDNs. Recommendation ITU-T Y.2616 illustrates five typical PTDN interworking scenarios and relevant interworking frameworks, interworking mechanisms and corresponding interworking procedures on the data plane, control plane and management plane.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2616	2014-08-29	13	11.1002/1000/12282

Keywords

PTDN, interworking mechanism, interworking framework, data plane, control plane, management plane.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

Page

Recommendation ITU-T Y.2616

Interworking mechanisms in public packet telecom data networks

1 Scope

This Recommendation defines the interworking scenarios, interworking frameworks, interworking mechanisms and corresponding interworking procedures on the data plane, control plane and management plane as well as interworking security considerations relating to public packet telecom data networks (PTDNs).

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 Y.1401] Recommendation ITU-T Y.1401 (2008), *Principles of interworking*.

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

[ITU-T Y.2615] Recommendation ITU-T Y.2615 (2012), *Routing mechanisms in public packet telecommunication data networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 control plane [ITU-T Y.2011]: The set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control.

3.1.2 data plane [ITU-T Y.2011]: The set of functions used to transfer data in the stratum or layer under consideration.

3.1.3 interworking [ITU-T Y.1401]: The term "interworking" is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication.

3.1.4 interworking function [ITU-T Y.1401]: These functions are referred to in the interworking definition, which include the conversion between protocols and the mapping of one protocol to another. The functionality required between networks can be separated from the functionality, if any, required in end system.

3.1.5 management plane [ITU-T Y.2011]: The set of functions used to manage entities in the stratum or layer under consideration, plus the functions required to support this management.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ED	Edge Device
ID	Identifier
IP	Internet Protocol
IWF	Interworking Function
MC	Multicast
McID	Multicast Identifier
NMS	Network Management System
NNI	Network to Network Interface
OAM	Operation, Administration and Maintenance
PDN	Packet Data Network
PTDN	Public packet Telecom Data Network
QoS	Quality of Service
VPN	Virtual Private Network
VPNID	Virtual Private Network Identifier

5 Conventions

In this Recommendation, the following conventions are used:

The keywords "**is required to**" and "**are required to**" indicate a requirement or requirements which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended to**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor can optionally provide the feature and still claim conformance with the specification.

6 Interworking scenarios

6.1 Interworking between two peer PTDNs

In the scenario shown in Figure 6-1, two peer PTDNs that belong to different operators need to interwork with each other and the interworking process is limited to these two PTDNs.

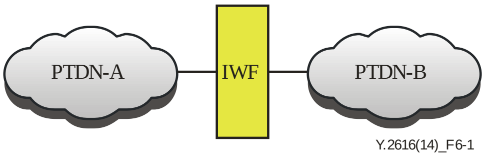

Figure 6-1 – Interworking between two peer PTDNs

6.2 PTDNs interworking across another PTDN

In the scenario shown in Figure 6-2, two PTDNs that belong to different operators (or different private networks) interwork with each other across a third PTDN.

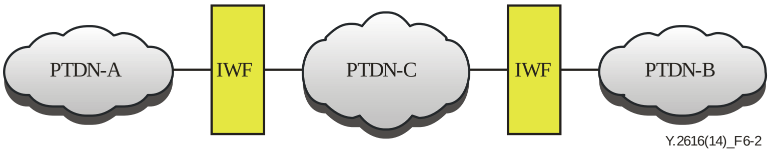

Figure 6-2 – PTDNs interworking across another PTDN

6.3 PTDNs interworking via an IP network (or other PDN)

In the scenario shown in Figure 6-3, two separated PTDNs interwork via an IP network (or other PDN). The IP network (or other PDN) provides a kind of tunnel mechanism between two PTDNs. The data packets from the sending PTDN are encapsulated in an IP network (or other PDN) tunnel, they are then sent to the receiving PTDN and are de-capsulated at the border of the receiving PTDN.

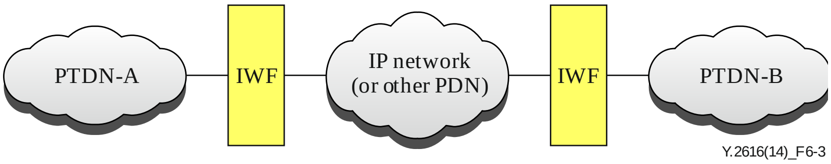

Figure 6-3 – PTDNs interworking via an IP network (or other PDN)

6.4 Interworking of two IP networks (IP islands) via a PTDN

In the scenario shown in Figure 6-4, two separated IP networks (or other PDNs) interwork via a PTDN that provides a kind of tunnel mechanism between the two IP networks (or other PDNs). The data packets from the sending IP network (or other PDN) are encapsulated in a PTDN tunnel, they are then sent to the receiving IP network (or other PDN) and are then de-capsulated at the border of the receiving IP network (or other PDN).

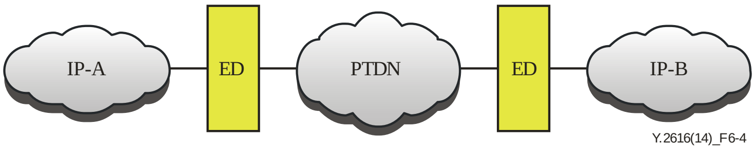

Figure 6-4 – Interworking of two separated IP networks (or other PDNs) via a PTDN

6.5 Interworking between a PTDN and a PDN

The interworking scenario shown in Figure 6-5 involves service interworking between the service terminals of an IP network (or other PDN) and the service terminals of a PTDN.

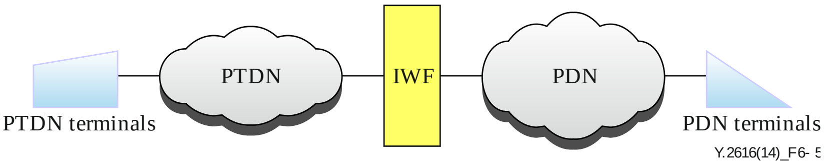

Figure 6-5 – Service interworking between a PTDN and a PDN

7 Two peer interworking PTDNs

Figure 7-1 provides a general framework of two peer PTDNs interworking.

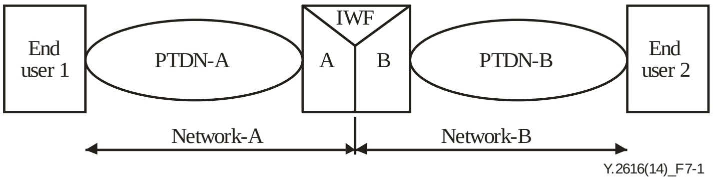

Figure 7-1 – Two peer PTDNs interworking framework

In this figure, IWF indicates the interworking function module. All data need to traverse the IWF module when two peer PTDNs that belong to different operators (or private networks) interwork with each other. An interworking function module comprises a data plane, a control plane and a management plane.

7.1 Interworking requirements

When two peer PTDNs are interworking, the following interworking requirements apply:

– Routing information is required to be exchanged between PTDN-A and PTDN-B.

– The QoS guarantee mechanisms of PTDN-A and PTDN-B are required to be supported in the IWF module.

– Each PTDN has its own independent virtual network management mechanism and virtual private network identifier (VPNID) assignment mechanism. The VPN is required to be terminated on the IWF module and the VPNID is required to be translated on the IWF module.

– Each PTDN has its own independent multicast management mechanism and multicast identifier or McID assignment mechanism. The multicast is required to be terminated in the IWF and the McID is required to be translated by the IWF.

– If network alarm information needs to be transferred, relevant alarm parameters are required to be translated via the IWF based on the local PTDN alarm management mechanism.

– If the network operation, administration and maintenance (OAM) information needs to be transferred, the relevant OAM parameters are required to be translated on IWF based on the local PTDN OAM mechanism.

7.2 Data plane interworking

Each PTDN has its own independent virtual network identifiers (VPNID). The VPNID is required to be translated when crossing an IWF.

Each PTDN has its own independent multicast identifiers (McID). The McID is required to be translated when crossing an IWF.

7.3 Control plane interworking

7.3.1 Addressing and routing

Two peer PTDNs adopt the same address mechanism and share the same address space. The two peer networks exchange routing information with each other and process this information. The updated routing information is then deployed by the network management system (NMS) or by a dominant node as defined in [ITU-T Y.2615].

7.3.2 Control signalling

In connection-oriented mode, when permanent connection(s) can be used, control signalling interworking is not required. In the case where two networks provide non-permanent connections, the IWF provides network to network interface (NNI) functions to intercept the control signalling and map the corresponding parameters and to generate and forward a new control signalling message.

In connectionless mode, if pre-provisioned virtual networks are available, interworking for control signalling is not required. In the case where two networks provide flexible virtual network service by control signalling, a virtual network across both networks and control signalling is required. In this case, the IWF provides NNI functions to intercept the control signalling, map the corresponding parameters and generate a new control signalling message to the other network. The information to be translated at the IWF includes:

– the VPNID in VPN control signalling;

– the McIDin multicast control signalling.

When the VPN or multicast is set up successfully in the destination network, the destination side of the IWF is required to respond with the new VPNID or McID to the source side of the IWF.

7.4 Management plane interworking

In the case where two peer PTDNs belong to different operators and their network management systems are independent, each operator takes charge only of its own PTDN. Each network management system (NMS) manages its own side of the IWF. For example, the network management system of PTDN-A manages and controls side A of the IWF, but does not manage or control side B of the IWF or the network behind side B.

7.5 OAM interworking

PTDN OAM messages contain performance, defect and protection switching information for a connection in connection-oriented mode, or for a virtual data plane (e.g., VPN) in connectionless mode.

Each network has its own OAM domain. Generally OAM messages do not cross the network's boundary. When end-to-end OAM is required, the IWF will intercept, process and re-encapsulate the OAM messages based on the local network OAM mechanism.

8 Interworking across a PTDN

Interworking across a PTDN is shown in Figure 8-1.

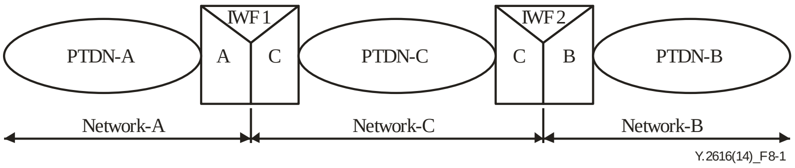

Figure 8-1 – Interworking across a PTDN

In this framework, there are three interworking cases:

– Network PTDN-A and Network PTDN-C

These two networks are peer networks. A PTDN-A user can communicate with a PTDN-C user across IWF1 which has the same functions as the IWF described in clause 7 of this Recommendation.

– Network PTDN-B and Network PTDN-C

These two networks are peer networks. A PTDN-B user can communicate with a PTDN-C user across IWF2 which has the same functions as the IWF described in clause 7 of this Recommendation.

– Network PTDN-A and Network PTDN-B

PTDN-A and PTDN-B reside on either side of the third network, PTDN-C. There are two modes to enable interworking between PTDN-A and PTDN-B:

- Mode 1: PTDN-C works as a transport network to provide a transport service between PTDN-A and PTDN-B. PTDN-C provides one or more virtual circuit(s) or VPN(s) as tunnel(s) to connect PTDN-A and PTDN-B. Since side A of IWF1 and side B of IWF2 are logically connected directly, these two half parts work together to provide the same functions with the IWF described in clause 7 of this Recommendation.
- Mode 2: PTDN-A will transfer relevant information to PTDN-C and PTDN-C will transfer relevant information to PTDN-B, so there are two translation times in this mode (i.e., two times when information is translated across an IWF). Each translation time will adhere to the mechanism described in clause 7 of this Recommendation.

When operating in mode 1, PTDN-A and PTDN-B are two peer networks and PTDN-C provides the tunnel service for interworking, so it operates in the same way as the interworking mechanism described in clause 9 of this Recommendation.

Clauses 8.1 to 8.5 focus on mode 2.

8.1 Interworking requirements

The following interworking requirements apply when two PTDNs interwork across a third PTDN (see Figure 8-1):

– Routing information is required to be exchanged. PTDN-C learns PTDN-A and PTDN-B routing information through IWF1 and IWF2, then advertises the necessary PTDN-B routing information to PTDN-A through IWF1 and advertises the necessary PTDN-A routing information to PTDN-B through IWF2.

– The QoS guarantee mechanisms of PTDN-A and PTDN-C are required to be supported in IWF1. The QoS guarantee mechanisms of PTDN-C and PTDN-B are required to be supported in IWF2.

– Each PTDN has its own independent virtual network management mechanism and VPNID assignment mechanism. The VPNID is required to be translated on each IWF.

– Each PTDN has its own independent multicast management mechanism and McID assignment mechanism. The McID is required to be translated on each IWF.

– If network alarm information needs to be transferred, relevant alarm parameters are required to be translated on IWF based on the local PTDN alarm management mechanism.

– If network OAM information needs to be transferred, relevant OAM parameters are required to be translated on IWF based on the local PTDN OAM mechanism.

8.2 Data plane interworking

Each PTDN has its own independent identifier for each virtual network and each virtual private network identifier (VPNID) is required to be translated on an IWF. Each PTDN has its own independent multicast identifiers (McID) and the McID is required to be translated on an IWF.

In this framework, the VPNID or McID will be translated twice.

8.3 Control plane interworking

8.3.1 Addressing and routing

All three networks adopt the same address mechanism and share the same address space. The two networks, PTDN-A and PTDN-B, will exchange the routing information through the PTDN-C network.

8.3.2 Control signalling

At each IWF, the same functions described in clause 7.3.2 of this Recommendation should be supported.

8.4 Management plane interworking

In principle, the network management of a PTDN is independent. Each network management system can only manage its own side of an IWF. For example, the network management system of PTDN-A manages and controls side A of IWF1 and does not manage or control side C of IWF1 or those networks behind side C.

8.5 OAM interworking

The OAM interworking mechanism is described in clause 7.5 of this Recommendation.

9 PTDNs interworking via an IP network (or other PDN)

Figure 9-1 shows two PTDNs interworking via an IP network (or other PDN).

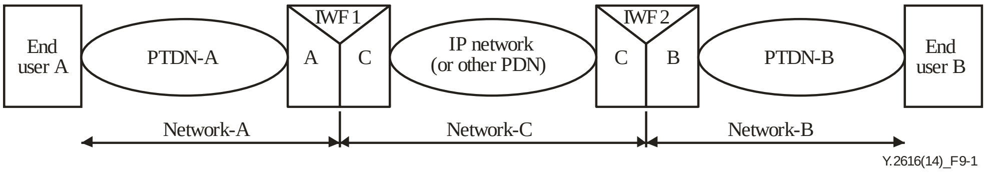

Figure 9-1 – Framework for PTDN's interworking via an IP network (or other PDN)

9.1 Interworking requirements

When two PTDNs interwork via an IP network (or other PDN), the following interworking requirements apply:

– Routing information is required to be exchanged between PTDN-A and PTDN-B.

– The IP network or other PDN network is recommended to support the traffic contracts and the QoS commitments made to PTDN-A and PTDN-B.

– Each PTDN has its own independent virtual network management mechanism and VPNID assignment mechanism. The VPNID is required to be translated on an IWF.

– Each PTDN has its own independent multicast management mechanism and McID assignment mechanism. The McID is required to be translated on an IWF.

– If the network alarm information needs to be transferred, relevant alarm parameters are required to be translated on IWF based on the local PTDN alarm management mechanism.

– If network OAM information needs to be transferred, relevant OAM parameters are required to be translated on IWF based on the local PTDN OAM mechanism.

9.2 Data plane interworking

A PTDN packet crossing Network-C will be encapsulated into one or more IP packets (or PDN packets) when entering a tunnel and will be de-capsulated into a PTDN packet at the end of the tunnel. The PTDN packet, as the payload of the IP or PDN packets, will be transported without change in the tunnel. When a PTDN packet enters the destination PTDN across side A of IWF1 or side B of IWF2, the VPNID or McID in the packet's header will be translated.

9.3 Control plane interworking

9.3.1 Addressing and routing

When two peer PTDNs adopt the same address mechanism and share the same address space, the two peer networks will exchange routing information with each other. This routing information is processed and deployed via a routing table per NMS or per a dominant node as defined in [ITU-T Y.2615].

9.3.2 Control signalling

When networks, PTDN-A and PTDN-B, work in connection-oriented mode and permanent connection(s) can be used, control signalling interworking is not required. When these two networks provide each other with non-permanent connections, an IWF provides the NNI function to intercept the control signalling and map the corresponding parameters and then generate and forward a new control signalling message.

When networks, PTDN-A and PTDN-B, work in connectionless mode and if pre-provisioned virtual networks are available, control signalling interworking is not required. When these two networks provide each other with flexible virtual network service by control signalling, IWF provides the NNI functions to intercept the control signalling, map the corresponding parameters and forward the control signalling message. The information to be translated at IWF includes:

– the VPNID in VPN control signalling;

– the McID in multicast control signalling.

When the VPN or multicast set up in the destination network successfully, the destination side of the IWF is required to respond with the new VPNID or McID to the source side of the IWF.

When interworking of control signalling is required, Network-C tunnels and transports the control signalling messages transparently and can optionally transport them in a separated tunnel.

9.4 Management plane interworking

When networks, PTDN-A and PTDN-B, are managed by different operators, each network management system manages and controls its own side of an IWF. For example in Figure 9-1, the network management system of PTDN-A manages and controls the side A of IWF1 and the network management system of PTDN-B manages and controls the side B of IWF2, while the network management system of Network C manages and controls the side C of both IWF1 and IWF2.

When PTDN-A and PTDN-B are managed by the same operator, management messages across Network-C will be transported transparently and can optionally be transported in a separated tunnel.

9.5 OAM interworking

The OAM interworking mechanism is as described in clause 7.5 of this Recommendation.

When OAM interworking is required, Network-C tunnels and transports OAM messages transparently.

10 Two IP networks (IP islands) interworking via a PTDN

Interworking of two separated IP networks (or other PDNs) via a PTDN is shown in Figure 10-1. IP networks are the most popular networks and PTDNs are required to support IP service access.

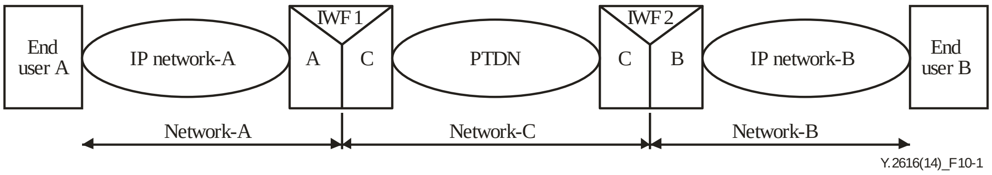

Figure 10-1 – Interworking framework of two separated IP networks (or other PDNs) via a PTDN

10.1 Interworking requirements

When two IP networks (or other PDNs) interwork via a PTDN, the following interworking requirements apply:

- Routing information is required to be exchanged between IP Network-A and IP Network-B.
- The PTDN network is recommended to support the traffic contracts and the QoS commitments made to the interworked Network-A and Network-B.
- IP network alarm information is required to be transferred transparently.

10.2 Data plane interworking

The PTDN provides one or several tunnel(s) with different transport characteristics. These tunnels connect the two separated IP networks (or other PDNs) and carry different QoS-guaranteed IP (or other PDN) traffic. A PTDN can work in connection-oriented mode and in connectionless mode (not simultaneously). So a tunnel can be a VPN in connectionless mode or a virtual circuit in connection-oriented mode.

10.3 Control plane interworking

IP network (or other PDN) network control signalling messages across the PTDN are transported transparently and can optionally be transported in a separated tunnel.

10.4 Management plane interworking

IP network (or other PDN) network management messages are transported transparently and can optionally be transported in a separated tunnel.

10.5 OAM interworking

IP network (or other PDN) OAM messages are transported transparently and can optionally be transported in a separated tunnel.

11 Interworking of a PTDN and a PDN

The interworking framework of a PTDN and a PDN, shown in Figure 11-1, provides end-to-end communication between a PTDN terminal and a PDN terminal.

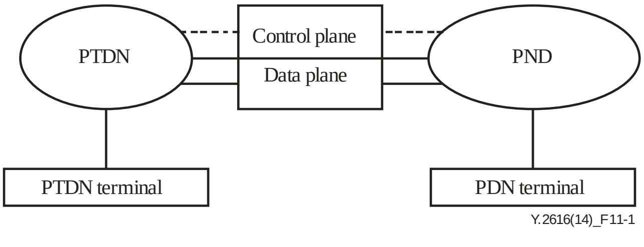

Figure 11-1 – Interworking framework of a PTDN and a PDN

There are two ways to achieve end-to-end connectivity:

- service interworking; and
- superimposition.

Service interworking implements semantically equivalent translation between the PTDN and PDN. If there is sufficient similarity in service characteristics between the PTDN and the PDN then IWF can map equivalent service characteristics between them. Due to lack of exact semantic equivalence, some PTDN services will not be available to PDN users and vice versa.

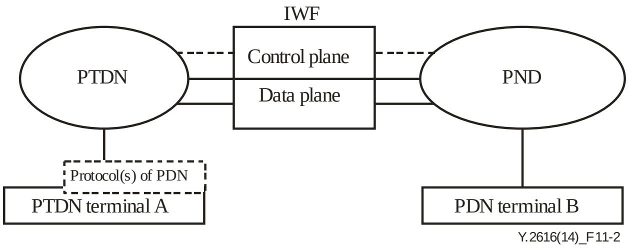

Figure 11-2 – Interworking framework of PTDN and PDN by superimposition

Figure 11-2 illustrates end-to-end connectivity achieved through superimposition. PTDN Terminal A has a PDN protocol stack and a PDN address which is set statically or dynamically. PTDN Terminal A encapsulates service data into PDN packets whose destination address is the address of PDN Terminal B and whose source address is the PDN address of PTDN Terminal A. PTDN Terminal A then re-encapsulates these PDN packets into PTDN packets. When these PTDN packets arrive at the IWF, the IWF de-capsulates the PTDN packets into PDN packets, then transfers these packets to the PDN network.

When PDN Terminal B sends data to PTDN Terminal A, PDN Terminal B encapsulates the service data into PDN packets in which the destination address is the PDN address of PTDN Terminal A. When these PDN packets arrive at the IWF, the IWF encapsulates these packets into PTDN packets in which the destination address is the PTDN address of PTDN Terminal A and then sends them to the PTDN.

12 Security considerations

PTDNs can have direct or indirect connectivity to both untrusted and trusted networks and therefore will be exposed to security risks and threats associated with connectivity to untrusted networks.

These threats to PTDN interworking include:

– unauthorized PTDN access;

– destruction of information and/or related resources (such as VPNID, McID);

– corruption or modification of information (such as control signalling, routing information, etc.);

– disclosure of information (such as control signalling, routing information, etc.);

– interruption of services and denial of services.

Each PTDN is responsible for security within its domain and protects its topology, reachability, and addressing details.

An IWF can provide optional mechanisms:

– to authenticate entities exchanging information across the IWF;

– to block all unauthorized access;

- to guarantee the integrity of the information (such as control signalling, routing information, etc.) exchanged across the IWF;
- to protect the confidentiality of certain types of information that may be required;
- to protect against both malicious attacks as well as unintentionally malfunctioning control entities;
- to forward the control signalling and management messages across an IWF in an isolated, resource guaranteed tunnel, VPN, or virtual channel.

Bibliography

[b-ITU-T I.322] Recommendation ITU-T I.322 (1999), *Generic protocol reference model for telecommunication networks*.

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[b-ITU-T X.323] Recommendation ITU-T X.323 (1988), *General arrangements for interworking between Packet-Switched Public Data Networks (PSPDNs)*.

[b-ITU-T X.371] Recommendation ITU-T X.371 (2001), *General arrangements for interworking between Public Data Networks and the Internet*.

[b-ITU-T Y.1251] Recommendation ITU-T Y.1251 (2002), *General architectural model for interworking*.

[b-ITU-T Y.2601] Recommendation ITU-T Y.2601 (2006), *Fundamental characteristics and requirements of future packet based networks*.

[b-ITU-T Y.2611] Recommendation ITU-T Y.2611 (2006), *High-level architecture of future packet based networks*.

[b-ITU-T Y.2612] Recommendation ITU-T Y.2612 (2009), *Generic requirements and framework of addressing, routing and forwarding in future packet-based networks*.

[b-ITU-T Y.2613] Recommendation ITU-T Y.2613 (2010), *General technical architecture for public packet telecommunication data network*.

[b-ITU-T Y.2614] Recommendation ITU-T Y.2614 (2011), *Network reliability in public packet telecommunication data networks*.

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, 2014