International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2614

(08/2011)

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

Next Generation Networks – Smart ubiquitous networks

Network reliability in public telecommunication data networks

Recommendation ITU-T Y.2614

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
Smart ubiquitous 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.3099

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

Recommendation ITU-T Y.2614

Network reliability in public telecommunication data networks

Summary

Recommendation ITU-T Y.2614 identifies the objectives, architecture and mechanisms for network reliability in public packet telecommunication data networks (PTDNs), including a description of link protection, trail protection, network failure detection, protection switching trigger and protection coordination mechanisms.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2614	2011-08-06	13

Keywords

FPBN, link protection, PTDN, reliability, trail protection.

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

Introduction

Network reliability in public telecommunication data networks (PTDN) shall be provided using link protection and trail protection mechanisms. In both protection mechanisms, two of protection types, 1:1 and 1:n protection are considered. In the trail protection mechanism, three routing models can be implemented.

Furthermore, three routing models, dual path routing model, shortest path routing model and alternative routing model, can be used to implement the trail protection in PTDN.

- The dual path routing model pre-calculates two disjoint paths based on ear decomposition, to provide 1:1 protection, from the source node to the destination node based on the network topology and resource information. These are the working path and the protection path.
- The shortest path routing model and the alternative routing model work together to provide 1:n protection.
- The alternative routing model can provide 1:n protection by itself. It can calculate several paths. One of them works as the working path, while the remaining paths will be protection paths.

Recommendation ITU-T Y.2614

Network reliability in public telecommunication data networks

1 Scope

This Recommendation identifies the objectives, architecture and mechanisms for network reliability in public packet telecommunication data networks (PTDNs), including a description of link protection, trail protection, network failure detection, protection switching trigger and protection coordination mechanisms.

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

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

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

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

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 bidirectional protection switching [b-ITU-T I.630]: A protection switching architecture in which, for a unidirectional failure, both directions (of the "trail", "subnetwork connection", etc.), including the affected direction and the unaffected direction, are switched to protection.

3.1.2 hold-off time [b-ITU-T G.870]: The time between declaration of signal degrade or signal fail, and the initialization of the protection switching algorithm.

3.1.3 manual protection [b-ITU-T M.2102]: Recovery is initiated by forced or manual switching to the alternative trail; return to original configuration is done by forced or manual switching to normal.

3.1.4 non-revertive (protection) operation [b-ITU-T G.870]: A protection switching operation, where the transport and selection of the normal traffic signal does not return to the working transport entity if the switch requests are terminated.

3.1.5 protection switching [b-ITU-T I.630]: A network survivability technique with dedicated protection resource allocation policy.

3.1.6 public packet telecommunication data network (PTDN) [ITU-T Y.2613]: A packet data network designed for the NGN transport stratum, which should be secure, trustworthy, controllable, and manageable, can meet all the requirements described in [ITU-T Y.2601]. PTDN is a hierarchical network, which can be subdivided into several network layers.

3.1.7 revertive (protection) operation [b-ITU-T G.870]: A protection switching operation, where the transport and selection of the normal traffic signal (service) always returns to (or remains on) the working transport entity if the switch requests are terminated; i.e., when the working transport entity has recovered from the defect or the external request is cleared.

3.1.8 switching time [b-ITU-T G.870]: Time between the initialization of the protection switching algorithm and the moment the traffic is selected from the standby transport entity.

3.1.9 trail protection [b-ITU-T G.780]: Normal traffic is carried over/selected from a protection trail instead of a working trail if the working trail fails, or if its performance falls below a required level.

3.1.10 unidirectional protection switching [b-ITU-T I.630]: A protection switching architecture in which, for a unidirectional failure (i.e., a failure affecting only one direction of transmission), only the affected direction (of the "trail", "subnetwork connection", etc.) is switched to protection.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 1:1 protection: A protection mechanism in which the traffic is sent only on the working path or on the protection path.

3.2.2 alternative routing model: A routing model providing multiple paths between a source public packet telecommunication data network (PTDN) node and a destination PTDN node.

NOTE – These paths are not required to be deterministic and unique. In this model, the sending path and the receiving path are not necessarily composed of the same nodes and links.

3.2.3 dual path routing model: A routing model providing two totally disjoint paths between a source public packet telecommunication data network (PTDN) node and a destination PTDN node.

NOTE – The two paths may not be the shortest paths.

3.2.4 link protection: A point-to-point protection mechanism.

NOTE – Protection switching and re-routing should not be initiated at the network layer unless link protection has failed.

3.2.5 shortest path routing model: A routing model providing a deterministic and unique path, which is the shortest path from a source public packet telecommunication data network (PTDN) node to a destination PTDN node.

NOTE – In this model, the path from the source node to the destination node results in the same as the path from the destination node to the source node.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IP	Internet Protocol
OAM	Operations, Administration and Maintenance
PTDN	Public packet Telecommunication Data Network
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy

WDM	Wavelength Division Multiplexing

5 Network reliability objectives

This clause describes the network reliability objectives for a PTDN.

5.1 Switching time

According to routing models supported in PTDN, service traffic can be switched from the working path to a protection path when a link or node fails. The switching time consists of two parts: one is the time that the node has received the notification message of network failure sent by the node nearest to the point of failure; the other is the time that protection switch has been completed from working path to protection path.

In PTDN, switching time should be no more than 50 ms.

5.2 Hold-off time

The PTDN is a layer network. A protection scheme is provided by each layer. So, the protection coordination between layers must be considered, in order to avoid back and forth protection switching. Hold-off time is useful for inter working of protection schemes. A hold-off timer is started when a defect condition is declared and its duration of the timer can be configured. When the hold-off timer expires, protection switching is initiated if a defect condition is still present at this point. Note that a defect condition does not have to be present for the entire duration of the hold-off period; only the state at the expiry of the hold-off timer is relevant.

In a PTDN, the hold-off time should be larger than the switch time of the lower network layer.

5.3 Protection types

The protection types can be either 1:1 protection type or 1:n protection type. Service traffic is transmitted either on the working path or on the protection path. In the 1:1 protection type, there are two disjoint paths between the source node and the destination node. One of them is the working path, the other one is the protection path. In the 1:n protection type, there are 1+ n paths between the source node and the destination node, one of them is the working path, the other n paths are protection paths.

In PTDN, 1:1 protection type and 1:n protection type of trail protection are recommended.

5.4 Switching types

There are two switching types, unidirectional switching and bidirectional switching. In unidirectional switching, the traffic sending path and the receiving path are different, so only the affected path is switched. In bidirectional switching, the traffic sending path and the receiving path usually are the same, so both paths can be switched.

In PTDN, unidirectional protection switching and bidirectional protection switching are recommended to be provided.

5.5 Operation types

There are two protection operation types, non-revertive operation type and revertive operation type. In non-revertive types, the service will not switch back to the working path when the working path is recovered. The service will be switched back to the working path only if the current protection path fails. In revertive types, the service will always switch back to the working path if the working path is recovered.

In PTDN, revertive and non-revertive operation types should be provided.

5.6 Manual protection

In PTDN, automatic protection switching and manual protection switching are supported. The operator can make manual protection switching, with manual protection switching usually having a higher priority than automatic protection switching.

5.7 Switch initiation criteria

In PTDN, the following protection switching initiation criteria are supported:

- externally initiated commands (e.g., in case of manual control);
- link or node on the working path fails, the protection path is ready and the hold-off timer has expired;
- the working path is recovered, in the revertive operation type.

6 Network reliability architecture

In PTDN, link protection and trail protection are required as follows:

- 1:1 protection and 1:n trail protection shall be provided;
- unidirectional and bidirectional switching types shall be supported; and
- revertive and non-revertive operation shall be supported.

6.1 Link protection

A protection scheme is provided by each layer in PTDN which includes many layers. Link protection works on the link layer. Link protection is a point-to-point protection mechanism. Protection switching and rerouting should not be initiated at the network layer unless link protection has failed.

The architecture for link protection is as shown in Figure 6-1.

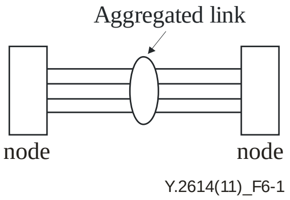

Figure 6-1 – Link protection architecture

In PTDN, there are two mechanisms for service traffic distribution on the aggregated links:

1) Traffic is distributed on all the aggregated physical links, but part of every link capability should be reserved, summing up to the capability of one or more links, for protection when one or more links break down.
2) One or more of the aggregated links do not transfer traffic unless one or more of the aggregated links break down.

The end nodes of the aggregated links can detect the failure of certain physical link(s) and distribute the traffic on the failed link(s) to other physical links.

6.2 Trail protection

Trail protection is an end-to-end protection mechanism. At least two paths from the source node to the same destination node should be pre-calculated based on the network topology and resource information in PTDN. One is the working path, the other(s) are the protection path(s).

Consecutive probe packets are used to detect defects of the working path or the protection path. When a network failure notification message has been received, service traffic should switch from the working path to the protection path when the hold-off timer has expired.

The architecture for trail protection is shown in Figure 6-2.

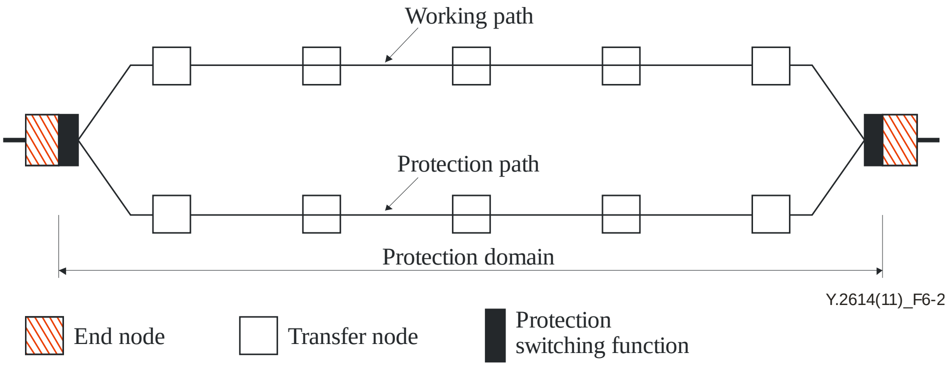

Figure 6-2 – Trail protection architecture

In PTDN, 1:1 protection type and 1:n protection type of trail protection should be provided.

In the 1:1 protection type, the dual path routing model is applied, which will pre-calculate two disjoint paths based on ear decomposition.

In 1:n protection type, there are two ways to implement:

1) The shortest path routing model and the alternative routing model are applied together. The shortest path routing model will provide one working path and the alternative routing model will provide n protection paths.

2) The alternative routing model is applied to calculate several paths; one of them serves as the working path, the remaining paths will be protection paths.

Consecutive probe packets are used to detect defects of a working or protection path. They are inserted at the source of the protection trail and detected and extracted at the sink of the protection trail.

6.3 Switch types

The protection switch types can be unidirectional switch types or bidirectional switch types.

In PTDN, the sending path and receiving path are usually the same, if the route is calculated based on the shortest path routing model or the dual path routing model. In both of these cases, a bidirectional switch is applied. However, the sending path and receiving path may be different if the route is calculated based on an alternative routing model. In this case, a unidirectional switch is applied.

6.4 Operation types

The protection operation types can be a non-revertive operation type or a revertive operation type.

In non-revertive operation types, after the protection switches from the working path to the protection path, the service traffic will not switch back to the working path when the working path is recovered. The service will be switched back to the working path only if the current protection path fails and the working path is recovered.

In the revertive operation type, the service will always switch back to the working path if the working path is recovered. In PTDN, the revertive operation type is recommended.

6.5 Network failure detection mechanism

There are two network failure detection mechanisms in PTDN. One is the link failure detection mechanism. It works at the link layer and detects in real time the status of a link by periodically transmitting link maintenance frames. The other is the trail failure detection mechanism. It works at the network layer and detects in real time the end-to-end connectivity by periodically transmitting OAM packets.

6.6 Protection switching trigger mechanism

Protection switching action should be conducted when:

1) initiated by operator control (e.g., manual switch, forced switch) without a higher priority switch request being in effect;
2) signal failure is declared on the working path, but not on the protection path, and the hold-off timer has expired; or
3) the wait-to-restore timer expires (revertive mode) and signal failure is not declared on the working path.

7 Link protection

In PTDN, a pair of nodes can be connected by multiple physical links to enhance the bandwidths and reliability between them. Multiple physical links should be aggregated as one logical link when calculating the route, and service traffic should be balanced among the multiple physical links according to the link bandwidth. When one or many of the aggregation links fail, service traffic carried by failed link(s) should be transferred to other available links, not switched from working path to protection path unless link protection fails.

In PTDN, link protection fails when:

1) all aggregated physical links break down;
2) the capability of the remaining links cannot meet the requirements of traffic when one or several aggregated links break down.

When link protection fails, a trail protection mechanism will be applied.

8 Trail protection

To implement trail protection in PTDN, three routing models are used. These are dual path routing model, shortest path routing model and alternative routing model.

In connectionless mode, a PTDN node determines the routing model based on the protection field's value, which consists of two bits in the packet header [ITU-T Y.2613]. When a network failure (link or node) occurs or the working paths recover, the value of the protection field is required to be modified.

If the value of the protection field is "00", it means the shortest path routing model is applied. In this case, service traffic may be interrupted when a network failure (link or node) occurs, unless the alternative routing model is applied, in which case, the value of the protection field is required to be modified from "00" to "10". In the alternative routing model, network reachability can be guaranteed but QoS cannot be guaranteed.

If the value of the protection field is "11" or "01", it means the dual path routing model is applied. In this case, service traffic will be switched from the working path to the protection path when network failure (link or node) occurs; or from the protection path to the working path when the working path is recovered in revertive operation type. Correspondingly, the value is required to be modified from "11" to "01" or from "01" to "11". It must be noted that QoS can be guaranteed only if the network resources of the working path and the protection path are exactly the same.

8.1 Dual path routing model

The dual path routing model pre-calculates two disjoint paths from the source node to the destination node based on the network topology and resource information.These are the working path and the protection path. Except for the source node and the destination node, there are other links or nodes common to the working path and the protection path.

Two conditions should be met for network topology in the dual path routing model:

1) every node in PTDN is connected to at least two other nodes;

2) every link in PTDN is a bidirectional link.

Two completely disjoint directed diagrams (see Figure 8-1) can be achieved by ear decomposition.

For more information about ear decomposition refer to Appendix I.

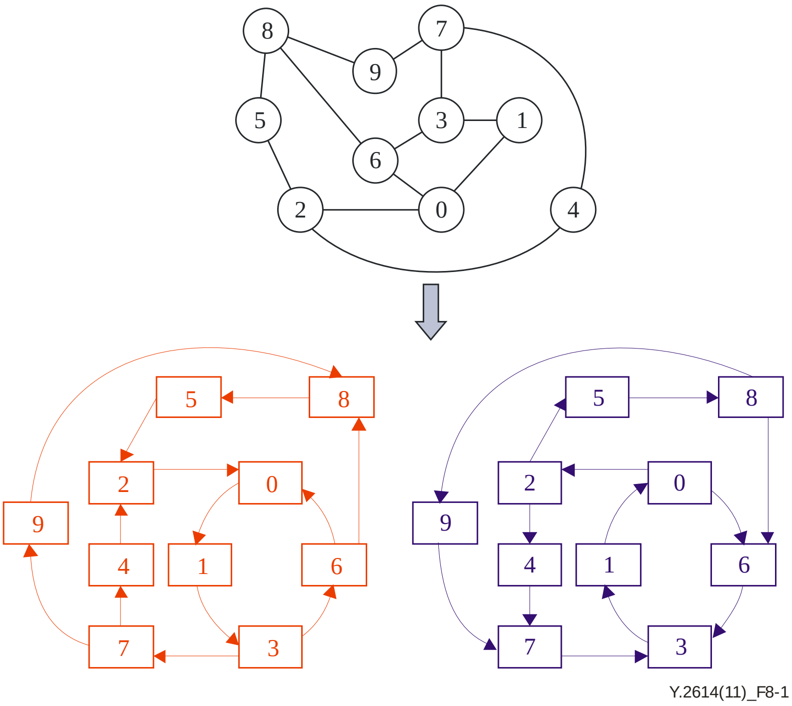

Figure 8-1 – Ear decomposition in dual path routing model

As shown in Figure 8-1, there are two disjoint paths between any two nodes. For example, there are two disjoint paths from node 1 to node 7. One is a working path along nodes 1, 3 and 7. The other is a protection path along nodes 1, 0, 2, 4 and 7.

When the working path fails, the nearest node of this point of failure will send a network failure notification message to the source node. On receipt of the notification message, the source node will switch the traffic from the working path to the protection path. The value of the protection field in the packet header is required to be reset from "11" to "01".

In revertive operation type, if the working path is recovered, service traffic will switch back to the working path; the value of the protection field in the packet header is required to be modified from "01" to "11".

In non-revertive operation type, even if the working path is recovered, service traffic will not switch back to the working path unless the protection path fails.

In the dual path routing model, QoS can be guaranteed when switched from the working path to the protection path or from the protection path to the working path if the network resources on the two paths are the same.

8.2 Shortest path routing model

The shortest path routing model provides a deterministic and unique path, which is the shortest path from the source PTDN node to the destination PTDN node. In this model, the sending path and receiving path must be the same. When there are multiple connections between PTDN domains on the boundary of the domain, only one connection with the highest priority is active.

The value of protection field in the packet header should be set "00" when a packet is transmitted using the shortest path routing model.

The alternative routing model will be applied to provide network reachability in case the shortest path routing model fails. In this case, the value of the protection field in the packet header should be modified to "10" from "00".

8.3 Alternative routing model

In the alternative routing model, many paths are pre-calculated and kept in a routing table; one of them is the working path. If the working path fails, the second route in the routing table will be active. These paths may not be the shortest, and the sending and receiving paths are not required to include the same nodes and links. The alternative routing model can be applied in two cases:

1) The working path is the shortest path; the alternative routing model provides the protection path(s).

   The failure of a node or link, or topology changes may result in the failure of the working path. In this situation, the alternative path routing model will provide the protection path(s). In this case, the value of the protection field in the packet header is required to be modified to "00" from "01".

2) Both the working path and the protection path(s) are provided by the alternative routing model.

   In the alternative routing model, the value of the protection field in the packet header should be set to "01". Many paths from the source node to the destination node will be pre-calculated and stored in the routing table, one of which is used as working path. When the working path fails, the protection path will be chosen from other paths in the routing table. In this case, the value of the protection field in the packet header should not be changed.

In the alternative routing model, network reachability can be guaranteed, but QoS cannot be guaranteed.

9 Protection coordination mechanism

If nodes are connected by multiple aggregated links, when one or many of the aggregated links fail, link protection should be applied first, and if link protection fails, trail protection should be initiated.

Moreover, hold-off time should be provided between the layer protections to avoid back and forth protection switching. For example, if a PTDN is based on the transport network (e.g., SDH, WDM), PTDN protection switching should not be initiated unless the hold-off timer has expired and a defect condition (e.g., link or node failure in the transport layer network) is still present at this point.

10 Security considerations

This Recommendation defines the mechanisms to produce one or several protection paths to protect the working path. The mechanisms are helpful to improve security of a PTDN. The reliability mechanisms described in this Recommendation assume that both working and protection paths are set up at the same time and in the same manner. Given that the setting of either path is performed by the normal PTDN procedures, no additional security risks specific to the reliability mechanisms described in this Recommendation are identified.

In terms of instability when protection applies, a hold-off time and a protection coordination mechanism have already been considered in this Recommendation.

Appendix I

Ear decomposition

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

An ear decomposition D={P0;P1;…;Pr – 1} of an undirected Graph G=(V,E) is a partition of E into an ordered collection of edge-disjoint simple paths P0;P1;…;Pr – 1, called ears, such that:

- P0 is a simple cycle.
- Pi (i>0) is a simple path with the end-points belonging to lower-numbered ears, and with no internal vertices belonging to lower-numbered ears.
- Pi (i>0) may also be a simple cycle. If it is a cycle consisting of only one edge, it is called a trivial ear.

An ear decomposition is called open if and only if there is no cycle for Pi (i>0).

In Figure I.1, the network topology on the left is decomposed into four ears, as shown on the right of Figure I.1. Among them, P_0 is a simple cycle composed of nodes 0, 1, 3 and 6; P_1 is composed of nodes 2, 4 and 7, with end-points 3 and 0 belonging to ear P_0, which is a lower-numbered ear compared to P_1; P_2 is composed of nodes 5 and 8, with end-points 2 and 6 belonging to ears P_1 and P_0 respectively, which are lower-numbered ears compared to P_2; P_3 is composed of node 9, with end-points 7 and 8 belonging to ears P_1 and P_2 respectively, which are lower-numbered ears compared to P_3.

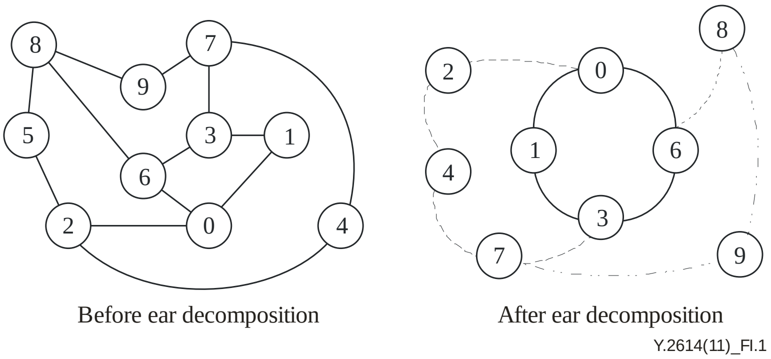

Figure I.1 – Ear decomposition

Ear decomposition exists if and only if the graph is 2-edge connected. In the PTDN, a 2-edge connected graph can provide protection for link failure and nodal failures.

Bibliography

[b-ITU-T G.780] Recommendation ITU-T G.780/Y.1351 (2010), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

[b-ITU-T G.870] Recommendation ITU-T G.870/Y.1352 (2010), *Terms and definitions for optical transport networks (OTN)*.

[b-ITU-T G.8131] Recommendation ITU-T G.8131/Y.1382 (2007), *Linear protection switching for transport MPLS (T-MPLS) networks*.

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

[b-ITU-T I.630] Recommendation ITU-T I.630 (1999), *ATM protection switching*.

[b-ITU-T M.2102] Recommendation ITU-T M.2102 (2000), *Maintenance thresholds and procedures for recovery mechanisms (protection and restoration) of international SDH VC trails (paths) and multiplex sections*.

[b-ITU-T X.25] Recommendation ITU-T X.25 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit*.

[b-ITU-T X.121] Recommendation ITU-T X.121 (2000), *International numbering plan for public data networks*.

[b-ITU-T X.136] Recommendation ITU-T X.136 (1997), *Accuracy and dependability performance values for public data networks when providing international packet-switched services*.

[b-ITU-T X.137] Recommendation ITU-T X.137 (1997), *Availability performance values for public data networks when providing international packet-switched services*.

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

[b-ITU-T X.212] Recommendation ITU-T X.212 (1995) | ISO/IEC 8886:1996, *Information technology – Open Systems Interconnection – Data Link service definition*.

[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.1001] Recommendation ITU-T Y.1001 (2000), *IP framework – A framework for convergence of telecommunications network and IP network technologies*.

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

[b-ITU-T Y.1720] Recommendation ITU-T Y.1720 (2006), *Protection switching for MPLS networks*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[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.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation 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, 2012