International Telecommunication Union

ITU-T G.7712/Y.1703

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Amendment 1

(02/2022)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Data over Transport – Generic aspects – Transport network control aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet protocol aspects – Operation, administration and maintenance

---

Architecture and specification of data communication network

Amendment 1

Recommendation ITU-T G.7712/Y.1703 (2019) – Amendment 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
General	G.7000–G.7099
Transport network control aspects	**G.7700–G.7799**
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

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

Recommendation ITU-T G.7712/Y.1703

Architecture and specification of data communication network

Amendment 1

Summary

Recommendation ITU-T G.7712/Y.1703 defines the architecture requirements for a data communication network (DCN) which may support distributed management communications related to the telecommunication management network (TMN), distributed control communications (e.g., signalling and routing) related to the automatically switched optical network (ASON), distributed control communications (e.g., signalling and routing) related to multiprotocol label switching – transport profile (MPLS-TP), control communications related to software defined networking (SDN), and other distributed communications (e.g., orderwire or voice communications, software download). The DCN architecture considers networks that are IP-only, open system interface (OSI)-only, and mixed (i.e., support both IP and OSI). The interworking between parts of the DCN supporting IP-only, parts supporting OSI-only, and parts supporting both IP and OSI are also specified – other protocols (other than IP or OSI) are outside the current scope of this Recommendation.

Various applications (e.g., TMN, ASON) require a packet-based communications network to transport information between various components. For example, the TMN requires a communications network, which is referred to as the management communication network (MCN) to transport management messages between TMN components (e.g., network element function (NEF) component and operations system function (OSF) component). ASON requires a communication network, which is referred to as the control communication network (CCN), and MPLS-TP requires a communication network, which is referred to as the signalling communication network (SCN) to transport signalling and routing messages between functional management and control (MC) components (e.g., connection controller (CC) components and routing controller (RC) components). This Recommendation specifies data communication functions that can be used to support one or more application's communication network.

The data communication functions provided in the 2001 version (version 1) of this Recommendation support connectionless network services. The 2003 revision (version 2) of this Recommendation adds the support of connection-oriented network SCN services by including a specific MPLS-based mechanism.

The 2010 revision (version 4) of this Recommendation provides the requirements for the MPLS transport profile (MPLS-TP) signalling communication channel (SCC) and management communication channel (MCC) data communication functions. The part of this Recommendation that addresses MPLS for transport networks complies with the transport profile of MPLS architecture as defined by Internet Engineering Task Force (IETF). In the event of a difference between this ITU-T Recommendation and any of the normatively referenced request for comments (RFCs) for MPLS-TP, the RFCs will take precedence.

The 2020 version (version 5) provides updates that cover control communications related to software defined networking (SDN). A new Appendix V is also added to this version to provide a mapping between clauses here and prior versions due to restructuring.

The 2022 version (version 5.1) provides updates of the definition of CCN and DCN, replacing SCN with CCN, replacing control component with MC component, and some editorial changes. A new sub clause of 8.2.5 is also added to this version for MTN ECC.

This Recommendation forms part of a family of Recommendations covering transport networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.7712/Y.1703	2001-11-29	15	11.1002/1000/5637
2.0	ITU-T G.7712/Y.1703	2003-03-16	15	11.1002/1000/6287
3.0	ITU-T G.7712/Y.1703	2008-06-22	15	11.1002/1000/9390
4.0	ITU-T G.7712/Y.1703	2010-09-06	15	11.1002/1000/10895
4.1	ITU-T G.7712/Y.1703 (2010) Amd. 1	2013-10-07	15	11.1002/1000/12000
4.2	ITU-T G.7712/Y.1703 (2010) Amd. 2	2016-02-26	15	11.1002/1000/12553
5.0	ITU-T G.7712/Y.1703	2019-08-29	15	11.1002/1000/14006
5.1	ITU-T G.7712/Y.1703 (2019) Amd. 1	2022-02-13	15	11.1002/1000/14900

Keywords

Data communication network, Internet protocol (IP), open system interface (OSI).

* 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 received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T G.7712/Y.1703

Architecture and specification of data communication network

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T G.7712 (2019).

1 Scope

This Recommendation defines the architecture requirements for a data communication network (DCN) which may support distributed management communications related to the telecommunication management network (TMN), distributed control ~~plane~~ communications (e.g., signalling and routing) related to the automatically switched optical network (ASON), distributed control ~~plane~~ communications (e.g., signalling and routing) related to multiprotocol label switching – transport profile (MPLS-TP), control ~~plane~~ communications related to software defined networking (SDN), and other distributed communications (e.g., orderwire or voice communications, software download). The DCN architecture considers networks that are IP-only, open system interface (OSI)-only, and mixed (i.e., support both IP and OSI). The interworking between parts of the DCN supporting IP-only, parts supporting OSI-only, and parts supporting both IP and OSI are also specified – other protocols (other than IP or OSI) are outside the current scope of this Recommendation.

The DCN provides Layer 1 (physical), Layer 2 (data-link) and Layer 3 (network) functionality and consists of routing/switching functionality interconnected via links. These links can be implemented over various interfaces, including wide area network (WAN) interfaces, local area network (LAN) interfaces, and embedded communication channels (ECCs).

Various applications (e.g., TMN, ASON) require a packet-based communication network to transport information between various components. For example, the TMN requires a communication network, which is referred to as the management communication network (MCN) to transport management messages between TMN components (e.g., network element function (NEF) component and operations support function (OSF) component). ASON requires a communication network, which is referred to as the control communication network (CCN), and MPLS-TP requires a communication networks, which ~~are~~ is referred to as signalling communication networks (SCNs) to transport signalling and routing messages between functional management and control (MC) ~~plane~~ components (e.g., connection controller (CC) components and routing controller (RC) components). This Recommendation specifies data communication functions (DCFs) that can be used to support one or more application's communication network.

The DCFs provided in this Recommendation support connectionless network services. Additional functions may be added in future versions of this Recommendation to support connection-oriented network services.

Version 4 of this Recommendation provided the requirements for the MPLS transport profile (MPLS-TP) signalling communication channel (SCC) and management communication channel (MCC) DCFs. The part of this Recommendation that addresses MPLS for transport networks complies with the transport profile of MPLS architecture as defined by Internet Engineering Task Force (IETF). In the event of a difference between this Recommendation and any of the normatively referenced request for comments (RFCs) for MPLS-TP, the RFCs will take precedence.

The 2020 version (version 5) provides updates that cover control ~~plane~~ communications related to software defined networking (SDN). A new Appendix V is also added to this version to provide a mapping between clauses here and prior versions due to restructuring.

The 2022 version (version 5.1) provides updates of the definition of CCN and DCN, replacing SCN with CCN, replacing the control component with the MC component, and some editorial changes. A new subclause of 8.2.5 is also added to this version for MTN ECC.

This Recommendation forms part of a family of Recommendations covering transport networks.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.698.1] Recommendation ITU-T G.698.1 (2009), *Multichannel DWDM applications with single-channel optical interfaces*.

[ITU-T G.698.2] Recommendation ITU-T G.698.2 (2018~~09~~), *Amplified multichannel dense wavelength division multiplexing applications with single channel optical interfaces*.

~~[ITU-T G.707] Recommendation ITU-T G.707/Y.1322 (2007), *Network node interface for the synchronous digital hierarchy (SDH).*~~

[ITU-T G.709] Recommendation ITU-T G.709/Y.1331 (2020~~16~~), *Interfaces for the Optical Transport Network (OTN)*.

[ITU-T G.783] Recommendation ITU-T G.783 (2006), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.

[ITU-T G.784] Recommendation ITU-T G.784 (2008), *Management aspects of synchronous digital hierarchy (SDH) transport network elements*.

[ITU-T G.798] Recommendation ITU-T G.798 (2017~~2~~), *Characteristics of optical transport network hierarchy equipment functional blocks*.

[ITU-T G.872] Recommendation ITU-T G.872 (2017~~9~~), *Architecture of optical transport network*.

[ITU-T G.874] Recommendation ITU-T G.874 (2020~~17~~), *Management aspects of optical transport network elements*.

[ITU-T G.7701] Recommendation ITU-T G.7701(2022), *Common control aspects*.

[ITU-T G.7702] Recommendation ITU-T G.7702 (2018), *Architecture for SDN control of transport networks*.

[ITU-T G.7703] Recommendation ITU-T G.7703/Y.1304 (2021), *Architecture for the automatically switched optical network*.

[ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2020~~12~~), *Common equipment management function requirements*, including Amendment 1 (2016).

[ITU-T G.7714] Recommendation ITU-T G.7714 (2005), *Generalized automatic discovery for transport entities*.

[ITU-T G.7714.1] Recommendation ITU-T G.7714.1 (2017), *Protocol for automatic discovery in transport networks*.

[ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2016~~6~~8), *Characteristics of Ethernet transport network equipment functional blocks*.

[ITU-T G.8051] Recommendation ITU-T G.8051/Y.1345 (2020~~15~~), *Management aspects of the Ethernet-over-Transport (EoT) capable network element*.

[ITU-T G.8312] Recommendation ITU-T G.8312 (2020), *Interfaces for metro transport networks*, including Amendment 1 (2022), ~~*Interfaces for metro transport networks – Amendment 1*~~.

~~[ITU-T G.8080] Recommendation ITU-T G.8080/Y.1304 (2012), *Architecture for the automatically switched optical network (ASON), Amendment 1 (2008), Amendment 2 (2010).*~~

~~[ITU-T G.8081] Recommendation ITU-T G.8081/Y.1353 (2012), *Terms and definitions for Automatically Switched Optical Networks (ASON).*~~

[ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*, including Amendment 1 (2003) and~~,~~ Amendment 2 (2005).

[ITU-T M.3013] Recommendation ITU-T M.3013 (2000), *Considerations for a telecommunications management network*.

[ITU-T M.3016.x] Recommendation ITU-T M.3016.x-series (2005), *TMN security overview*.

[ITU-T Q.811] Recommendation ITU-T Q.811 (2004), *Lower layer protocol profiles for the Q and X interfaces*.

[ITU-T Q.812] Recommendation ITU-T Q.812 (2004), *Upper layer protocol profiles for the Q and X interfaces*.

[ITU-T Q.921] Recommendation ITU-T Q.921 (1997), *ISDN user-network interface – Data link layer specification*, including Amendment 1 (2000).

[ITU-T X.233] Recommendation ITU-T X.233 (1997) | ISO/IEC 8473-1:1998, *Information technology – Protocol for providing the connectionless-mode network service: Protocol specification*.

[ITU-T X.263] Recommendation ITU-T X.263 (1998) | ISO/IEC TR 9577:1999, *Information technology – Protocol identification in the Network Layer*.

[ISO 9542] ISO 9542:1988, *Information processing systems – Telecommunications and information exchange between systems – End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*.

[ISO/IEC 10589] ISO/IEC 10589:2002, *Information technology – Telecommunications and information exchange between systems – Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*.

[IEEE 802.3] IEEE Std. 802.3-2018~~2~~, *IEEE Standard for Ethernet*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol DARPA Internet Program Protocol Specification*.

[IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[IETF RFC 826] IETF RFC 826 (1982), *Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*.

[IETF RFC 894] IETF RFC 894 (1984), *A Standard for the Transmission of IP Datagrams over Ethernet Networks*.

[IETF RFC 1122] IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.

[IETF RFC 1195] IETF RFC 1195 (1990), *Use of OSI IS-IS for Routing in TCP/IP and dual environments*.

[IETF RFC 1332] IETF RFC 1332 (1992), *The PPP Internet Protocol Control Protocol (IPCP)*.

[IETF RFC 1377] IETF RFC 1377 (1992), *The PPP OSI Network Layer Control Protocol (OSINLCP)*.

[IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*.

[IETF RFC 1662] IETF RFC 1662 (1994), *PPP in HDLC-like Framing*.

[IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

[IETF RFC 2328] IETF RFC 2328 (1998), *OSPF Version 2*.

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[IETF RFC 2472] IETF RFC 2472 (1998), *IP Version 6 over PPP*.

[IETF RFC 2740] IETF RFC 2740 (1999), *OSPF for IPv6*.

[IETF RFC 2784] IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE)*.

[IETF RFC 2961] IETF RFC 2961 (2001), *RSVP Refresh Overhead Reduction Extensions*.

[IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[IETF RFC 3032] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

[IETF RFC 3209] IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

[IETF RFC 3818] IETF RFC 3818 (2004), *IANA Considerations for the Point-to-Point Protocol (PPP)*.

[IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

[IETF RFC 5586] IETF RFC 5586 (2009), *MPLS Generic Associated Channel*.

[IETF RFC 5718] IETF RFC 5718 (2010), *An In-Band Data Communication Network For the MPLS Transport Profile*.

[IETF RFC 7581] IETF RFC 7581 (2015), *Routing and Wavelength Assignment Information Encoding for Wavelength Switched Optical Networks*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Terms defined in [ITU-T G.709]:

a) optical channel data unit (ODUk)

b) optical channel transport unit (OTUk)

c) OTM overhead signal (OOS)

d) general management communications overhead (COMMS OH)

e) optical tributary signal assembly (OTSiA)

f) optical tributary signal group (OTSiG)

g) optical tributary signal overhead (OTSiG-O)

3.1.2 Term defined in [ITU-T G.784]:

a) data communications channel (DCC)

~~**3.1.3 Terms defined in [ITU-T G.8080] and [ITU-T G.8081]:**~~

~~a) automatically switched optical network (ASON)~~

~~b) external network-network interface (E-NNI)~~

~~c) internal network-network interface (I-NNI)~~

~~d) user-network interface (UNI)~~

~~e) call controller (CallC)~~

~~f) connection controller (CC)~~

~~g) connection controller interface (CCI)~~

~~h) subnetwork connection controller (SN-CC)~~

3.1.4~~3~~ Term defined in [ITU-T G.874]:

a) general communication channel (GCC)

3.1.4 Terms defined in [ITU-T G.7701]:

a) automatically switched optical network (ASON)

b) call controller

c) connection controller (CC)

3.1.5 Terms defined in [ITU-T G.7703]:

a) external network-network interface (E-NNI)

b) internal network-network interface (I-NNI)

c) user-network interface (UNI)

3.1.5~~6~~ Terms defined in [ITU-T G.7710]:

a) x.management network

b) x.management subnetwork

3.1.6~~7~~ Term defined in [ITU-T G.872]:

a) optical transport network (OTN)

3.1.7~~8~~ Terms defined in [ITU-T M.3010]:

a) adaptation device (AD)

b) data communications function (DCF)

c) mediation device (MD)

d) network element (NE)

e) network element function (NEF)

f) operations system (OS)

g) operations system function (OSF)

h) Q interface

i) transformation function

j) workstation function (WSF)

3.1.~~8~~9 Term defined in [ITU-T M.3013]:

a) message communication function (MCF)

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 automatic encapsulating data communication function (AE-DCF): An AE-DCF automatically encapsulates packets when necessary, so that they may be routed by network elements (NEs) that would otherwise be unable to forward them. An AE-DCF also features a matching de-encapsulation function to restore the packet back to its original form once it has traversed incompatible NEs.

3.2.2 control communication channel (CCC): An CCC provides a dedicated logical operations channel between NEs for control communications. The physical channel supporting the CCC is technology specific.

3.2.3 connection controller interface (CCI): A CCI is an interface between a subnetwork in the transport resource and the control domain.

3.2.~~2~~4 control communication~~s~~ network (CCN): A part of the data communication network (DCN) that is used to support communications across the reference points defined for a software defined networking (SDN) management and control (MC) system in [ITU-T G.7702], or an automatically switched optical network (ASON) MC system in [ITU-T G.7703], e.g., CPI, UNI, NNI~~for control components to communicate with each other is referred to as the control communications network (CCN). The control component could be either SDN control components or ASON control component~~.

3.2.~~3~~5 data communication network (DCN): The DCN is a packet switched layer network that supports management and control communications ~~Layer 1 (physical), Layer 2 (data link), and Layer 3 (network) functionality~~. A DCN can ~~be designed to~~ support transport of ~~distributed~~ management communications related to the telecommunication management network (TMN), management and control ~~distributed signalling~~ communications related to software defined networking (SDN) or ~~the~~ automatically switched optical network (ASON), and other operations communications (e.g., ~~orderwire/voice communications,~~ software downloads, overhead communications channel (OCN) etc.).

3.2.~~4~~6 embedded communication channel (ECC): An ECC provides a logical operations channel between network elements (NEs) that can be utilized by multiple applications (e.g., management applications, control ~~plane~~ applications). The physical channel supporting the ECC is technology specific. Examples of physical channels supporting the ECC are: a data communication channel (DCC) ~~channel~~ within synchronous digital hierarchy (SDH), general communication channel (GCC) ~~channel~~ within optical transport network (OTN) optical channel transport unit/optical channel data unit (OTUk/ODUk), or the general management communications overhead (COMMS OH) channel within the OTN optical supervisory channel (OSC)~~OOS~~.

3.2.~~5~~7 IP routing interworking function: An Internet protocol (IP) routing interworking function allows IP topology or routes to be passed from one IP routing protocol to a different incompatible IP routing protocol. For example, an IP routing interworking function may form a gateway between an integrated intermediate system-to-intermediate system (IS-IS) routed data communication network (DCN) and an open shortest path first (OSPF) routed DCN.

3.2.~~6~~8 management communication channel (MCC): An MCC provides a dedicated logical operations channel between NEs for management communications. The physical channel supporting the MCC is technology specific.

3.2.~~7~~9 network-layer interworking function: A network-layer interworking function provides interoperability between nodes that support incompatible network-layer protocols. An example of a network-layer interworking function is static generic routing encapsulation (GRE) tunnels, or an automatic encapsulating data communication function (AE-DCF).

3.2.10 management communication network (MCN): A part of the data communication network (DCN) that is used for management communication.

3.2.~~8~~11 non-MPLS-TP server to MPLS-TP adaptation function (SRV/MT_A): The non-multiprotocol label switching – transport profile (non-MPLS-TP) server to MPLS-TP adaptation function is defined as an ITU-T G.805 adaptation function between a non-MPLS server layer network and the MPLS-TP layer network.

3.2.~~9~~12 overhead communications channel (OCC): The overhead communications network (OCN) provides one or more channels for the communication of the overhead. These channels are referred to as the overhead communications channel (OCC).

3.2.~~10~~13 overhead communications network (OCN): A part of a data communication network (DCN) that is used for overhead communication is referred to as the overhead communications network (OCN).

3.2.~~11~~14 signalling communication channel (SCC): An SCC provides a dedicated logical operations channel between network elements (NEs) for ~~control plane~~ signalling communications. ~~This SCC may not only be used for ASON signalling but may also carry other control plane messages, e.g., routing messages. The physical channel supporting the SCC is technology specific.~~

Note that in an MPTS-TP control domain, the terms signalling communication channel (SCC) is used instead and it is equivalent to the generic terms control communication channel (CCC).

3.2.15 signalling communication network (SCN): A part of the data communication network (DCN) that is used for signalling communication.

Note that in an MPLS-TP control domain, the terms signalling communication network (SCN) is used instead and it is equivalent to the generic term control communication network (CCN).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AD	Adaptation Device
AE-DCF	Automatic Encapsulating Data Communication Function
AI	Adapted Information
AP	Access Point
ARP	Address Resolution Protocol
ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
BDI	Backward Defect Indication
CallC	Call Controller
CC	Connection Controller
CCC	Control Communication Channel

CCI	Connection Controller Interface
CCN	Control Communication Network
CI	Characteristic Information
CLNP	Connectionless Network Layer Protocol
CLNS	Connectionless Network Layer Service
COMMS OH	General Management Communications Overhead
CP	Connection Point
CPI	Control Plane Interface
DCC	Data Communication Channel
DCF	Data Communication Function
DCN	Data Communication Network
DF	Don't Fragment
ECC	Embedded Communication Channel
EMF	Equipment Management Function
EoT	Ethernet over Transport
ERO	Explicit Route Object
ES	End System
ESH	End System Hello
ES-IS	End System-to-Intermediate System
ETH	Ethernet MAC layer
FlexE	Flex Ethernet
FwP	Forwarding Points
G-ACh	Generic Associated Channel
GAL	Generic Associated Channel Label
GCC	General Communication Channel
GFP	Generic Framing Procedure
GFP-F	Frame-mapped GFP
GNE	Gateway Network Element
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
ICMP	Internet Control Message Protocol
ID	Identifier
IIH	IS-IS Hello
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPI	Initial Protocol Identifier
IPv4	Internet Protocol Version 4

IPv6	Internet Protocol Version 6
IS	Intermediate System
ISDN	Integrated Services Digital Network
ISH	Intermediate System Hello [ISO 9542]
IS-IS	Intermediate System-to-Intermediate System
IWF	Interworking Function
LAN	Local Area Network
LAPD	Link-Access Procedure D-Channel
LCN	Local Communication Network
LER	Label Edge Router
LMP	Link Management Protocol
LSP	Label Switched Path
LS-PDU	Link State Protocol Data Unit
LSR	Label Switched Router
MAC	Media Access Control
MC	Management and Control
MCC	Management Communication Channel
MCF	Message Communication Function
MCN	Management Communication Network
MD	Mediation Device
MPLS-TP	Multiprotocol Label Switching – Transport Profile
MTN	Metro Transport Network
MTNP	MTN Path Layer
MTNS	MTN Section Layer
MTU	Maximum Transmission Unit
NC	Network Connection
NE	Network Element
NEF	Network Element Function
NIM	Non-Intrusive Monitoring
NLPID	Network Layer Protocol Identifier
NNE	Network NE
NNI	Network-to-Network Interface
NSAP	Network Service Access Point
OCC	Overhead Communications Channel
OCh	Optical Channel
OCh-O	Optical Channel Overhead
OCh-P	Optical Channel Payload

OCN	Overhead Communications Network
ODUk	Optical Channel Data Unit
OOB	Out-of-Band
OOS	OTM Overhead Signal
OPS	Optical Physical Section
OS	Operations System
OSC	Optical Supervisory Channel
OSF	Operations System Function
OSI	Open System Interface
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OTM	Optical Transport Module
OTN	Optical Transport Network
OTSi	Optical Tributary Signal
OTSiA	Optical Tributary Signal Assembly
OTSiG	Optical Tributary Signal Group
OTSiG-O	Optical Tributary Signal Group – Overhead
OTUk	Optical Channel Transport Unit
PDU	Protocol Data Unit
PHOP	Previous HOP
PID	Protocol Identifier
PPP	Point-to-Point Protocol
RC	Routing Controller
RSVP-ORE	Resource Reservation Protocol – Overhead Reduction Extensions
SCC	Signalling Communication Channel
SCN	Signalling Communication Network
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Networking
SID	System Identifier
~~SN-CC~~	~~Subnetwork Connection Controller~~
S/OMS	SDH/OTN Management Subnetwork
SP	Segmentation Permitted
SPF	Shortest Path First
SRM	Send Routing Message
SSF	Server Signal Fail
TCP	Termination Connection Point
TCP	Transmission Control Protocol

TF	Translation Function
TFP	Termination Flow Point
TLV	Type Length Value
TMN	Telecommunication Management Network
TNE	Transport Network Element
TSF	Trail Signal Fail
TT	Trail Termination
UDP	User Datagram Protocol
UNI	User-to-Network Interface
UPI	User Payload Identifier
WAN	Wide Area Network
WS	Work Station
WSF	Work Station Function

5 Conventions

The following conventions are used throughout this Recommendation:

Mixed DCN: A mixed DCN supports multiple network layer protocols (e.g., OSI and IPv4). It is possible in a mixed DCN that the path between two communicating entities (e.g., an OS and a managed network element (NE)) will traverse some parts that only support one network layer protocol (e.g., OSI), and other parts that only support another network layer protocol (e.g., IPv4). To provide communication between such entities, one network layer protocol should be encapsulated into the other network layer protocol at the boundary of those parts supporting different network layer protocols.

OSI-only DCN: An OSI-only DCN supports only connectionless network layer protocol (CLNP) as the network layer protocol. Therefore, the end-to-end path between two communicating entities (e.g., an OS and a managed NE) will support CLNP, and encapsulation of one network layer protocol into another network layer protocol is not required to support such communications.

IPv4-only DCN: An IPv4-only DCN supports only IPv4 as the network layer protocol. Therefore, the end-to-end path between two communicating entities (e.g., an OS and a managed NE) will support IPv4, and encapsulation of one network layer protocol into another network layer protocol is not required to support such communications.

IPv6-only DCN: An IPv6-only DCN supports only IPv6 as the network layer protocol. Therefore, the end-to-end path between two communicating entities (e.g., an OS and a managed NE) will support IPv6, and encapsulation of one network layer protocol into another network layer protocol is not required to support such communications.

6 DCN applications

Various applications (e.g., TMN, ASON, MPLS-TP, SDN, overhead communications network (OCN)) require a packet-based communication network to transport information between various components. For example, the TMN requires a communication network, which is referred to as the MCN to transport management messages between TMN components (e.g., network element function (NEF) component and OSF component). ASON and SDN application requires a communication network, which is referred to as the control communication network (CCN) to transport control messages between ~~control~~ MC components (e.g., CC components, RC components). The control

communication network used for ASON signal communication is also referred to as a control ~~signalling~~ communication network (~~SCN~~CCN). This Recommendation specifies data communication functions that can be used to support one or more application's communication network.

Figure 6-1 illustrates example applications that can be supported via the DCN. Each application can be supported on separate DCNs or on the same DCN depending on the network design.

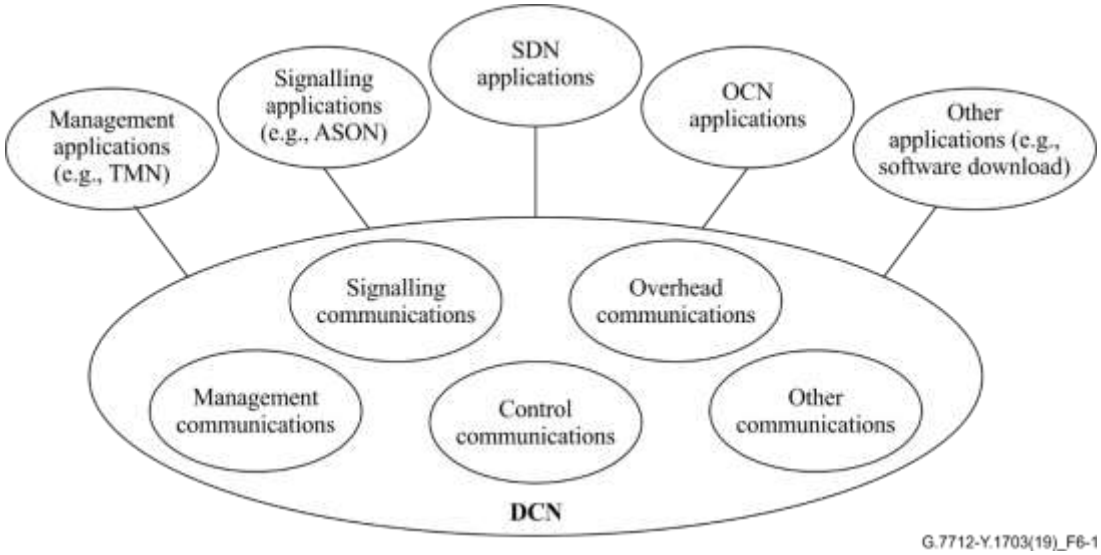


Figure 6-1 – Example applications supported by a DCN

The conceptual DCN is a collection of resources to support the transfer of information among distributed components. As discussed above, examples of distributed communication that can be supported by the DCN are distributed management communications related to the TMN, distributed control ~~plane~~ communications related to the ASON, and communication related to SDN. In the case of a DCN supporting distributed management communications, the distributed components are TMN components (NEs, adaptation devices (ADs), operations systems (OSs), mediation devices (MDs), and work stations (WSs) containing TMN functions such as OSF, translation function (TF), NEF, work station function (WSF)). [ITU-T M.3010] and [ITU-T M.3013] provide further specifications for the TMN functions. In the case of a DCN supporting distributed signalling communications, the distributed components are ASON components (NEs containing ASON call controller (CallC)/CC functions). [ITU-T G.~~8080~~7703] provides further specifications for the ASON functions. In the case of SDN communications further details are provided in [ITU-T G.7702].

A number of telecommunication technologies can support the DCN functions, such as circuit switching, packet switching, LAN, asynchronous transfer mode (ATM), synchronous digital hierarchy (SDH), optical transport network (OTN), MPLS-TP and Ethernet over transport (EoT). Important aspects of the DCN are the quality of service, information transfer rate, and diversity of routing to support specific operational requirements of the distributed communications supported across the DCN (e.g., distributed management communications, distributed signalling communications).

The goal of an interface specification is to ensure meaningful interchange of data between interconnected devices through a DCN to perform a given function (e.g., TMN function, ASON function, SDN function, OCN function). An interface is designed to ensure independence of the type of device or of the supplier. This requires compatible communication protocols and compatible data representations for the messages, including compatible generic message definitions for TMN management functions, ASON control functions, and SDN control and SDN management functions.

The DCN is responsible for providing compatible communication at the network layer (Layer 3), data-link layer (Layer 2), and physical layer (Layer 1).

Consideration of interfaces should be given to compatibility with the most efficient data transport facilities available to each individual network element (e.g., leased circuits, circuit-switched connections, packet-switched connections, signalling system No. 7, embedded communication channels (ECCs) of the SDH, OTN, MPLS-TP, Ethernet, and integrated services digital network (ISDN) access network D- and B-channels).

This Recommendation specifies the lower three layers for data communication and, therefore, any interworking between protocols within the lower three layers. Such interworking is provided by the DCF. Examples of such interworking are illustrated in Figure 6-2. Note that such interworking does not terminate the Layer 3 protocols. One example is interworking between different physical layers via a common Layer 2 protocol (e.g., bridging media access control (MAC) frames from a LAN interface to an ECC). Another example is interworking between different data-link layer protocols via a common Layer 3 protocol (e.g., routing IP packets from a LAN interface to an ECC). The third example, illustrated in Figure 6-2, shows interworking between different network layer protocols via a Layer 3 tunnelling function (in this example, OSI is encapsulated/tunnelled over IP; however, IP over OSI encapsulation/tunnelling is also possible).

The type of information transported between the distributed components depends on the type of interfaces supported between the components. A DCN supporting distributed management communications related to the TMN needs to support the transport of information associated with the TMN interfaces defined in [ITU-T M.3010]. A DCN supporting distributed control ~~plane~~ communications related to the ASON needs to support the transport of information associated with the ASON interfaces defined in [ITU-T G.~~8080~~7703]. A DCN supporting communications related to SDN needs to support the transport of information associated with the SDN interfaces defined in [ITU-T G.7702].

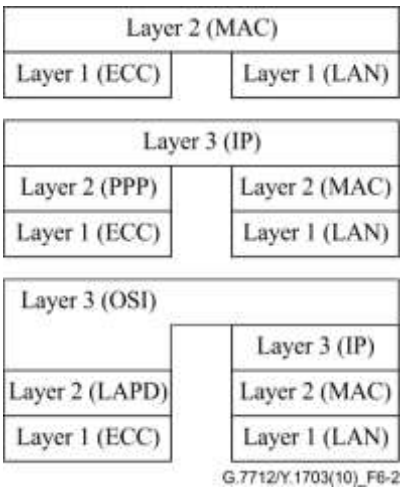


Figure 6-2 – Examples of DCN interworking

6.1 TMN application

The TMN requires a communications network, which is referred to as the MCN to transport management messages between TMN components (e.g., NEF component and OSF component). Figure 6-3 illustrates an example relationship of the MCN and the TMN. The interfaces between the various elements (e.g., OS, WS, NE) and the MCN, as illustrated in Figure 6-3, are logical and can be supported over a single physical MCN interface or multiple MCN interfaces.

Figure 6-4 illustrates an example of a physical implementation of an MCN supporting distributed management communications. Depending on the choice of implementation of the MCN, the physical elements may support any combination of ECC interfaces, LAN interfaces, and WAN interfaces. Figure 6-4 also illustrates the types of management plane functional blocks that can be supported in various physical elements. Refer to [ITU-T M.3010] and [ITU-T M.3013] for detailed specifications

regarding these management functional blocks. A DCF is part of each physical element and provides data communication functions.

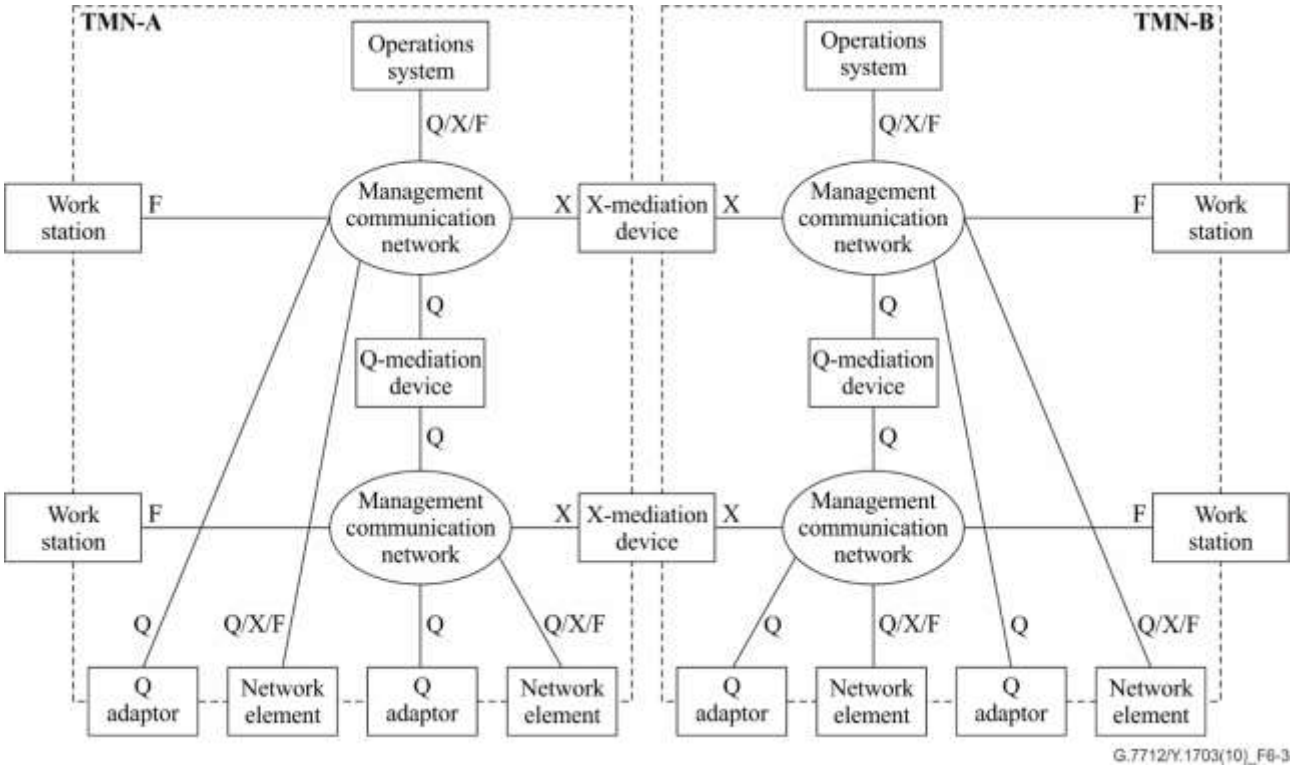


Figure 6-3 – Example relationship of TMN interfaces and MCN

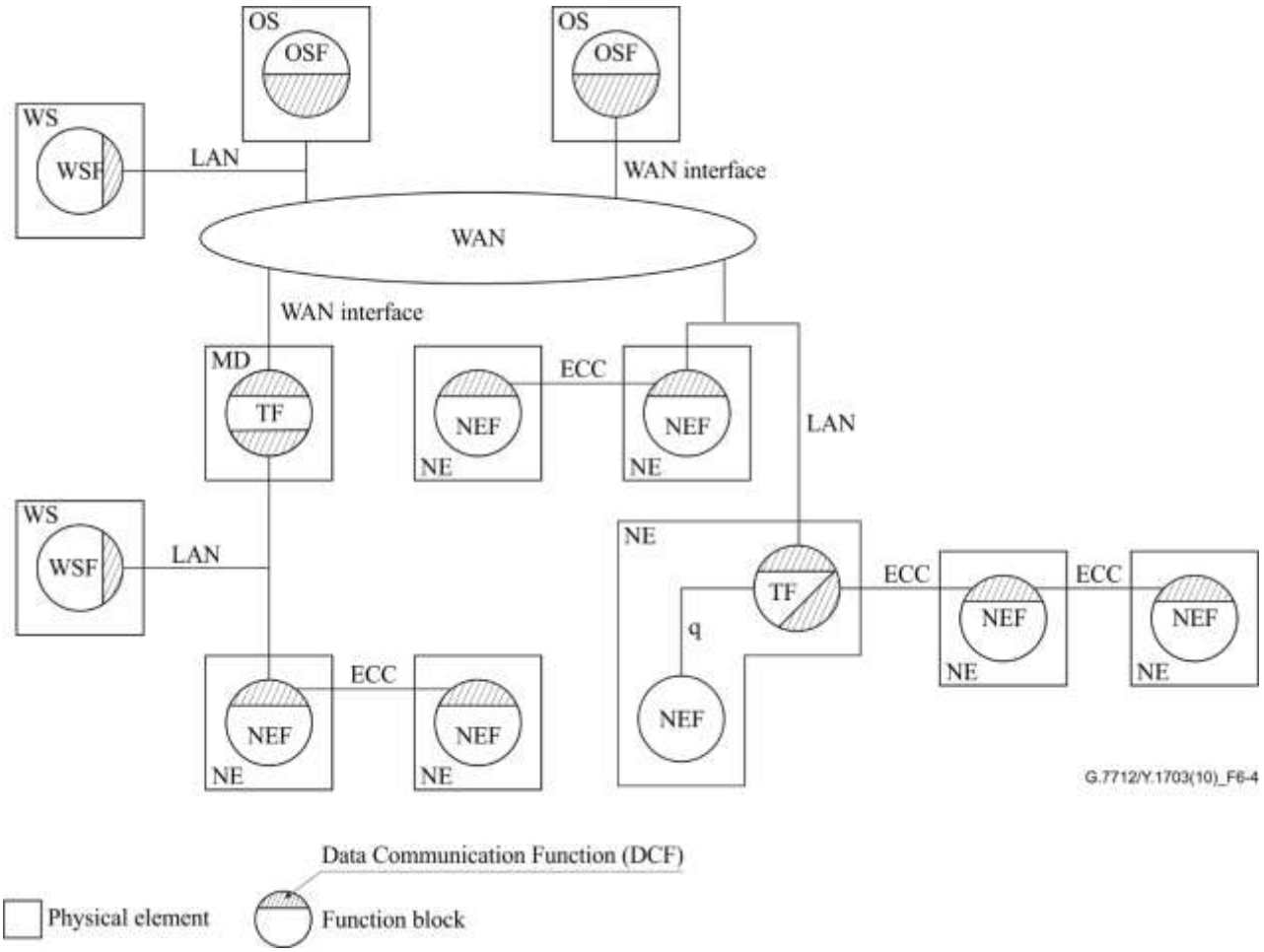


Figure 6-4 – Example of physical implementation of MCN supporting TMN

6.1.1 X management subnetwork architecture

In Figure 6-5, a number of points should be noted concerning the architecture of a X management subnetwork:

– *Multiple NEs at a single site*

Multiple addressable SDH, OTN, or MPLS-TP NEs may appear at a given site. For example, in Figure 6-5, network network element (NNE) and gateway network element (GNE) may be collocated at a single equipment site.

– *SDH/OTN/MPLS-TP NEs and their communication functions*

The message communication function (MCF) of an SDH, OTN, or MPLS-TP NE terminates (in the sense of the lower protocol layers) routes, or otherwise processes messages on the ECC or connected via an external interface.

i) All NEs are required to terminate the ECC. This means that each NE must be able to perform the functions of an OSI end system (ES) or IP host.

ii) NEs may also be required to route ECC messages between ports according to routing control information held in the NE. This means that an NE may also be required to perform the functions of an OSI intermediate system or IP router.

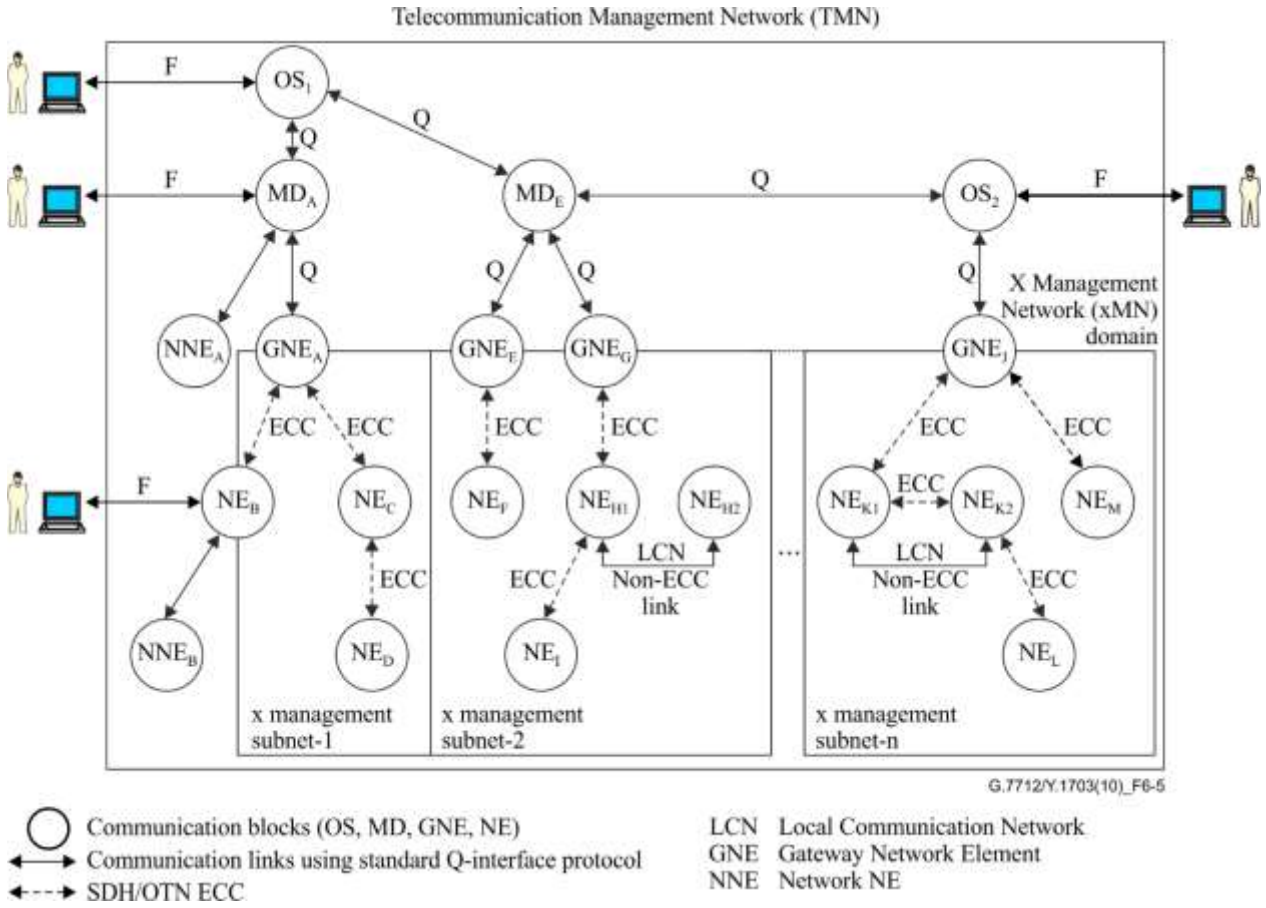
– *SDH/OTN/MPLS-TP inter-site communications*

The inter-site or inter-office communications link between SDH/OTN/MPLS-TP NEs may be formed from the SDH/OTN/MPLS-TP ECCs.

– *SDH/OTN/MPLS-TP intra-site communications*

Within a particular site, SDH/OTN/MPLS-TP NEs may communicate via an intra-site ECC or via a local communication network (LCN). Figure 6-5 illustrates both instances of this interface.

NOTE – A standardized LCN for communicating between collocated network elements has been proposed as an alternative to the use of an ECC. The LCN would potentially be used as a general site communication network serving SDH, OTN, MPLS-TP, and non-SDH/OTN/MPLS-TP NEs (NNEs).



NOTE – The designation "Q" is used in a generic sense.

Figure 6-5 – TMN, management network and management subnetwork model

6.1.1.1 Topology for management subnetwork

Figure 6-6 illustrates example MCN topologies, such as linear, ring, mesh, and star utilizing ECCs and/or LCN (e.g., [IEEE 802.3] Ethernet LAN) as the physical links interconnecting the network elements. Figure 6-7 illustrates how a management subnetwork could be supported on each topology. Common to each topology are the dual gateways (GNE_1 and GNE_2) which allow reliable access to the NEs within the management subnetwork. Another common aspect to each of the example topologies is that each topology allows multiple diverse paths between any NE within the management subnetwork and the OS.

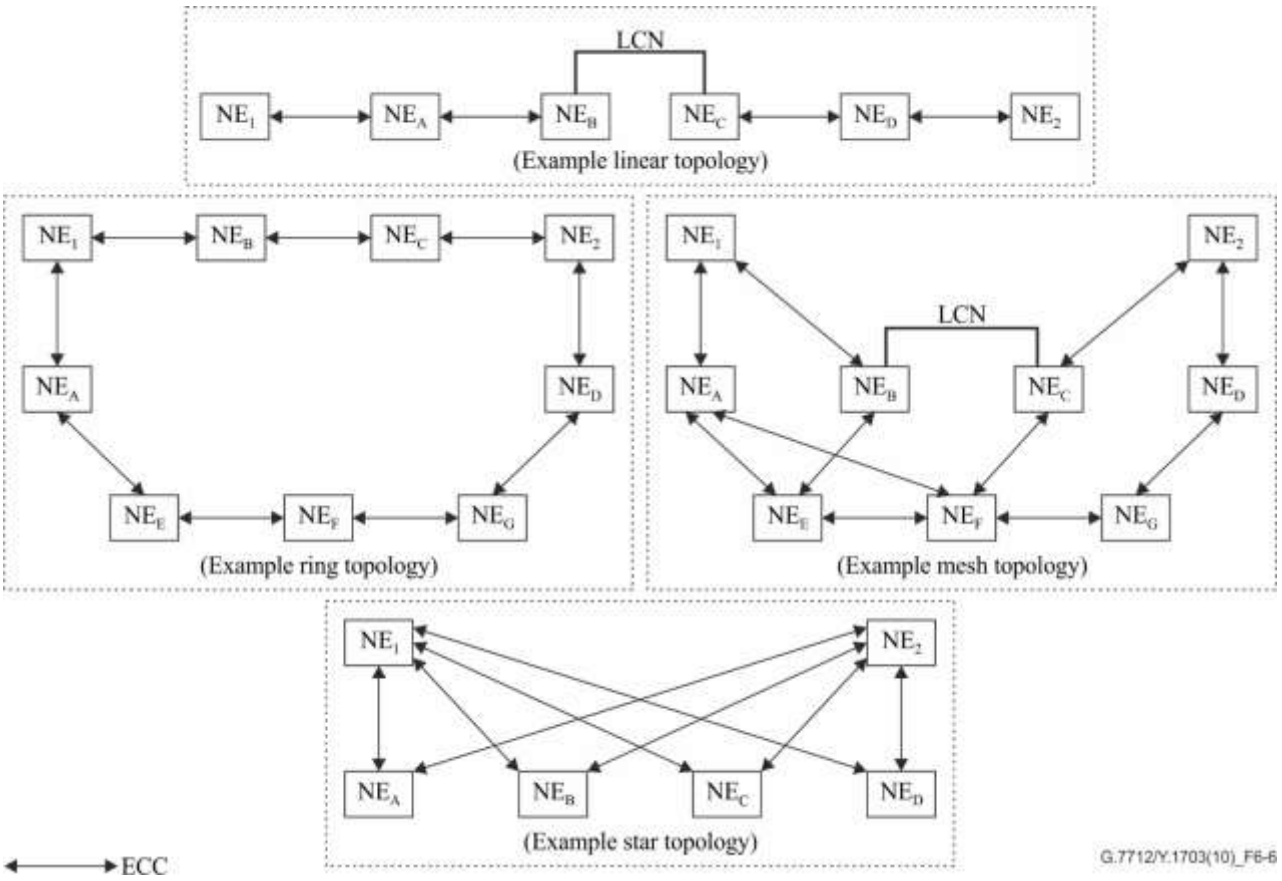


Figure 6-6 – Example topologies

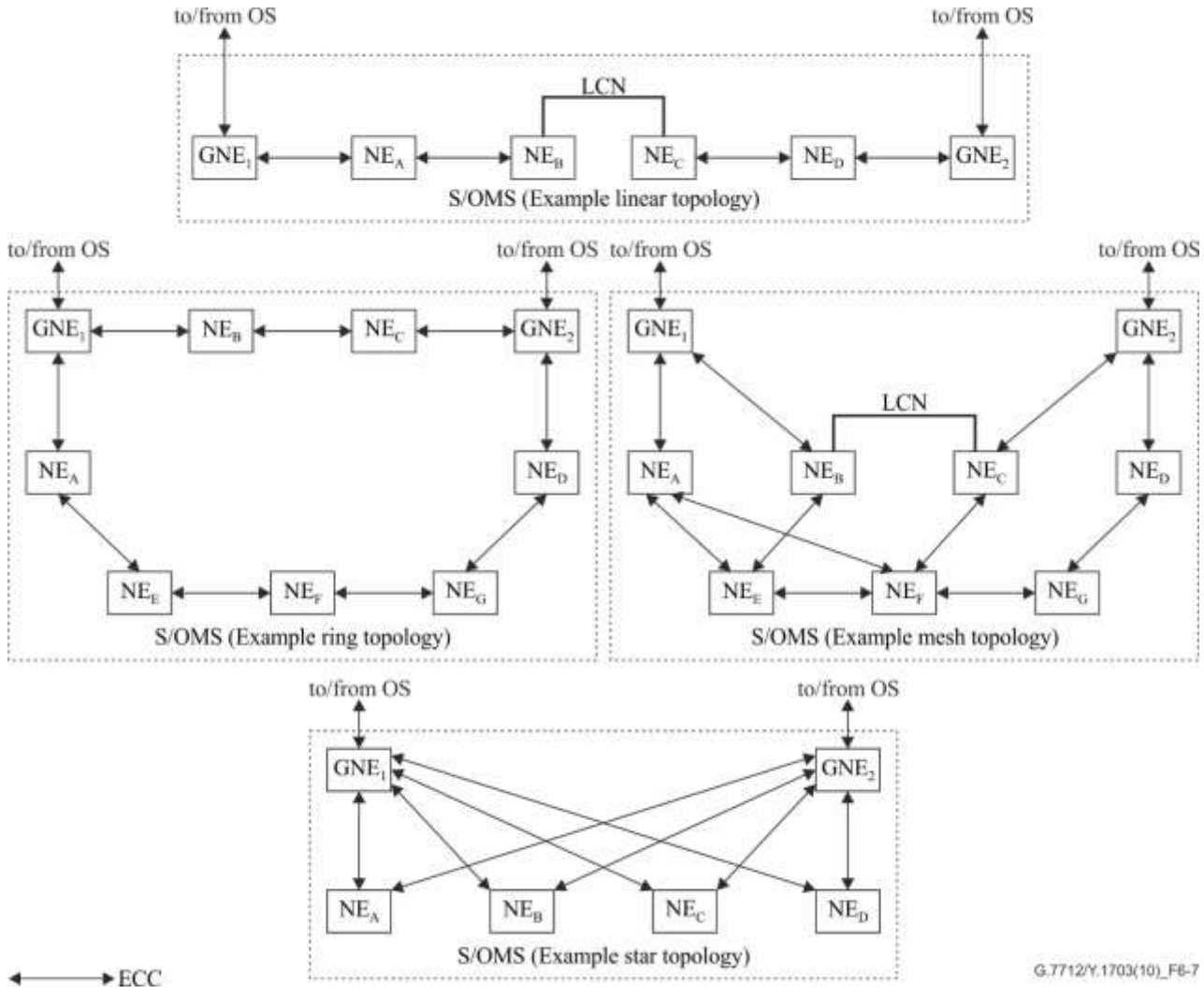


Figure 6-7 – Supporting a management subnetwork on various topologies

6.1.2 Reliability of MCN

An MCN should be designed to prevent a single fault from making the transfer of critical management messages impossible.

An MCN should be designed to ensure that congestion in the MCN does not cause the blocking or excessive delay of network management messages that are intended to correct a failure or fault.

OSs and NEs that provide an emergency function may require alternate or duplicate access channels to the MCN for redundancy.

6.1.3 Security of MCN

See [ITU-T M.3016.x] for MCN security requirements.

6.1.4 MCN s

The DCF within the TMN entities shall support the ES (in OSI terms) or host (in IP terms) functionality.

- When the DCF within the TMN entities support ECC interfaces, the following functions are required to be supported:
  - ECC access function (as specified in clause 8.1);
  - ECC data-link layer termination function (as specified in clause 8.2);

  - "Network layer PDU into ECC data-link layer frame" encapsulation function (as specified in clause 8.3.1);
  - "MPLS PDU into ECC data-link layer" encapsulation function (as specified in clause 9.3.1), if native MPLS is used in the DCN.
- When the DCF within the TMN entities support Ethernet LAN interfaces, the following functions are required to be supported:
  - Ethernet LAN physical layer termination function (as specified in clause 9.1);
  - "Network layer PDU into Ethernet frame" encapsulation function (as specified in clause 8.3.1.5);
  - "MPLS PDU into Ethernet frame" encapsulation function (as specified in clause 9.3.1.1), if native MPLS is used in the DCN.

The DCF within the TMN entities may operate as an intermediate system (IS) (in OSI terms) or as a router (in IP terms). The DCF within TMN entities that operate as IS/routers must be capable of routing within their Level-1 area and, therefore, must provide the functionality of a Level-1 IS/router. Additionally, the DCF within a TMN entity may be provisioned as a Level-2 IS/router, which provides the capability of routing from one area to another. The functionality of a Level-2 IS/router is not needed in the DCF of all TMN entities. An example of a DCF supporting Level-2 IS/router functionality might be the DCF within a gateway NE.

- When the DCF, within the TMN entities, operates as an IS/router, the following functions are required to be supported:
  - Network layer protocol data unit (PDU) forwarding function (as specified in clause 8.3.2);
  - Network layer routing function (as specified in clause 8.3.6).

The DCF within a TMN entity that supports IP may be connected directly to a DCF in a neighbouring TMN entity that supports only OSI.

- When the DCF within a TMN entity that supports IP is connected directly to a DCF in a neighbouring TMN entity that supports only OSI, the following function is required to be supported in the DCF supporting IP:
  - Network layer PDU interworking function (IWF) (as specified in clause 8.3.3).

The DCF within a TMN entity may have to forward a network layer PDU across a network that does not support the same network layer type.

- When the DCF within a TMN entity must forward a network layer PDU across a network that does not support the same network layer type, the following functions are required to be supported:
  - Network layer PDU encapsulation function (as specified in clause 8.3.4);
  - Network layer PDU tunnelling function (as specified in clause 8.3.5).

The DCF within a TMN entity that supports IP using open shortest path first (OSPF) routing may be connected directly to a DCF in a neighbouring TMN entity that supports IP using integrated intermediate system-to-intermediate system (IS-IS).

- When the DCF within a TMN entity that supports IP using OSPF routing is connected directly to a DCF in a neighbouring TMN entity that supports IP using integrated IS-IS, the following function is required to be supported in the DCF supporting OSPF:
  - IP routing interworking function (as specified in clause 8.3.7).

6.2 ASON application

The ASON~~/MPLS-TP~~ control ~~plane~~ domain requires a communications network, which is referred to as the control ~~signalling~~ communication network (~~SCN~~CCN) to transport signalling and routing protocol messages between ASON~~/MPLS-TP control plane~~MC components (e.g., CC components, RC components).

In the following, ASON is used as an example for a control ~~plane~~ application. What is described for the ASON control ~~plane~~ domain is also applicable to the MPLS-TP control ~~plane~~domain. Note that in the MPLS-TP control domain, the terms signalling communication network (SCN) and communication channel (SCC) are used instead and they are equivalent to the generic term control communication network (CCN) and control communication channel (CCC).

Figure 6-8 illustrates an example relationship of the CCN ~~SCN~~ and the ASON. The interfaces between the various elements and the CCN~~SCN~~, as illustrated in Figure 6-8, are logical and can be supported over a single physical CCN ~~SCN~~ interface, or multiple CCN ~~SCN~~ interfaces.

Figure 6-9 illustrates an example of a physical implementation of a ~~SCN~~ CCN supporting distributed signalling communications. Depending on the choice of implementation of the ~~SCN~~CCN, the physical elements may support any combination of ~~SCC~~ CCC interfaces, LAN interfaces, and WAN interfaces. Figure 6-9 also illustrates the types of control ~~plane~~ functional blocks that can be supported in various physical elements. Refer to [ITU-T G.~~8080~~7703] for detailed specifications regarding these control functional blocks. A DCF is part of each physical element and provides data communication functionality.

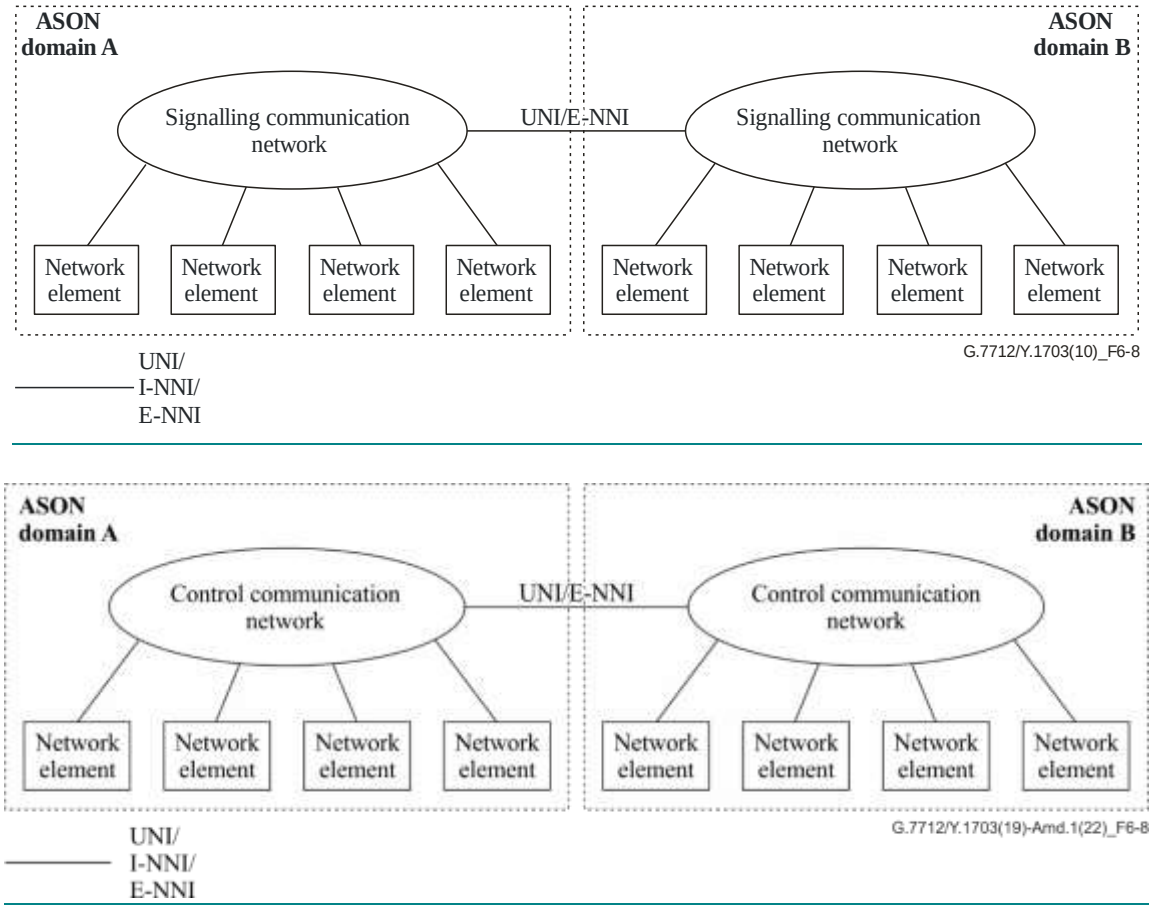


Figure 6-8 – Example relationship of ASON interfaces to ~~SCN~~CCN

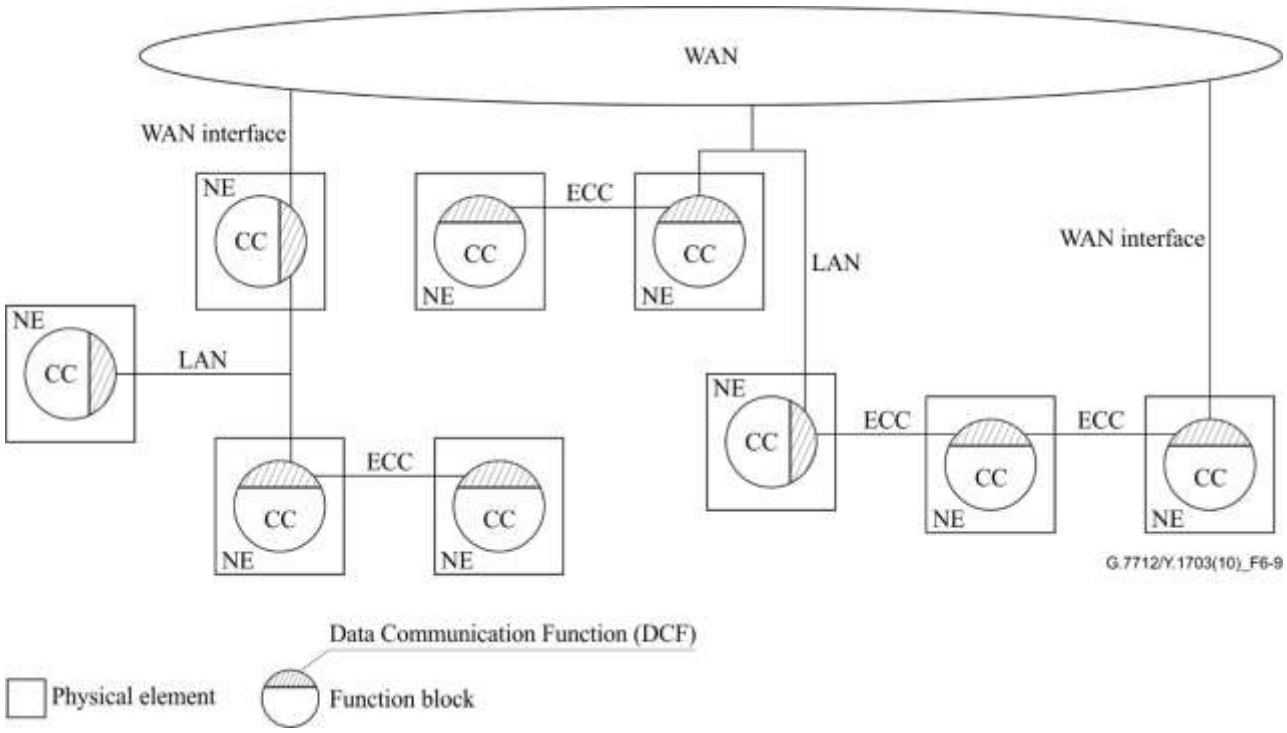


Figure 6-9 – Example of physical implementation of CCN ~~SCN~~ supporting ASON

6.2.1 Topology of CCN~~SCN~~

Figure 6-10 illustrates example topologies, such as linear, ring, mesh, and star utilizing ECCs and/or LCNs (e.g., Ethernet LAN) as the physical links interconnecting the network elements. Figure 6-11 illustrates how an ASON signalling network could be supported on each topology. Common to each topology is that alternate diverse paths exist between the communicating entities (i.e., the ASON capable NEs). Note that to support alternate diverse paths between communicating ASON NEs under a linear topology, an external WAN link could be provided between the edge ASON NEs.

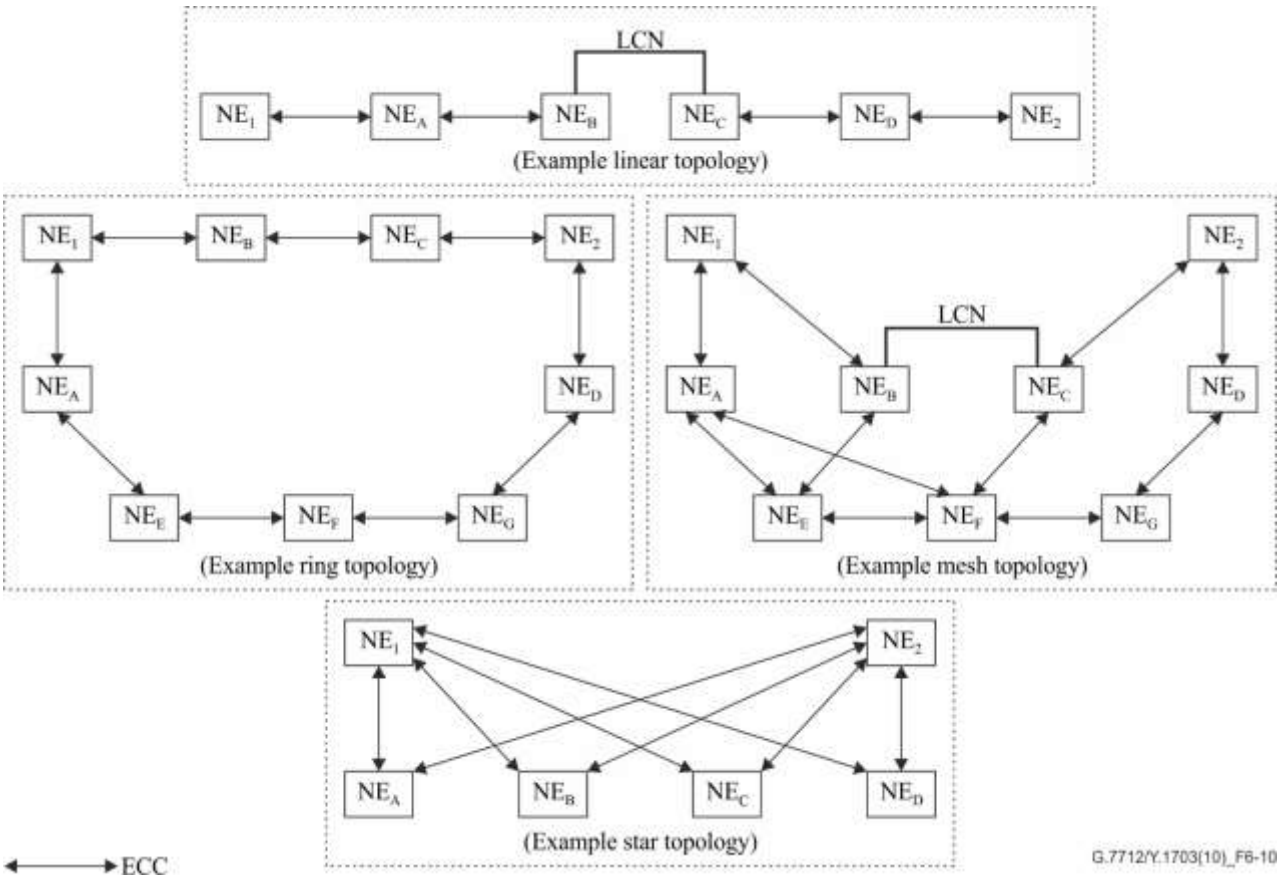


Figure 6-10 – Example topologies

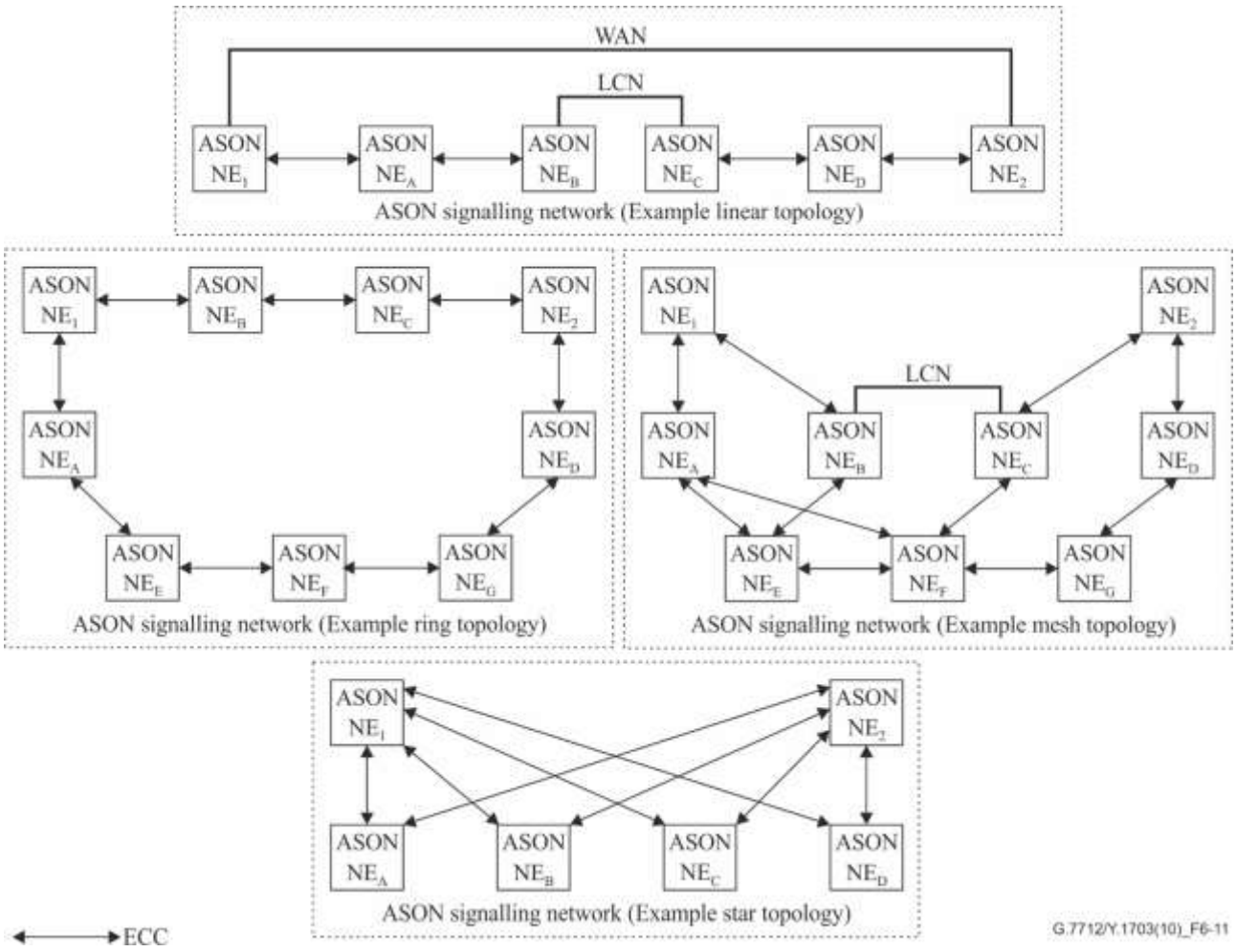


Figure 6-11 – Supporting an ASON signalling network on various topologies

Figure 6-12 illustrates how the ASON signalling network could consist of three different portions: the customer-network portion, the intra-administrative domain portion, and the inter-administrative domain portion. This example shows a mesh topology utilizing ECCs, LCNs (e.g., Ethernet LAN), and leased lines (e.g., DS1/E1, VC-3/4) as the physical links interconnecting the ASON NEs. The topology of the intra-administrative domain portion allows signalling to have alternate diverse paths between two communicating ASON NEs. The topology of the inter-administrative domain portion depends on agreements between administrative domains A and B. This example illustrates dual access points between the administrative domains. The topology of the customer-network portion depends on agreements between the customer and service provider. This example illustrates a single access point between the customer and the network.

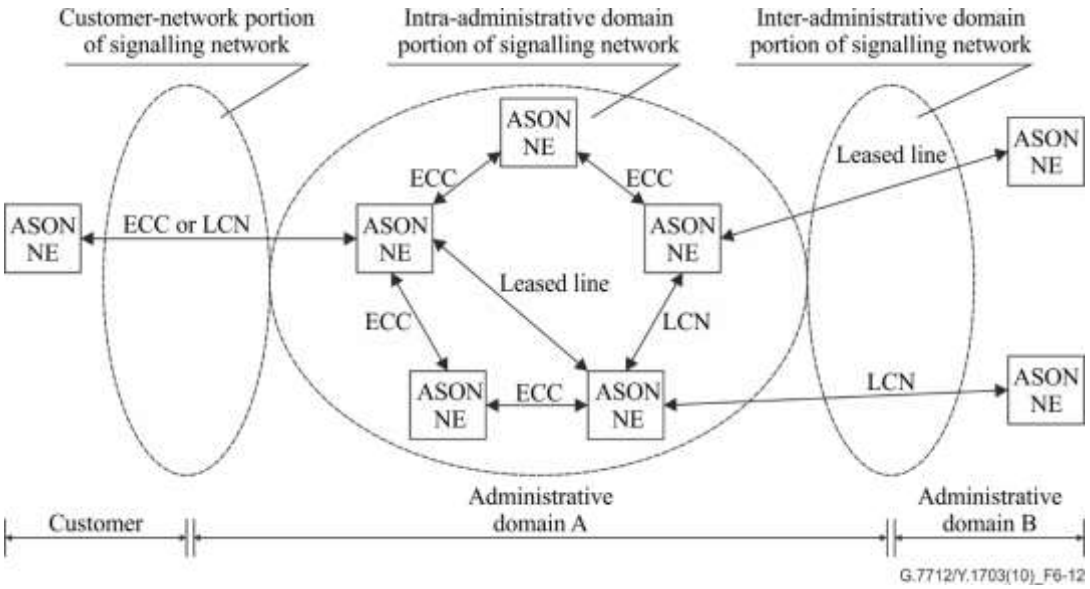


Figure 6-12 – Example ~~SCN~~CCN

6.2.2 Reliability of ~~SCN~~CCN

Figure 6-13 illustrates ASON control messages being transported over a CCN~~SCN~~. It illustrates the following logical interfaces:

User-to-network interface (UNI);

Network-to-network interface (NNI);

Connection controller interface (CCI).

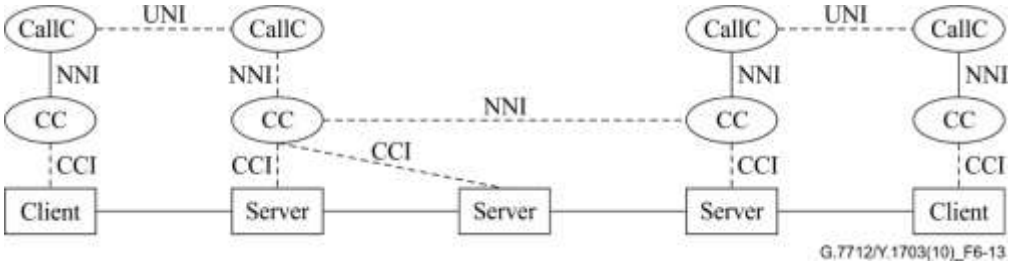


Figure 6-13 – ASON interfaces supported on ~~SCN~~CCN

In this example, the messages across the UNI, NNI, and CCI logical interfaces are carried via the CCN~~SCN~~ network. The CCN~~SCN~~ may consist of various subnetworks, where logical links in some subnetworks may share common physical routes with the transport network, but such a configuration is neither required nor excluded.

It is possible for the CCN~~SCN~~ to experience an independent failure from the transport network. Such a scenario is illustrated in Figures 6-14 and 6-15. In this example, which focuses on ASON messages transported over the CCN~~SCN~~, an independent failure to the CCN~~SCN~~ would affect new connection setup and connection tear-down requests.

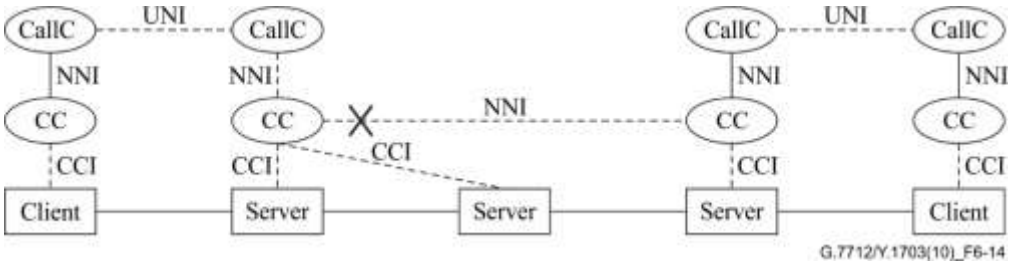


Figure 6-14 – ~~SCN~~ CCN failure impacting signalling interface

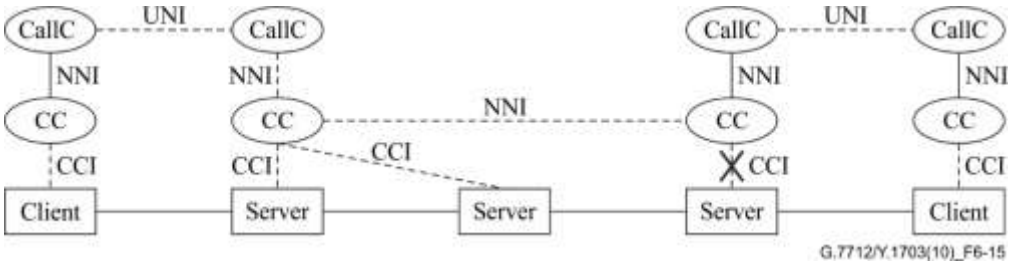


Figure 6-15 – CCN ~~SCN~~ failure impacting CCI interface

As indicated in Figure 6-15, it is also possible for some logical links within the CCN ~~SCN~~ to share common physical routes with the transport network. In this case, it is possible for the CCN ~~SCN~~ to experience a failure that is not independent from the transport network (i.e., failure interrupts both CCN ~~SCN~~ traffic as well as transport traffic), as shown in Figure 6-16. In this example, which focuses on ASON messages transported over the CCN~~SCN~~, such a failure may impact restoration when ASON is used to provide restoration of existing connections. It is, therefore, critical for the CCN ~~SCN~~ to provide resiliency when transporting restoration messages.

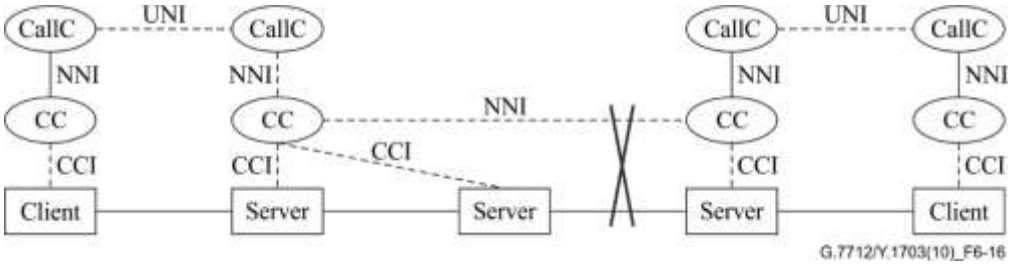


Figure 6-16 – CCN~~SCN~~ failure impacting both signalling and data interfaces

If the ASON application is only used to provide connection-setup and teardown, a connectionless CCN ~~SCN~~ may be sufficient. However, if the ASON application is also used to provide restoration, a connection-oriented CCN ~~SCN~~ may be required. A connection-oriented CCN ~~SCN~~ would require specification of additional functions to support connection-oriented network services.

The CCN ~~SCN~~ reliability requirements are as follows:

The CCN ~~SCN~~ shall support various levels of restoration depending on the reliability requirements of the communicating components for which it provides transport (i.e., restoration can be supported between those communicating components requiring highly reliable communications without requiring restoration to be supported among all communicating components).

One way of achieving reliable CCN ~~SCN~~ is through use of packet 1+1 protection for connection-oriented protocols such as MPLS as described in clause 6.2.4.

The ~~SCN~~ CCN may provide transport for restoration messages. In such a case, the ~~SCN~~ CCN should be fast enough to allow proper operation of the connections under control by these restoration messages control.

6.2.3 Security of CCN~~SCN~~

A CCN ~~SCN~~ supporting ASON messages may provide connectivity between different administrative domains. When a CCN ~~SCN~~ provides connectivity between administrative boundaries, precautions must be taken such that only those messages that are allowed to pass between the two administrative domains are able to cross the interface, while other messages which are not allowed to pass between administrative domains are prevented from crossing the interface. The CCN ~~SCN~~ needs to ensure that only a selected set of messages, which are allowed by the administrative parties on either side of the interface, are actually able to pass across the interface.

[b-IETF RFC 5920] describes the security threats relevant in the context of MPLS and generalized MPLS (GMPLS) (also relevant in the context of MPLS-TP) and the defensive techniques to combat those threats.

6.2.4 CCN ~~SCN~~ data communication functions

The DCF within the ASON entities shall support the ES (in OSI terms) or host (in IP terms) functionality.

- When the DCF within the ASON entities support ECC interfaces, the following functions are required to be supported:
  - ECC access function (as specified in clause 8.1);
  - ECC data-link layer termination function (as specified in clause 8.2);
  - "Network layer PDU into ECC data-link layer frame" encapsulation function (as specified in clause 8.3.1).
- When the DCF within the ASON entities support Ethernet LAN interfaces, the following functions are required to be supported:
  - Ethernet LAN physical layer termination function (as specified in clause 9.1);
  - "Network layer PDU into Ethernet frame" encapsulation function (as specified in clause 8.3.1.5).

The DCF within the ASON entities may operate as an intermediate system (IS) (in OSI terms), or as a router (in IP terms). The routing protocol used for DCF determines how to forward ~~SCN~~ CCN messages to their destination. The DCF within ASON entities that operate as IS/routers must be capable of routing within their Level-1 area and, therefore, must provide the functionality of a Level-1 IS/router. Additionally, the DCF within an ASON entity may be provisioned as a Level-2 IS/router, which provides the capability of routing from one area to another. The functionality of a Level-2 IS/router is not needed in the DCF of all ASON entities.

- When the DCF within the ASON entities operate as an IS/router, the following functions are required to be supported:
  - Network layer PDU forwarding function (as specified in clause 8.3.2);
  - Network layer routing function (as specified in clause 8.3.6).

The DCF within an ASON entity that supports IP may be connected directly to a DCF in a neighbouring ASON entity that supports only OSI.

- When the DCF within an ASON entity that supports IP is connected directly to a DCF in a neighbouring TMN entity that supports only OSI, the following function is required to be supported in the DCF supporting IP:
  - Network layer PDU interworking function (as specified in clause 8.3.3).

The DCF within an ASON entity may have to forward a network layer PDU across a network that does not support the same network layer type.

- When the DCF within an ASON entity must forward a network layer PDU across a network that does not support the same network layer type, the following functions are required to be supported:
  - Network layer PDU encapsulation function (as specified in clause 8.3.4);
  - Network layer PDU tunnelling function (as specified in clause 8.3.5).

The DCF within an ASON entity that supports IP using OSPF routing may be connected directly to a DCF in a neighbouring ASON entity that supports IP using integrated IS-IS.

- When the DCF within an ASON entity that supports IP using OSPF routing is connected directly to a DCF in a neighbouring ASON entity that supports IP using integrated IS-IS, the following function is required to be supported in the DCF supporting OSPF:
  - IP routing interworking function (as specified in clause 8.3.7).

The DCF within the ASON entities may operate as a label edge router (LER).

When the DCF within the ASON entities operates as an LER, the following functions are required to be supported:

- If the DCF supports ECC interfaces, the "MPLS PDU into ECC data-link layer" encapsulation function (as specified in clause 9.3.1).
- If the DCF supports LAN interfaces, the "MPLS PDU into Ethernet frame" encapsulation function (as specified in clause 9.3.1.1).
- MPLS label switched path (LSP) signalling function (as specified in clause 9.3.2).
- MPLS LSP forwarding function (as specified in clause 9.3.3).
- MPLS LSP path computation function (as specified in clause 9.3.4).
- "Network layer PDU into MPLS" encapsulation function (as specified in clause 9.3.5).

The DCF within the ASON entities may operate as a label switched router (LSR).

When the DCF within the ASON entities operate as an LSR, the following functions are required to be supported:

- If the DCF supports ECC interfaces, the "MPLS PDU into ECC data-link layer" encapsulation function (as specified in clause 9.3.1).
- If the DCF supports LAN interfaces, the "MPLS PDU into Ethernet frame" encapsulation function (as specified in clause 9.3.1.1).
- MPLS LSP signalling function (as specified in clause 9.3.2).
- MPLS LSP forwarding function (as specified in clause 9.3.3).

The DCF within the ASON entities may provide packet 1+1 protection capability.

The minimum requirements to provide packet 1+1 protection service are as follows:

- There is no additional capability required on the interior nodes of the network;
- The network should support the establishment of diversely routed connections.
- *Ingress node*
  - Must be able to associate the two connections that are used to provide packet level 1+1 protection between two end nodes;
  - Must support the carrying of an identifier in the packet which will be used to identify duplicate copies of a packet at the egress node;
  - Must be able to dual-feed each packet on these two mated connections.

- *Egress node*
  - Must be able to associate the two connections that are used to provide packet level 1+1 protection between two end nodes;
  - Must be able to identify the duplicate copies of a dual-fed packet using the identifier;
  - Must be able to select and forward one, and only one, copy of a packet.

The mechanism to associate the two diverse connections as well as the format and location of the sequence identifier shall be as described in clause 9.3.6.

6.3 SDN application

SDN controllers require a communication network, which is referred to as the control communication~~s~~ network (CCN) to transport SDN control messages between SDN components (e.g., SDN controller to the NEs, SDN controller to SDN controller, SDN controller to SDN applications).

Figure 6-17 illustrates an example relationship of the CCN and the SDN. The interfaces between the various elements, as illustrated in Figure 6-17, are logical and can be supported over a single physical CCN interface, or multiple CCN interfaces.

Figure 6-18 illustrates an example of a physical implementation of a CCN supporting control communications for SDN network. Depending on the choice of implementation of the CCN, the physical elements may support any combination of CCN interfaces, LAN interfaces, and WAN interfaces. Figure 6-18 also illustrates the types of control functional blocks that can be supported in various physical elements. Refer to [ITU-T G.7702] for detailed specifications regarding these control functional blocks. A DCF is part of each physical element and provides data communication functionality.

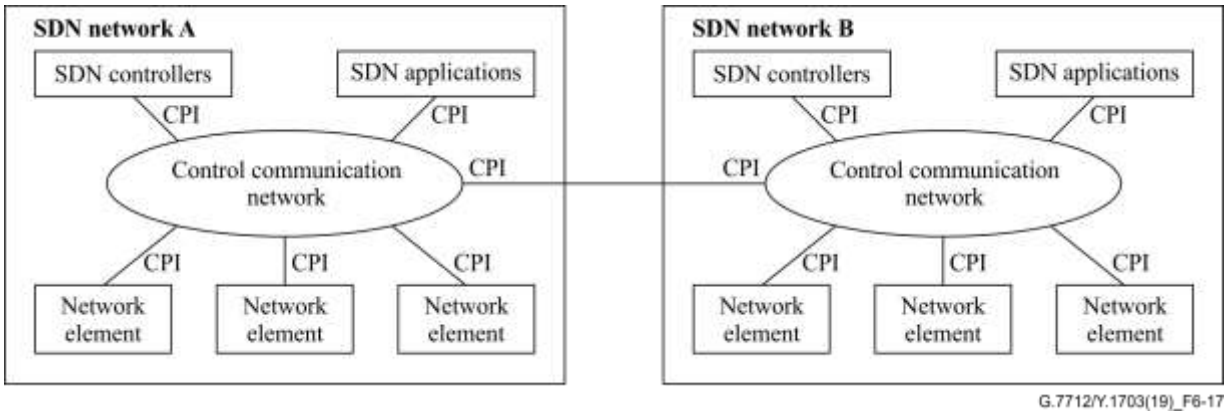


Figure 6-17 – Example relationship of SDN interfaces to CCN

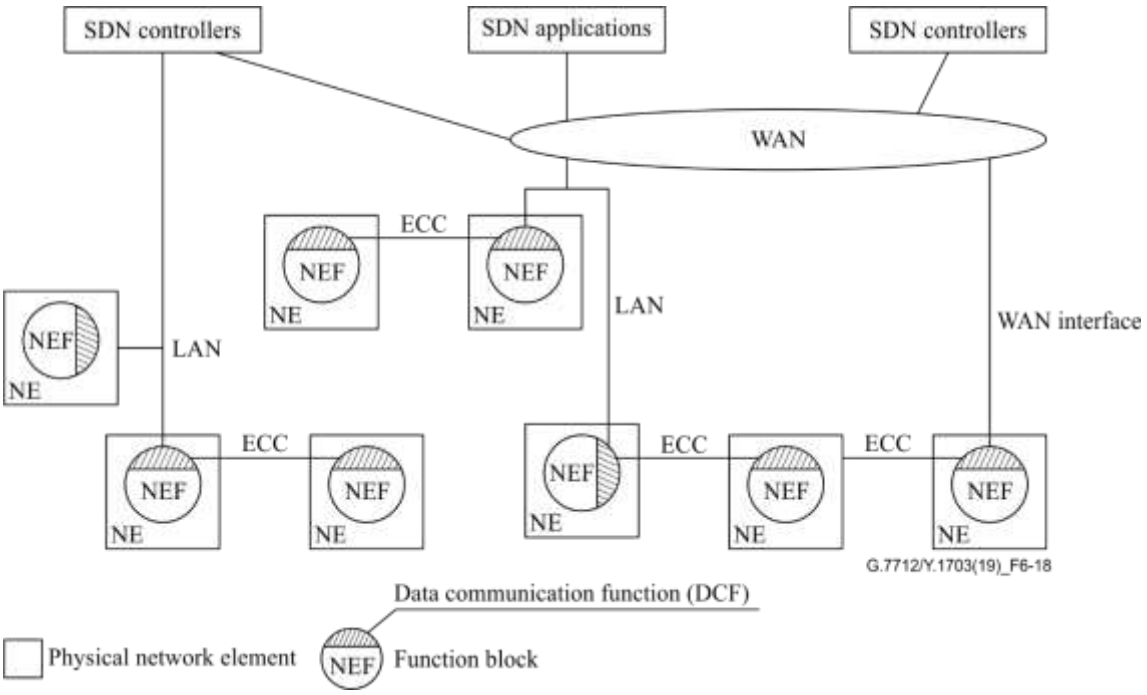


Figure 6-18 – Example of physical implementation of CCN supporting SDN

6.3.1 Supported SDN interfaces

SDN controllers can be arranged in multi-levels hierarchy. Each SDN controller instance can be implemented as a centralized SDN controller instance or can be implemented in a distributed way be a federation of functional SDN controller components. The CCN for SDN network needs to support ~~both intra-SDN controller communications, i.e., communication between components as defined in [ITU-T G.7702], and also~~ inter-SDN controller communication, i.e., the communication between the high-level controller and low-level controllers. The interworking of components in different levels of SDN controllers are also depicted in [ITU-T G.7702]. Communications between SDN applications and SDN controllers also need to be supported by the CCN.

6.3.2 Topology of SDN communications

An SDN controller communicates with others at its adjacent level in the hierarchical arrangement of SDN controllers, SDN controllers may communicate with another SDN controller at an adjacent level, or communicate with SDN applications when there is an SDN application on top of it. The SDN controller has no sense whether it is another SDN controller or SDN application communicating with it. An SDN controller could communicate directly with physical NEs when it has the scope of the resource as transport name space (i.e., the FP name space); this can occur at any level of a hierarchy as any level may have access to a resource view with FP name spaces.

6.3.3 Reliability of SDN communications

The control messages crossing the CCN network are critical for operations of the network. It is possible for the CCN to experience failure which could be independent from the transport network or coupled with failure of the transport network. Ways of achieving reliable CCN could be through use of packet 1+1 protection for connection-oriented protocols such as MPLS as described in clause 6.2.4 or any other redundancy technology.

6.3.4 Security of SDN communications

A CCN supporting SDN control messages communication may provide connectivity 1) between ~~SDN control components~~ SDN controllers, and 2) between SDN applications and SDN controllers ~~components~~. The SDN applications may reside on a customer's network domain and SDN controllers reside on an operator's network domain. The SDN controllers may control the resources of different layer networks which may be in different ~~MCC~~control domains. When a CCN provides connectivity that crosses the boundary between different ~~MCC~~ control domains, precautions must be taken such that only those messages that are allowed to pass between the two ~~MCC~~ control domains are permitted to cross the boundary.

[b-ONF TR-530] "Threat analysis for SDN architecture" describes the threats to SDN controllers, SDN NE and SDN applications. [b-ONF TR-529] "Security Foundation Requirements for SDN Controllers" describes defensive techniques to combat these threats.

6.4 Other applications requiring communication networks

Besides TMN, ASON and SDN applications, other applications such as overhead communication (e.g., optical channel (OCh) or optical tributary signal group (OTSiG) non-associated overhead), voice communications (e.g., orderwire), software downloads and operator specific communications require a communication network to provide transport of information between components.

A DCN that is used for overhead communication is referred to as the OCN. The OCN provides one or more channels for the communication of the overhead. These channels are referred to as the overhead communications channel (OCC). Described below is an application of the OCN for OCh and OTSiG non-associated layer overhead communication.

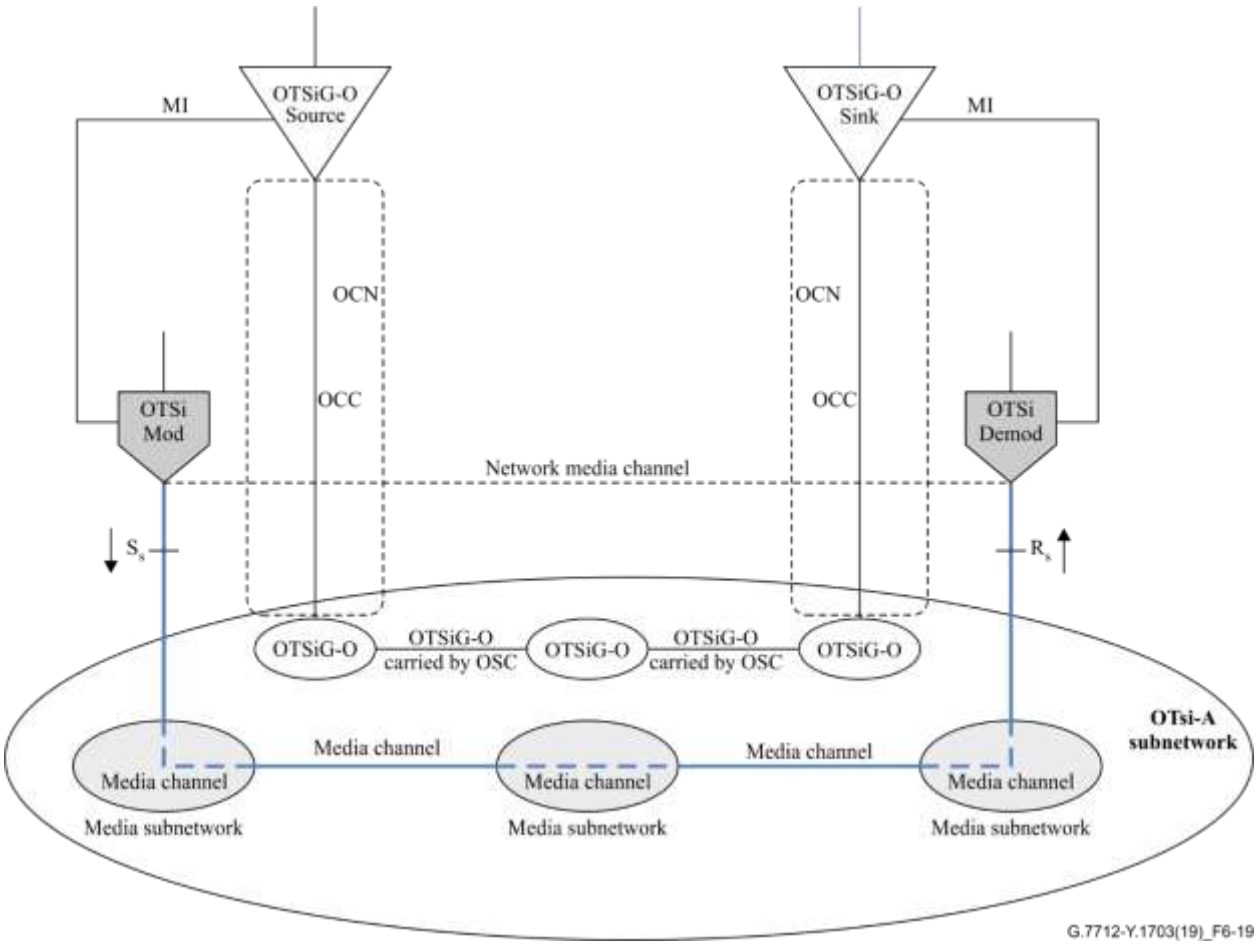
6.4.1 OTSiG|OCh non-associated overhead communication application

The OTSiG|OCh network uses non-associated overhead (OTSiG|optical channel overhead (OCh-O)), which is normally transported in the OTM-n.m via the optical transport module (OTM) overhead signal (OOS) carried in the optical supervisory channel (OSC). For the case where an OTSiG|OCh signal is transported in a single channel intra-domain interface as described in [ITU-T G.698.1] and [ITU-T G.698.2], the OSC may not be available. To transport this across the interface between the media|OCh subnetwork and the OTSiG|OCh source/sink, an OCC within the overhead communications network (OCN) is used as shown in Figure 6-19. The OTSiG|OCh-O messages must be carried in a PDU that is encapsulated into the OCN packet/frame format for the technology used in the OCN. The OTSiG|OCh-O PDU must contain sufficient information so that the source, sink and intermediate points can verify the connectivity.

In this application, the OCN provides point-to-point connectivity between two OTSiG|OCh-O connection points (OTSiG|OCh-O CP) to transport the OTSiG|OCh-O associated with the OTSiG and OCh payload (OCh-P). See Figure 6-19 (from Figure 12-1 of [ITU-T G.872]). The OCN should be able to support one or more of these point-to-point connections simultaneously.

An OCN should be designed to ensure that a single fault does not prevent the transfer of the OTSiG|OCh-O messages. The OCN should be designed to ensure that the messages are delivered correctly and does not impose blocking or excessive delay.

The protocol used for OTSiG|OCh–O communication is defined in Annex D.



NOTE 1 – From Figure ~~12~~17-1 of [ITU-T G.~~872~~807]
NOTE 2 – S_s and R_s in this figure identify the reference points defined in [ITU-T G.698.1] and [ITU-T G.698.2].

Figure 6-19 – OTSiG overhead transport for the case of single channel IaDI

6.5 Separation of various applications

Depending on the network design, network size, link capacity, security requirements and performance requirements, various levels of separation between the multiple applications (e.g., TMN, ASON, SDN) are possible. The level of separation that is provided is a choice that is made among operators and vendors when designing the network. The following are examples of various levels of separation.

Option A: The DCN can be designed such that the MCN, ~~SCN~~CCN, and other applications (e.g., operator-specific communications) are supported on the same Layer 3 network (e.g., share the same IP network).

Option B: The DCN can be designed such that the MCN, ~~SCN~~CCN, and other applications (e.g., operator-specific communications) are supported on separate Layer 3 networks; however, they may share some of the same physical links.

Option C: The DCN can be designed such that the MCN, ~~SCN~~CCN, and other applications (e.g., operator-specific communications) are supported on separate physical networks (i.e., separate Layer 3 networks that do not share any of the same physical links).

7 DCN functional architecture

The DCN architecture requirements in this clause apply to IP-only domains, OSI-only domains, and mixed IP+OSI domains. The DCN architecture requirements are technology independent. Technology-specific Recommendations such as [ITU-T G.784] for SDH and [ITU-T G.874] for OTN will specify which requirements are applicable for that particular technology.

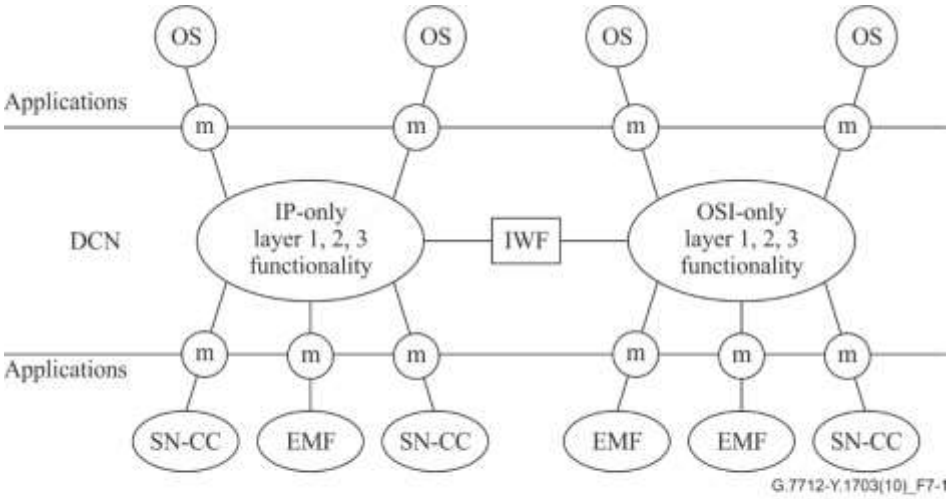
The DCN is aware of Layer 1, Layer 2, and Layer 3 protocols and is transparent to upper-layer protocols used by the applications for which it transports.

A DCN may be designed such that only IP is supported. A DCN supporting only IP may consist of various subnetworks using different physical and data link layer protocols; however, all subnetworks will support IP as the network layer protocol.

However, since embedded DCN networks support OSI, some DCNs may consist of parts that support IP-only, parts that support OSI-only, and parts that support both IP and OSI.

Those parts of the DCN supporting IP (i.e., either those parts supporting only IP or those parts supporting IP and OSI) may consist of DCFs that support IP-only (i.e., a single stack IP-only DCFs) and/or DCFs supporting IP and OSI (e.g., a dual-stack DCF which is capable of routing both IP and OSI packets). Those parts of the DCN supporting only OSI would consist of DCFs that support OSI-only (i.e., a single stack OSI-only DCF).

Figure 7-1 illustrates the functional architecture of the DCN. As discussed above, the DCN may be composed of parts that only support IP, parts that only support OSI, and parts that support both IP and OSI. An IWF between those parts of the DCN supporting IP-only, OSI-only, and IP and OSI, and mapping functions which map applications to the IP layer are also specified. To provide such transport, the DCN supports Layer 1 (physical), Layer 2 (data-link), and Layer 3 (network) functionality. The architecture requirements for those parts of the DCN supporting IP only, OSI only as well as the requirements for interworking between those parts of the DCN supporting IP-only, OSI-only, and IP and OSI are specified. The cloud in Figure 7-1, representing the IP-only part of the DCN, is an abstract view of the DCN and therefore may also apply to a single IP NE interconnected to OSI NEs via an IWF.



EMF Equipment Management Function.
IWF Interworking Function.
m Mapping between application and DCN.
OS Operations System.
SN-CC Subnetwork Connection Controller.

Figure 7-1 – Functional architecture of DCN

8 Data communication function requirements

This clause provides specifications for various data communication functions related to ECC interfaces, [IEEE 802.3] Ethernet LAN interfaces, and network layer capabilities.

8.1 L1 Physical layer requirements

An ECC access function provides access to the ECC bit stream. This function is defined in technology-specific equipment Recommendations (e.g., [ITU-T G.783] (SDH), [ITU-T G.798] (OTH), and [ITU-T G.8021] (Ethernet transport)). The bit rates and definitions of the various ECCs (e.g., data communication channel (DCC), general communication channel (GCC), and general management communications overhead (COMMS OH) in OSC) are provided in the technology-specific Recommendations (e.g., [ITU-T G.784], [ITU-T G.874], and [ITU-T G.8051]).

8.2 L2 Data link layer requirement

An ECC data-link layer termination function provides the common data-link layer processing regardless of the network layer PDU encapsulated within the data-link layer frame. The mapping of the data-link layer frame into the ECC is also provided by this function. This function is specified in the technology-specific Recommendations. However, the specification for the SDH ECC data-link layer termination function, the OTN ECC data-link layer termination function, ~~and~~ the MPLS-TP SCC data-link layer termination function and the MTN ECC data-link layer termination function is provided below.

8.2.1 SDH ECC (DCC)

8.2.1.1 Mapping the data-link layer frame into the SDH ECC

The high-level data link control (HDLC) framed signal is a serial bit stream containing stuffed frames surrounded by one or more flag sequences. The HDLC framed signal format is defined in [ITU-T Q.921] for link-access procedure D-channel (LAPD), and [IETF RFC 1662] for point-to-point protocol (PPP) in HDLC framing. A HDLC frame consists of N octets as presented in Figure 8-1. The HDLC frame is transmitted right to left and top to bottom. A 0 bit is inserted after all sequences of five consecutive 1 bits within the HDLC frame content (octets 2 to N–1) ensuring that a flag or abort sequence is not simulated within a frame.

The mapping of the HDLC framed signal into the DCC channel is bit-synchronous (rather than octet-synchronous) since the stuffed HDLC frame does not necessarily contain an integer number of octets as a consequence of the 0-insertion process. Therefore, there is no direct mapping of a stuffed HDLC frame into bytes within a DCC channel. The HDLC signal generator derives its timing from the ServerLayer/DCC_A function (i.e., the DCC_CI_CK signal) for SDH. The following ServerLayer/DCC_A functions are defined in [ITU-T G.783]: MSn/DCC_A function, MS256/DCC_A function, and RSn/DCC_A function.

The HDLC framed signal is a serial bit stream and will be inserted into the DCC channel such that the bits will be transmitted on the STM-N in the same order that they were received from the HDLC frame signal generator.

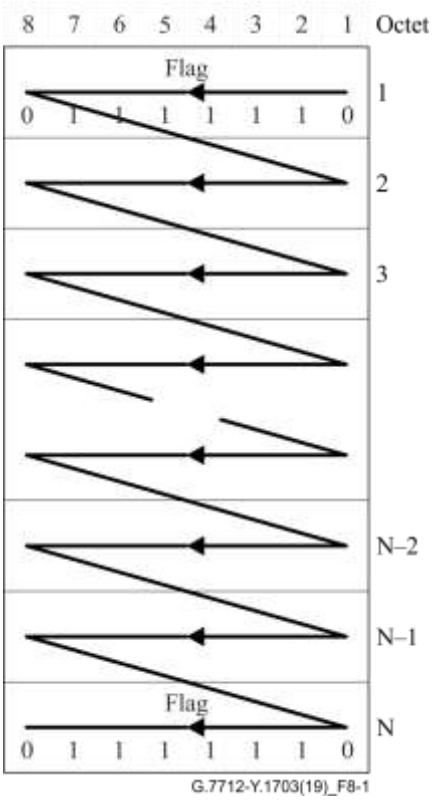


Figure 8-1 – HDLC frame format

8.2.1.2 SDH ECC data-link layer protocol specification

The three types of interfaces identified are: IP-only interfaces, OSI-only interfaces, and dual interfaces (dual interfaces are interfaces that can carry both IP and OSI packets). When carrying only IP over the DCC, PPP in HDLC framing shall be used as the data-link layer protocol. Since dual interfaces can carry both IP and OSI, it is possible for a dual interface to be connected to either an IP-only interface, an OSI-only interface, or another dual interface. OSI-only interfaces exist in networks today, and the data-link protocol used on such interfaces is LAPD as defined in [ITU-T G.784]. To allow dual interfaces to connect to either an IP-only interface or an OSI-only interface, the data-link layer protocol supported on a dual interface must be configurable to support either PPP in HDLC or LAPD. An exception is allowed for embedded SDH NEs supporting LAPD in hardware that are upgraded to support dual interfaces. To limit the amount of hardware upgrades, it is allowed for upgraded SDH NEs to support only LAPD.

8.2.1.2.1 IP-only interface

IP-only interfaces are illustrated in Figure 8-2.

Figure 8-2 – IP-only interface

IP-only interfaces shall use PPP as per [IETF RFC 1661] and [IETF RFC 1332].

8.2.1.2.2 OSI-only interface

OSI-only interfaces are illustrated in Figure 8-3.

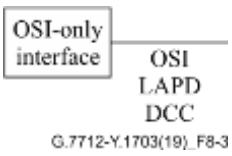


Figure 8-3 – OSI-only interface

OSI-only interfaces shall use LAPD as per [ITU-T G.784].

8.2.1.2.3 Dual interface (IP+OSI)

Dual interfaces (dual interfaces are interfaces that can carry OSI and IP packets) can be connected to IP-only interfaces, OSI-only interfaces, or other dual interfaces. To allow dual interfaces to be connected to other IP-only interfaces or other OSI-only interfaces, the data-link protocol on the dual interface must be configurable to switch between PPP in HDLC framing (as per [IETF RFC 1662]) and LAPD (as per [ITU-T G.784]) as illustrated in Figure 8-4. Note that embedded SDH NEs supporting LAPD in hardware that are upgraded to support IP are not required to support PPP in HDLC framing on its dual interfaces. Therefore, its dual interfaces are only required to support LAPD.

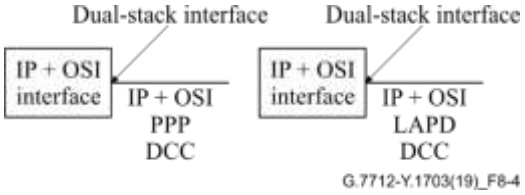


Figure 8-4 – Dual interface

Dual interfaces supporting PPP shall use PPP as per [IETF RFC 1661], [IETF RFC 1332], and [IETF RFC 1377].

Dual interfaces supporting LAPD shall use LAPD as per [ITU-T G.784].

8.2.2 OTN ECC (GCC)

8.2.2.1 Mapping the data-link layer frame into the OTN GCC (OTN COMMS channel)

The HDLC framed signal is a serial bit stream containing stuffed frames surrounded by one or more flag sequences. The HDLC framed signal format is defined in [IETF RFC 1662] for PPP in HDLC framing. A HDLC frame consists of N octets as presented in Figure 8-1. The HDLC frame is transmitted right to left and top to bottom. A 0 bit is inserted after all sequences of five consecutive 1 bits within the HDLC frame content (octets 2 to N–1) ensuring that a flag or abort sequence is not simulated within a frame.

The mapping of the HDLC framed signal into the GCC channel (GCC0, GCC1, and GCC2) is bit-synchronous (rather than octet-synchronous) since the stuffed HDLC frame does not necessarily contain an integer number of octets as a consequence of the 0-insertion process. Therefore, there is no direct mapping of a stuffed HDLC frame into bytes within a GCC (COMMS) channel. The HDLC signal generator derives its timing from the ServerLayer/COMMS_A function (i.e., the COMMS_CI_CK signal) for OTN. The following ServerLayer/COMMS_A functions are defined in [ITU-T G.798]:

- OTUk[V]/COMMS_A (GCC0);
- ODUkP/COMMS_A or optical channel data unit (ODUk)/COMMS_AC (GCC1 and GCC2).

[ITU-T G.709] also defines the COMMS OH as the general ECC for OTM-N interfaces (OTN OOS). The specific physical frame structure and coding for the COMMS OH is outside the scope of [ITU-T G.709]. Therefore, the corresponding adaptation functions are for further study.

The HDLC framed signal is a serial bit stream and will be inserted into the GCC channel such that the bits will be transmitted on the OTM-N interface in the same order that they were received from the HDLC framed signal generator as depicted in Figure 8-1.

8.2.2.2 OTN ECC data-link layer protocol specification

The three types of interfaces identified are: IP-only interfaces, OSI-only interfaces, and dual interfaces (dual interfaces are interfaces that can carry both IP and OSI packets). When carrying only IP over the GCC, PPP in HDLC framing shall be used as the data-link layer protocol. Since dual interfaces can carry both IP and OSI, it is possible for a dual interface to be connected to either an IP-only interface, an OSI-only interface, or another dual interface.

8.2.2.2.1 IP-only interface

IP-only interfaces are illustrated in Figure 8-5.

Figure 8-5 – IP-only interface

IP-only interfaces shall use PPP as per [IETF RFC 1661] and [IETF RFC 1332].

8.2.2.2.2 OSI-only interface

OSI-only interfaces are illustrated in Figure 8-6.

Figure 8-6 – OSI-only interface

OSI-only interfaces shall use PPP as per [IETF RFC 1661] and [IETF RFC 1377].

8.2.2.2.3 Dual interface (IP+OSI)

Dual interfaces (dual interfaces are interfaces that can carry OSI and IP packets) can be connected to IP-only interfaces, OSI-only interfaces, or other dual interfaces.

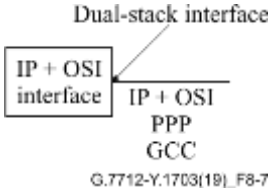


Figure 8-7 – Dual interface

Dual interfaces shall use PPP as per [IETF RFC 1661], [IETF RFC 1332], and [IETF RFC 1377].

8.2.3 MPLS-TP ECC

For MPLS-TP, the following options define how the control ~~plane~~ (signalling) communication can be carried with respect to the associated user traffic:

- In-band (see clause 8.2.3.1),
- Out-of-band (OOB), in-fibre (see clauses 8.2.3.1.1, 8.2.3.1.2, 8.2.3.1.5.1 and 8.2.3.1.5.2);
- Out-of-fibre, aligned topology;
- Out-of-fibre, independent topology (see clause 8.2.3.1.4).

The DCN architecture, as described in this Recommendation, supports all the options listed above.

The following possibilities are defined for constructing the signalling communication network (SCN):

- SCN link sharing a server layer trail with MPLS-TP user traffic;
- SCN link utilizing the MPLS-TP SCC as per [IETF RFC 5718];
- SCN link utilizing a dedicated MPLS-TP LSP;
- Separate and independent SCN link.

Note that in an MPLS-TP control domain, the terms signalling communication network (SCN) and communication channel (SCC) are used instead and they are equivalent to the generic terms control communication network (CCN) and control communication channel (CCC).

8.2.3.1 MPLS-TP SCN

8.2.3.1.1 SCN link sharing server layer trail with MPLS-TP user traffic

A SCN link sharing a server layer trail with MPLS-TP user traffic is an out-of-band, in-fibre configuration where the server layer trail provides both the SCN link as well as the MPLS-TP link. In this case, the SCN link and MPLS-TP link share the bandwidth provided by the common server layer trail as illustrated in Figure 8-8. Due to the bandwidth sharing, a traffic shaping and conditioning function may be needed to prevent the SCC from exceeding its committed bandwidth in congestion situations.

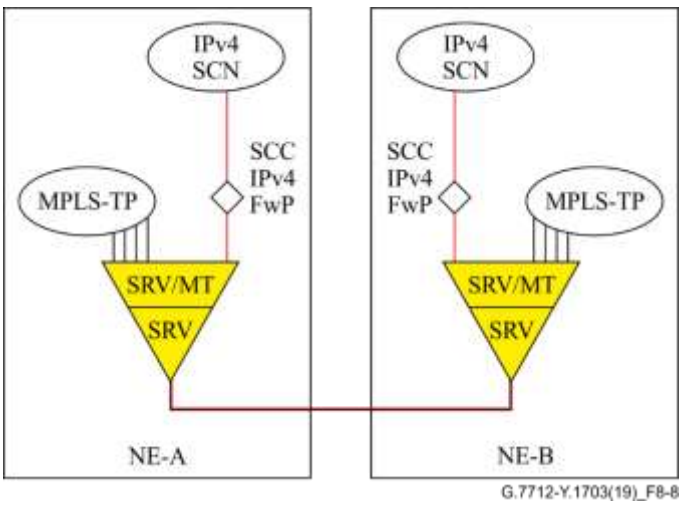


Figure 8-8 – Example of MPLS-TP NEs interconnected by a shared server trail providing an SCN link

As shown in Figure 8-8, the native SCN packets (e.g., IPv4/IPv6 or OSI CLNP packets) are directly encapsulated into the server layer. The server adaptation function recognizes SCN packets as non-MPLS frames and encapsulates them by using the related payload type identifier (e.g., by using the related user payload identifier (UPI) when generic framing procedure (GFP) encapsulation is used, or by using the related Ethertype when Ethernet encapsulation is used).

It is noted that the server layer payload type identifier may also be used for other data flows across the server layer trail and that the SCN packets may not be distinguishable from these other flows based on the server layer payload type identifier. In such cases, a deeper packet inspection may be needed (e.g., based on the destination address of the packet) to distinguish the SCN packets from the packets belonging to the other flows.

8.2.3.1.2 SCN MPLS-TP SCC as per [IETF RFC 5718]

A SCN link utilizing the MPLS-TP SCC as per [IETF RFC 5718] is an out-of-band, in-fibre configuration which is illustrated in Figure 8-9. In this case, the SCN link is provided by the MPLS-TP trail termination function and shares the bandwidth with the MPLS-TP user traffic (MPLS-TP LSPs) in a similar way as for the previous scenario. Due to the bandwidth sharing, a traffic shaping and conditioning function may be needed to prevent the SCC from exceeding its committed bandwidth in congestion situations.

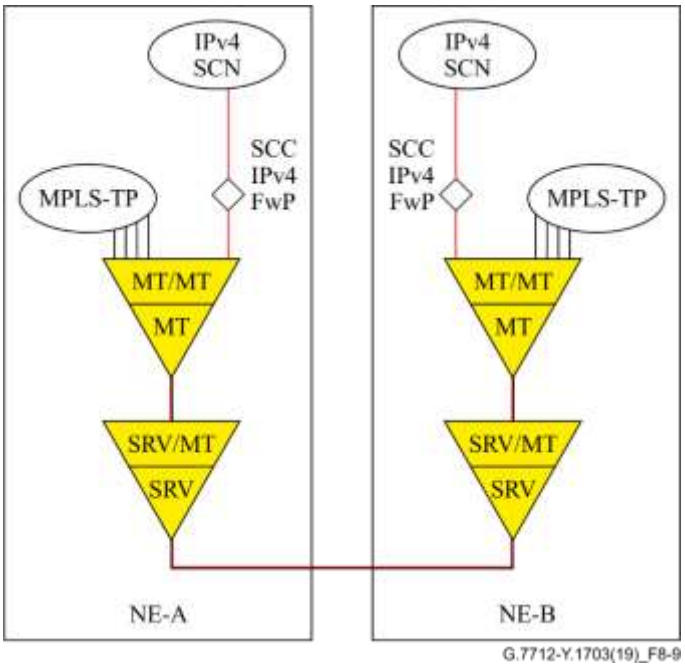


Figure 8-9 – MPLS-TP NEs interconnected by a MPLS-TP trail providing an SCN link

8.2.3.1.3 SCN link utilizing a dedicated MPLS-TP LSP

A SCN link utilizing a dedicated MPLS-TP LSP is an out-of-band, in-fibre configuration which is illustrated in Figure 8-10. The SCN link is created by establishing this dedicated MPLS-TP LSP. This dedicated MPLS-TP LSP can be multiplexed with the MPLS-TP LSPs carrying user traffic (MPLS-TP user traffic) which are transported over a common server layer trail.

In this case, the native SCN packets (e.g., IPv4/IPv6 or OSI CLNP packets) are encapsulated into a dedicated MPLS-TP trail as defined in [IETF RFC 3032]. This dedicated MPLS-TP trail must not be used for other traffic.

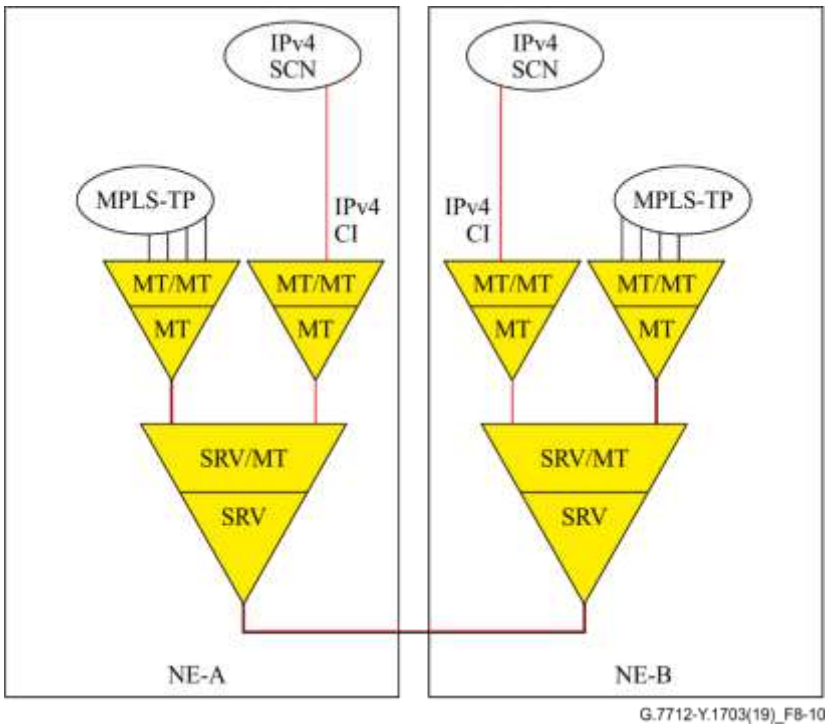


Figure 8-10 – MPLS-TP NEs interconnected by a dedicated MPLS-TP trail providing an SCN link

8.2.3.1.4 Separate and independent SCN links

Separate and thus independent SCN links can also be used for MPLS-TP. These are SCN links that do not share link resources carrying MPLS-TP traffic, and are thus independent of the MPLS-TP layer network topology.

The details of independent SCN links for MPLS-TP are outside the scope of this Recommendation.

8.2.3.1.5 MPLS-TP SCC data-link layer termination function

A more detailed description of the shared SCN link option, as defined in clause 8.2.3.1.1, is provided below.

8.2.3.1.5.1 Non-MPLS-TP server layer trail providing an SCN link (SCN link sharing a server layer trail with MPLS-TP user traffic)

Figure 8-11 shows a model of the SRV/MT_A adaptation function that includes the SCC and MCC forwarding points (FwP) in addition to the MPLS-TP connection points. The diamonds in the figure represent the traffic shaping and conditioning functions that may be needed to prevent the SCC and MCC forwarding points from exceeding their committed bandwidth in congestion situations.

Examples of non-MPLS-TP server layers providing an SCN link are:

- Ethernet PHY;
- GFP over SDH using virtual concatenation (VCAT);
- GFP over the OTN (ODUk).

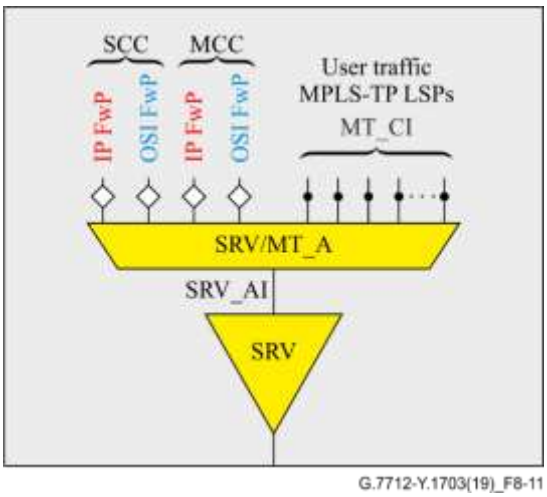


Figure 8-11 – MPLS-TP to server layer adaptation function providing SCC and MCC forwarding points

The SCC directly utilizes the IP and OSI forwarding points provided by the server layer.

The layer-2 code points (L2CPs, e.g., the Ethertype field in case of an Ethernet PHY or the UPI field in case of frame-mapped GFP (GFP-F)) are used to distinguish the SCC from the other flows such as the user traffic (MPLS-TP LSPs) and the MCC, unless the SCC and the MCC are sharing the same layer-2 code point (e.g., IPv4).

User traffic MPLS-TP LSPs (shown for the sake of completeness):

L2 header	L2CP=MPLS	MPLS-TP packet

SCC IPv4 packets:

L2 header	L2CP=IPv4	SCC IPv4 packet

SCC IPv6 packets:

L2 header	L2CP=IPv6	SCC IPv6 packet

SCC OSI packets:

L2 header	L2CP=OSI	SCC OSI packet

8.2.3.1.5.2 SCN link utilizing the MPLS-TP SCC as per [IETF RFC 5718]

[IETF RFC 5718] defines the packet format of the generic associated channel (G-Ach) SCC packet for MPLS-TP, which is based on the generic associated channel label (GAL)/G-ACh definition as per [IETF RFC 5586].

The specification of the MPLS-TP to SCC adaptation function can be found in Annex C.

8.2.3.1.5.3 SCN link utilizing a dedicated MPLS-TP LSP

IPv4 and IPv6 packets must be encapsulated into MPLS-TP as per [IETF RFC 3032].

The encapsulation of OSI CLNP packets into MPLS-TP is for further study.

8.2.3.2 MPLS-TP MCN

The same possibilities as described above for the SCN are defined for constructing the MCN:

- MCN link sharing a server layer trail with MPLS-TP user traffic;

- MCN link utilizing the MPLS-TP SCC as per [IETF RFC 5718];
- MCN link utilizing a dedicated MPLS-TP LSP;
- Separate and independent MCN links.

A more detailed description of the MCC data-link layer termination function is provided below.

8.2.3.2.1 Non-MPLS-TP server layer trail providing an MCN link (MCN link sharing a server layer trail with MPLS-TP user traffic)

Refer to clause 8.4.1. It shall be noted that a deeper packet inspection may be needed (e.g., based on the destination address of the packet) to distinguish the MCC packets from the SCC packets in case the same layer-2 code point is used for the MCC and the SCC.

8.2.3.2.2 MCN link utilizing the MPLS-TP MCC as per [IETF RFC 5718]

[IETF RFC 5718] defines the packet format of the G-ACh MCC packet for MPLS-TP, which is based on the GAL/G-ACh definition, as per [IETF RFC 5586].

The specification of the MPLS-TP to MCC adaptation function can be found in Annex C.

8.2.3.2.3 MCN link utilizing a dedicated MPLS-TP LSP

IPv4 and IPv6 packets must be encapsulated into MPLS-TP, as per [IETF RFC 3032].

The encapsulation of OSI CLNP packets into MPLS-TP is for further study.

8.2.4 EoT ECC

For further study.

8.2.5 MTN ECC

For the metro transport network (MTN), the following options define how the control communication can be carried with respect to the associated user traffic:

- in-band (see clause 8.2.5.2);
- out-of-band, in-fibre (see clause 8.2.5.1);
- out-of-fibre, independent topology (see clause 8.2.5.3).

The DCN architecture, as described in this Recommendation, supports all the options listed above.

The following possibilities are defined for constructing the control communication network (CCN):

- CCN link utilizing the MTNS MCC (MTN COMMS channel) as per [ITU-T G.8312];
- CCN link sharing MTNP trail with MTN user traffic;
- separate and independent CCN link.

During the automatic provisioning process for MTN NE, the MTN COMMS channel provided by the MTNS MCC is used to connect the MTN NE with the MC system. After that, the MC system can configure the MTN NE with which kinds of MTN CCN should be used for further operations.

8.2.5.1 CCN link utilizing the MTNS MCC (MTN COMMS channel)

A CCN link utilizing the MTN ECC as per [ITU-T G.8312] is an out-of-band, in-fibre configuration which is illustrated in Figure 8-12.

CCN frames can be Ethernet encapsulated and carried in the MTNS MCC (MTN COMMS channel). Figure 8-12 shows the architectures for this type.

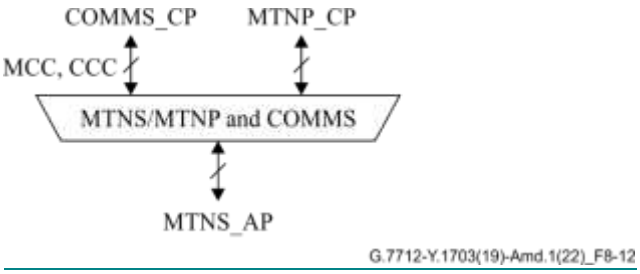


Figure 8-12 – CCN link utilizing the MTN COMMS channel

8.2.5.1.1 Mapping the data-link layer frame into the MTN ECC

The CCN packets should be encapsulated into the MAC frames and then encoded into a sequence of 64B/66B blocks as specified in clause 81 and clause 82.2.4 of [IEEE 802.3]. The sequence of blocks would be transmitted through the MTNS MCC block by block.

8.2.5.1.2 MTN ECC data-link layer protocol specification

When carrying IP (IPv4 or IPv6) over the MTNS MCC, the MAC frame shall be used as the data-link layer protocol. IP-only interfaces are illustrated in Figure 8-13.

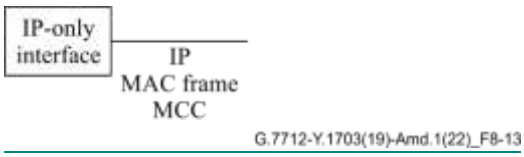


Figure 8-13 – IP-only interface

8.2.5.2 CCN link sharing MTNP trail with MTN user traffic

A CCN link sharing an MTNP trail with an MTN client (Ethernet MAC frame signal) is an in-band configuration where the MTNP trail provides both the client link as well as CCN link. Due to bandwidth sharing, a traffic shaping and conditioning function may be needed to prevent the CCN traffic from exceeding its committed bandwidth in congestion situations. The bandwidth for the CCN could be configured. This type of CCN has an advantage of large and configurable bandwidth in managing a large MTN network.

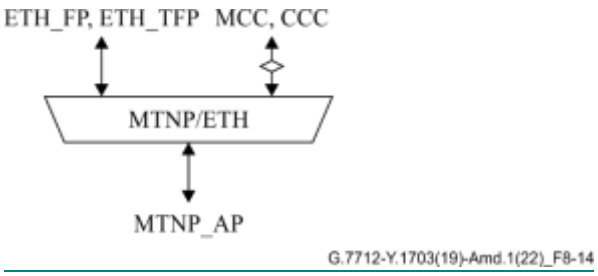


Figure 8-14 – CCN link sharing MTNP trail with MTN user traffic

Figure 8-14 shows a model of the MTNP/ETH adaptation function that includes the CCC and MCC forwarding points (FwP). The MTN CCN packets should be encapsulated into the MAC frames. The MTN CCN packets would be multiplexed with the MTN client packets in the MTNP/ETH function block. The MTNP/ETH adaptation function processes the MTN CCN packets as the usual MTN client packets.

To distinguish the MTN CCN packets with the MTN client packets sharing the same MTNP trail, the Ethertype field in the Ethernet frame may be used, when they use the different layer-2 code points; for example, MTN client traffic uses MPLS and MTN CCN packets use IPv4 or IPV6. It is noted that the Ethertype field value may be the same and then CCN packets may not be distinguishable from the MTN client traffic based on this field. In such cases, a dedicated VLAN ID for MTN CCN packets or a deeper packet inspection may be needed to distinguish the CCN packets from packets belonging to MTN client traffic.

8.2.5.3 Separate and independent CCN links

Separate and thus independent CCN links can also be used for MTN. These are CCN links that do not share link resources carrying MTN traffic, and are thus independent of the MTN layer network topology.

The details of independent CCN links for MTN are outside the scope of this Recommendation.

8.3 L3 Network layer requirements

8.3.1 L3 into L2 encapsulation function

A "Network layer PDU into ECC data-link frame" encapsulation function encapsulates and unencapsulates the network layer PDU into the data-link frame. This function also processes the protocol identifier. This function is defined in the technology-specific Recommendations. However, the specification for the "Network layer PDU into SDH ECC data-link frame" encapsulation function is provided below.

8.3.1.1 L3 into SDH ECC data-link frame encapsulation function

The specification of the "Network layer PDU into SDH ECC data-link frame" encapsulation function for IP-only interfaces, OSI-only interfaces, and dual interfaces is provided below.

8.3.1.1.1 IP-only interface

IP-only interfaces must use only PPPinHDLCframing/DCC, as per [IETF RFC 1662].

An IP-only interface is defined as follows:

The transmit end

– Shall put IS-IS packets directly into PPP information field, as per [IETF RFC 1661], with the OSI protocol value, as per [IETF RFC 1377], into the PPP protocol field;

– Shall put IPv4 packets directly into PPP information field, as per [IETF RFC 1661], with the IPv4 protocol value, as per [IETF RFC 1332], into the PPP protocol field;

– Shall put IPv6 packets directly into PPP information field, as per [IETF RFC 1661], with the IPv6 protocol value, as per [IETF RFC 2472], into the PPP protocol field.

The receive end

– An IS-IS packet is identified if the PPP protocol field has the OSI protocol value as per [IETF RFC 1377], and if the packet has the network layer protocol identifier (NLPID) for IS-IS, as specified in [ITU-T X.263];

– An IPv4 packet is identified if the PPP protocol field has the IPv4 protocol value, as per [IETF RFC 1332];

– An IPv6 packet is identified if the PPP protocol field has the IPv6 protocol value, as per [IETF RFC 2472].

8.3.1.1.2 OSI-only interface

OSI-only interfaces must use only LAPD/DCC, as per [ITU-T G.784].

An OSI-only interface is defined as follows:

The transmit end

– Shall put CLNP, IS-IS, and end system-to-intermediate system (ES-IS) packets directly into LAPD payload, as per [ITU-T G.784].

The receive end

– Shall inspect the protocol identifier located in the first octet of the LAPD payload. The value of this identifier is consistent with the values assigned in [ITU-T X.263]. If the PDU received is for a protocol not supported by the receiver, then the PDU shall be discarded.

8.3.1.1.3 Dual (IP+OSI) interface

A dual interface supporting PPP as the data-link protocol is defined as follows:

The transmit end

– Shall put CLNP, IS-IS, and ES-IS packets directly into PPP information field, as per [IETF RFC 1661], with the OSI protocol value, as per [IETF RFC 1377], into the PPP protocol field;

– Shall put IPv4 packets directly into PPP information field, as per [IETF RFC 1661], with the IPv4 protocol value, as per [IETF RFC 1332], into the PPP protocol field;

– Shall put IPv6 packets directly into PPP information field, as per [IETF RFC 1661], with the IPv6 protocol value, as per [IETF RFC 2472], into the PPP protocol field.

The receive end

– An OSI packet is identified if the PPP protocol field has the OSI protocol value, as per [IETF RFC 1377];

– An IPv4 packet is identified if the PPP protocol field has the IPv4 protocol value, as per [IETF RFC 1332];

– An IPv6 packet is identified if the PPP protocol field has the IPv6 protocol value, as per [IETF RFC 2472].

A dual interface supporting LAPD as the data-link protocol is defined as follows:

The transmit end

– Shall put CLNP, IS-IS, and ES-IS packets directly into LAPD payload as per [ITU-T G.784];

– Shall put IP packets directly into LAPD payload, with a one-octet protocol identifier prepended. This identifier will be consistent with [ITU-T X.263] assigned values for IPv4 and IPv6.

The receive end

– Shall inspect the protocol identifier located in the first octet of the LAPD payload. The value of this identifier is consistent with the values assigned in [ITU-T X.263]. If the PDU received is for a protocol not supported by the receiver, then the PDU shall be discarded.

8.3.1.2 L3 into MPLS-TP SCC data-link frame encapsulation function

The G-ACh, as defined in [IETF RFC 5586], can be used to carry SCC messages over an MPLS-TP section or a MPLS-TP segment. An SCC message is encapsulated as per [IETF RFC 5718]. The channel type field must be set to 0x0002 indicating that the packet is a G-ACh SCC packet carrying an SCC message. The PPP protocol identifiers, as per [IETF RFC 1661] and [IETF RFC 3818], are used to indicate the PDU type of the SCC message. Examples are provided in Table 8-1 below:

Table 8-1 – Examples of PID values for G-ACh SCC packets

Protocol identifier (PID) value as per [IETF RFC 1661] and [IETF RFC 3818]	Protocol name
0x0021	Internet protocol version 4
0x0023	OSI network layer
0x0057	Internet protocol version 6

8.3.1.3 L3 into MPLS-TP MCC data-link frame encapsulation function

The G-ACh, as defined in [IETF RFC 5586], can be used to carry MCC messages over an MPLS-TP section or a MPLS-TP segment. An MCC message is encapsulated as per [IETF RFC 5718]. The channel type field must be set to 0x0001 indicating that the packet is a G-ACh MCC packet carrying an MCC message. The PPP protocol identifiers, as per [IETF RFC 1661] and [IETF RFC 3818], are used to indicate the PDU type of the MCC message.

8.3.1.4 L3 into EoT MCC data-link frame encapsulation function

For further study.

8.3.1.5 L3 into Ethernet frame encapsulation function

This function encapsulates and unencapsulates a network layer PDU into an IEEE 802.3 or Ethernet (version 2) frame.

It shall encapsulate network layer PDUs into IEEE 802.3 or Ethernet (version 2) frames according to the following rules:

- It shall encapsulate and unencapsulate CLNP, IS-IS, and ES-IS PDUs into IEEE 802.3 frames, as per [ITU-T Q.811];
- It shall encapsulate and unencapsulate IP packets into Ethernet (version 2) frames, as per [IETF RFC 894];
- IP addresses shall be mapped to Ethernet MAC addresses utilizing the address resolution protocol in [IETF RFC 826].

It shall determine the received frame type (IEEE 802.3 or Ethernet version 2), as per section 2.3.3 in [IETF RFC 1122].

8.3.2 L3 forwarding function

The network layer PDU forwarding function forwards network layer packets.

If this function forwards CLNP packets, it shall forward CLNP packets, as per [ITU-T Q.811].

If this function forwards IPv4 packets, it shall forward IPv4 packets, as per [IETF RFC 791].

If this function forwards IPv6 packets, it shall forward IPv6 packets, as per [IETF RFC 2460].

The preferred addressing format is IPv6. The IP routing protocol should be able to deal with IPv6 and IPv4 addressing.

8.3.3 L3 interworking function

The network layer PDU interworking function ensures that neighbouring DCF functions, running different network layer protocols can communicate. The DCF supporting IP is required to support OSI to allow communication to the neighbouring DCF supporting only OSI.

The network layer PDU interworking function between two IP networks is for further study.

8.3.4 L3 to L3 encapsulation function

The network layer PDU encapsulation function encapsulates and unencapsulates one network layer PDU into another network layer PDU.

CLNP packets shall be encapsulated over IP using generic routing encapsulation (GRE), as specified in [IETF RFC 2784], as payload in an IP packet using an IP protocol number of 47 (decimal) and with the *Don't Fragment* (DF) bit not set. As per [IETF RFC 2784], the GRE shall contain an Ethertype to indicate what network layer protocol is being encapsulated. The industry standard for OSI Ethertype, which is 00FE (hex) shall be used.

IP packets shall be encapsulated over connectionless network layer service (CLNS) using GRE, as specified in [IETF RFC 2784], as the data payload of a CLNP data type PDU, as specified in [ITU-T X.233], using a network service access point (NSAP) selector value of 47 (decimal) and with the segmentation permitted (SP) flag set. Further information is available in [b-IETF RFC 3147].

IP packets shall be encapsulated over IP using GRE, as specified in [IETF RFC 2784], as payload in an IP packet using an IP protocol number of 47 (decimal) and with the *Don't Fragment* (DF) bit not set.

As an option, the network layer PDU encapsulation function may forward PDUs across incompatible nodes via the automatic encapsulation procedure described in Annex B. Note that a DCF supporting the automatic encapsulation procedure, described in Annex B, is compatible with and can be deployed in the same area as a DCF that does not support the automatic encapsulation procedure.

8.3.5 L3 tunnelling function

The network layer PDU tunnelling function provides a static tunnel between two DCFs supporting the same network layer PDU. For a tunnel with a configured maximum transmission unit (MTU) size, any IP packet that cannot be forwarded over the tunnel because it is larger than the MTU size, and has its DF bit set, should be discarded, and an Internet control message protocol (ICMP) unreachable error message (in particular the "fragmentation needed and DF set" code), as per [IETF RFC 792], for IPv4 should be sent back to the originator of the packet. In the case of IPv6, the path MTU discovery procedure ensures that the source node only sends packets that are smaller than the minimum MTU along the path. However, in the unlikely event that an IP packet is received by an intermediate node that is larger than the MTU size of the link towards the next hop, the packet is dropped and an ICMP Packet Too Big message, as per [IETF RFC 4443], should be sent back to the originator of the packet.

8.3.6 L3 routing function

The network layer routing function routes network layer packets.

A DCF supporting OSI routing shall support IS-IS, as per [ISO/IEC 10589].

A DCF supporting IP routing shall support integrated IS-IS (see clause 8.3.6.1 for integrated IS-IS requirements) and may also support OSPF, as per [IETF RFC 2328] and [IETF RFC 2740], as well as other IP routing protocols.

8.3.6.1 Integrated IS-IS requirements

A DCF supporting integrated IS-IS shall support [IETF RFC 1195].

A DCF supporting integrated IS-IS shall support three-way handshaking on all point-to-point links (see Annex A for three-way handshaking requirements). Three-way handshaking modifies the adjacency creation and maintenance behaviour specified in [ISO/IEC 10589].

8.3.6.1.1 Network-layer protocol aware adjacency creation

The DCF shall include a "protocols supported" type length value (TLV) in all IS-IS hello (IIH) and intermediate system hello (ISH) PDUs on all interfaces, and in all link state protocol data units (LS-PDUs) with LS-PDU number 0, as per [IETF RFC 1195].

On receipt of an IS-IS ISH or IIH PDU, the DCF shall inspect the PDU to see if it contains a "protocols supported" TLV. This shall take place on all interfaces, whether LAN, DCC or other links. If an ISH or IIH PDU does not contain a "protocols supported" TLV, then it shall be treated as if it contains a "protocols supported" TLV containing only the NLPID for CLNP.

The DCF shall compare the NLPIDs listed in the "protocols supported" TLV (assuming only CLNP, if none, is present) with the network layer protocols that the DCF is itself capable of forwarding.

If no adjacency exists with the neighbour that sent the ISH or IIH, and if the DCF is not capable of forwarding any of the network layer protocols listed in the "protocols supported" TLV of the ISH or IIH received from the neighbour, then the DCF shall not form an adjacency with that neighbour.

If an adjacency does exist with the neighbour that sent the ISH or IIH, and if the DCF is not capable of forwarding any of the network layer protocols listed in the "protocols supported" TLV of the ISH or IIH received from the neighbour, then the DCF shall delete the adjacency with that neighbour and generate a ProtocolsSupportedMismatch event.

If the DCF is itself capable of forwarding one or more of the network layer protocols listed in the "protocols supported" TLV of a received ISH or IIH, then the DCF shall process the ISH or IIH as normal.

The DCF shall not consider the value of the "protocols supported" TLV of LS-PDUs during this process.

A DCF that cannot forward CLNP PDUs shall ignore end system hello (ESH) PDUs and consequently shall not advertise reachability to OSI end systems.

8.3.6.1.2 IS-IS domain-wide IP prefix distribution

DCFs supporting Level-1, Level-2 integrated IS-IS shall support the advertising of configured IP destination prefixes learned via Level-2 into Level-1 LS-PDUs, as well as IP destination prefixes learned via Level-1 into Level-2 LS-PDUs. The default behaviour, when no IP destination prefixes have been configured, shall be to not propagate any Level-2 prefixes into Level-1 LS-PDUs, while all Level-1 learned prefixes shall be propagated into Level-2 LS-PDUs.

8.3.6.1.2.1 Configuration prefixes

The operator shall provision two tables that control the propagation of prefixes. One table shall control propagation from Level-1 to Level-2, while the other controls propagation from Level-2 to Level-1.

8.3.6.1.2.2 Tagging of propagated prefixes

Since propagating prefixes from Level-2 into Level-1 and subsequently from Level-1 back into Level-2 can introduce routing loops, a tag is necessary to identify the source of the prefix. This tag, called the up/down bit, is stored in the previously unused high-order bit (bit 8) of the default metric field in IP reachability TLVs and IP external reachability TLVs. Existing implementations of IS-IS that support [IETF RFC 1195] will not be impacted by the redefinition of this bit, as [IETF RFC 1195] requires it to be set to zero when originating LS-PDUs, and ignored upon receipt. Further information is available in [b-IETF RFC 2966].

IP reachability TLVs and IP external reachability TLVs shall be processed in the same manner. The type of TLV received will be the same type used when the prefix is propagated from the Level-2 to a Level-1 area, as well as from a Level-1 area to the Level-2.

This is different from [IETF RFC 1195], which limited IP external reachability TLVs to appearing only in Level-2 LS-PDUs.

8.3.6.1.2.2.1 Transmission of LS-PDUs with IP reachability TLVs and IP external reachability TLVs

As with normal [IETF RFC 1195], the value of the up/down bit shall be zero for all IP TLVs in Level-2 LS-PDUs. The value of the up/down bit shall be zero for Level-1 LS-PDUs originated within a Level-1 area.

The up/down bit shall be set to one in an IP TLVs in Level-1 LS-PDU when a Level-1, Level-2 Integrated IS-IS NEs is propagating a configured prefix from Level-2 to Level-1.

8.3.6.1.2.2.2 Reception of LS-PDUs with IP reachability TLVs and IP external reachability TLVs

A DCF supporting integrated IS-IS shall ignore the value of the up/down bit when developing routes for use within a Level-1 area or for the Level-2.

A DCF supporting Level-1, Level-2 integrated IS-IS that receives an LS-PDU with an IP TLV for a prefix that matches an entry in the Level-1 to Level-2 propagation table shall advertise the appropriate prefix from Level-1 to Level-2.

A DCF supporting Level-1, Level-2 integrated IS-IS that receives an LS-PDU with an IP TLV with the up/down bit set to one shall never use the prefix for propagation of information from Level-1 to Level-2.

8.3.6.1.2.2.3 Use the up/down bit in Level-2 LS-PDUs

The use of up/down bit in Level-2 LS-PDUs is for further study.

8.3.6.1.2.3 Route preference

Given that prefixes can now be propagated from Level-2 to Level-1, the route preferences, specified in [IETF RFC 1195], must be updated to take into account this new source. The resulting route preference order is as follows:

1) L1 intra-area routes with internal metric;
   L1 external routes with internal metric.
2) L2 intra-area routes with internal metric;
   L2 external routes with internal metric;
   Inter-area routes propagated from L1 into the L2 with internal metric;
   Inter-area external routes propagated from L1 into the L2 with internal metric.
3) Inter-area routes propagated from L2 into an L1 area with internal metric;
   External routes propagated from L2 into an L1 area with internal metric.
4) L1 external routes with external metric.
5) L2 external routes with external metric;
   Inter-area external routes propagated from L1 into the L2 with external metric.
6) Inter-area external routes propagated from L2 into an L1 area with external metric.

8.3.7 L3 IP routing interworking function

A DCF supporting the IP routing interworking function shall support route-filtering mechanisms, per sections 7.5 and 7.6 of [IETF RFC 1812], so that networks with two routing protocols can be connected via more than one exchange point.

8.3.8 Applications to L3 mapping function

OSI applications running over (a part of) the DCN that only supports IP may be mapped into IP as specified in [ITU-T Q.812] dealing with [b-IETF RFC 2126] transmission control protocol (TCP)/IP

protocol profile. Such a mapping is a Layer 4 solution and is therefore outside the scope of this Recommendation. Another option for carrying OSI applications across (a part of) the DCN that only supports IP is to provide OSI over IP Layer 3 encapsulation as specified in clause 8.3.4.

The mapping of IP applications over (a part of) the DCN supporting IP shall be in accordance with IP suite specifications.

8.4 Other requirements

8.4.1 Provisioning requirements

Every NE must support the creation of an interface that does not have any physical manifestation. This interface must be provisionable with an IP address.

The LSP size shall be configurable.

This allows the MTU size within the domain to be set.

Area ID provisioning per interface, including ECC channels and LAN, is required for OSPF.

8.4.2 Security requirements

Care must be taken to avoid unwanted interactions (addresses, etc.) between a public IP network and a DCN supporting IP.

9 Specific DCN L3|L2|L1 technology requirements

9.1 Ethernet LAN as L1&L2

An Ethernet LAN physical termination function terminates the physical Ethernet interface, as defined in [IEEE 802.3].

One or more of the following rates shall be supported: 1 Mbit/s, 10 Mbit/s, 100 Mbit/s, 1Gbit/s or any other higher bitrate as defined in [IEEE 802.3].

Access to terminated ECC channels is allowed by network elements supporting Ethernet LAN interfaces. Not all network elements supporting ECC channels need to support Ethernet LAN ports, as long as there is an ECC path from a network element terminating the ECC channel and another network element providing Ethernet LAN ports.

9.2 Ethernet WAN as L1&L2

Ethernet transport technologies such as Ethernet frames over ODUk can be used to carry DCN messages as an in-band channel. The mapping of Ethernet frames to ODUk refer to [ITU-T G.709]

9.3 Native MPLS as L3

This clause describes aspects of using native MPLS as ECC (SCC or MCC). Additional clarification may be provided in a future revision of this Recommendation.

9.3.1 MPLS PDU into L2 encapsulation function

This function encapsulates and unencapsulates a MPLS PDU into an ECC data-link layer frame.

If PPP is the supported data link protocol on the ECC interface, the following is required:

– *At transmit end*

  Shall put MPLS packets directly into PPP information field as per [IETF RFC 1661], with the MPLS protocol value of 0281 hex into the PPP protocol field, as per [IETF RFC 3032], section 4.3, for MPLS Unicast.

– *At receive end*

An MPLS packet is identified if the PPP protocol field has the MPLS protocol value of 0281 hex, as per [IETF RFC 3032], section 4.3, for MPLS Unicast.

9.3.1.1 "MPLS PDU into Ethernet frame" encapsulation function

This function encapsulates and unencapsulates a MPLS PDU into an Ethernet (version 2) frame.

It shall encapsulate MPLS PDUs into Ethernet (version 2) frames, as per [IETF RFC 894], using an Ethertype value of 8847 hex as per [IETF RFC 3032], section 5, for MPLS Unicast.

9.3.2 MPLS LSP signalling function

The MPLS LSP signalling function provides the signalling necessary to set up the MPLS LSP.

A DCF supporting the MPLS LSP signalling function shall support the following reservation model: Explicit Path with a strict route via simple nodes (32 bits IP-address), for point-to-point unicast LSP, via the Reservation Style "FF" over IPv4.

The Path message is forwarded to the destination along a path specified by a list of IP-addresses in the explicit route object (ERO). Each node (LSR) in the path records the ERO. Via the Label Request object, the nodes (LSRs) provide label binding for the session. See [IETF RFC 3209] – RSVP-TE, sections 2.2, 3.1, 4.2 and 4.3.

The destination node responds with a Resv message, which is sent upstream towards the sender, in reverse order of the node-list in the ERO. The Label in the Label object of the Resv message is used in each intermediate LSR to associate outgoing traffic with this LSP. If the node is not the sender, it allocates a new Label and places that in the Label object of the Resv message, which it sends upstream to the previous HOP (PHOP). See [IETF RFC 3209] – RSVP-TE, sections 2.2 and 3.2 and 4.1.

If the node cannot fulfil the request, it sends a PathErr or ResvErr message to the sender node. See [IETF RFC 3209] – RSVP-TE, section 4.5.

The soft-state procedure of RSVP implies periodic sending of a full representation of the LSP state in Resv and Path messages to maintain the LSP. The Srefresh message is used in place of the periodic sending of standard Path and Resv messages. Each MessageID in the Srefresh message represents a full Path or Resv message, for which the state is not changed. See [IETF RFC 2961] – Resource Reservation Protocol – Overhead Reduction Extensions (RSVP-ORE), section 5.5.

A MESSAGE_ID_NACK object is used to indicate that a received MessageID does not match, and a full Path or Resv message is needed to restore the LSP. See [IETF RFC 2961] – RSVP-ORE, section 5.4.

A MESSAGE_ID_ACK object is used to acknowledge the receipt of messages containing the MESSAGE_ID object and for which the ACK_Desired flag is set. It is part of the Srefresh re-transmission algorithm as described in [IETF RFC 2961] – RSVP-ORE, section 6.3.

9.3.3 MPLS LSP forwarding function

The MPLS LSP forwarding function forwards the incoming MPLS packet to an outgoing interface based on its MPLS label and the next hop label forwarding entry (NHLFE), as per [IETF RFC 3031].

The sequence of packets must be maintained within an LSP.

9.3.4 MPLS LSP path computation function

The MPLS LSP path computation function calculates the path for a unidirectional LSP. This function shall be able to calculate paths for two unidirectional LSPs to the same destination such that their paths do not traverse the same node or subnetwork.

9.3.5 "Network layer packet into MPLS" encapsulation function

The "Network layer packet into MPLS" encapsulation function adds/removes the MPLS label stack entry to/from the network layer packet, as per [IETF RFC 3032].

9.3.6 MPLS packet 1+1 protection function

9.3.6.1 Associating two LSPs

The ingress and egress nodes shall identify and associate the two LSPs providing packet 1+1 service. This association between two LSPs can be established using either network management interface or signalling.

For the case of signalling, an identifier shall be transferred across each of the diverse LSPs. The identifier shall be identical on each of the diverse LSPs and shall be unique amongst LSPs initiated by the ingress node and amongst LSPs terminated by the egress node.

The specific mechanism for assigning the identifier, as well as how the identifier is transported within the signalling protocol, is for further study. The mechanism will be similar to the one required for associating LSPs for other MPLS-based protection mechanisms such as 1+1 or 1:1.

In order to meet the requirement that there are no signalling extensions required at the intermediate nodes, the identifier and the LSP service type (i.e., packet 1+1) shall be carried within opaque objects.

9.3.6.2 Sequence identifier format

The sequence number shall be used as the identifier for packet 1+1 protection. Each copy of the dual-fed packet is assigned the same unique sequence number by the ingress node. The sequence number of the next packet is generated by adding one to the current sequence number.

The egress node uses the sequence number to make sure that only the first received copy of the packet is selected, whereas the second received copy is discarded. The egress node strips off the sequence number from the packet right after its selection and before passing to the upper layer of the stack. Note that packet 1+1 recovery scheme is independent of the applications/protocols supported above MPLS.

The sequence number shall be carried in every packet as the first four bytes of the MPLS payload of each of the LSP providing packet 1+1 protection. The initial sequence number that is assigned to the first packet by the ingress node shall be agreed between the ingress and egress nodes. The default value of the initial sequence number is zero.

The sequence number is located after the 4-bytes MPLS encapsulation header as illustrated in Figure 9-1.

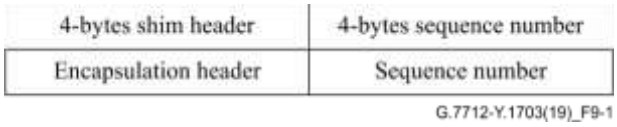


Figure 9-1 – Sequence identifier format

Annex A

Requirements for three-way handshaking

(This annex forms an integral part of this Recommendation.)

The three-way handshaking procedure is based upon and designed to be compatible with the IETF IS-IS Working Group's Three-way Handshaking function ([b-IETF RFC 3373]).

A.1 Point-to-point three-way adjacency TLV

A DCF supporting integrated IS-IS shall include a TLV in all point-to-point IIH PDUs. The structure of the TLV shall be:

Type = 0xF0 (decimal 240)

Length = 5 to 17 octets

Value:

Adjacency three-way state (one octet):

0 = Up

1 = Initializing

2 = Down

Extended local circuit ID of four octets

Neighbour system ID of zero to eight octets, if known

Neighbour extended local circuit ID of four octets, if known

The extended local circuit ID shall be assigned by the DCF when the circuit is created, and the DCF shall use a different value for each point-to-point circuit that it has.

The adjacency three-way state reported in the TLV shall be as specified in clause A.2.

A.2 Adjacency three-way state

A DCF supporting integrated IS-IS shall have an adjacency three-way state for each point-to-point circuit. This state is different to the state specified in [ISO/IEC 10589].

If no adjacency exists on a link, then the adjacency three-way state shall be set to "Down".

If a DCF receives an ISH on a point-to-point link and this results in a new adjacency being created with adjacency state "Initializing", then the adjacency three-way state shall be set to "Down".

If a DCF receives a point-to-point IIH that does not contain a three-way adjacency TLV, then the DCF shall behave as per [ISO/IEC 10589], but shall include the TLV in IIH PDUs on that link reporting the adjacency three-way state as "Down".

If a DCF receives a point-to-point IIH PDU that contains a three-way adjacency TLV, then the DCF shall behave differently to [ISO/IEC 10589] IIH PDU processing as follows:

– If the neighbour system ID and the neighbour extended local circuit ID fields of the TLV are present and if either neighbour system ID does not match the ID of the DCF, or the neighbour extended local circuit ID does not match the extended ID of the DCF, then the IIH PDU shall be discarded and shall not be processed;

– If the IIH PDU results in the [ISO/IEC 10589] state tables producing an "Up" or "Accept", and if the received adjacency three-way state is "Down", then the DCF shall set its adjacency three-way state to "Initializing";

– If the IIH PDU results in the [ISO/IEC 10589] state tables producing an "Up" or "Accept", and if the received adjacency three-way state is "Initializing", then the DCF shall change its adjacency three-way state from "Down" or "Initializing" to "Up" and generate an "AdjacencyChangeState(Up)" event;
– If the IIH PDU results in the [ISO/IEC 10589] state tables producing an "Up" or "Accept", and if the received adjacency three-way state is "Initializing", then if the DCF already has an adjacency three-way state of "Up", it shall maintain the adjacency three-way state of "Up";
– If the IIH PDU results in the [ISO/IEC 10589] state tables producing an "Up" or "Accept", and if the received adjacency three-way state is "Up", then if the DCF already has an adjacency three-way state of "Down", it will generate an "AdjacencyStateChange(Down)" event with the reason "Neighbour restarted" and the adjacency shall be deleted with no further IIH PDU processing taking place;
– If the IIH PDU results in the [ISO/IEC 10589] state tables producing an "Up" or "Accept", and if the received adjacency three-way state is "Up", then if the DCF already has an adjacency three-way state of "Initializing", then it will change its adjacency three-way state to "Up" and generate an "AdjacencyChangeState(Up)" event;
– If the IIH PDU results in the [ISO/IEC 10589] state tables producing an "Up" or "Accept", and if the received adjacency three-way state is "Up", then if the DCF already has an adjacency three-way state of "Up", it shall maintain the adjacency three-way state of "Up";
– Following the comparison of source ID from the PDU with the local system, ID and manipulation of the circuit ID shall not be performed.

If the IIH PDU results in the [ISO/IEC 10589] state tables producing an "Up" or "Accept", then the DCF shall:

1) copy the adjacency areaAddressOfNeighbour entries from the area addresses field of the PDU;
2) set the holdingTimer value of the holding time field from the PDU; and
3) set the neighbourSystemID to the value of the source ID field from the PDU as per [ISO/IEC 10589].

Annex B

Requirements for automatic encapsulation

(This annex forms an integral part of this Recommendation.)

B.1 Introduction

This annex provides a specification for the optional automatic encapsulating data communication function (AE-DCF) that enables nodes that support routing of differing incompatible network layer protocols, such as CLNS, IPv4 or IPv6 to be present in a single IS-IS Level-1 area or Level-2 subdomain, and which automatically encapsulates one network layer protocol into another as required, provided that all of the nodes support IS-IS or integrated IS-IS routing.

B.2 Scope

The AE-DCF is an optional function. When it is provided, it shall function as specified in this annex. The requirements in this annex apply only to DCFs that contain the additional functionality of an AE-DCF. The AE-DCF also requires certain behaviours from DCFs that do not include AE-DCF functionality, in order to interwork with them. Requirements for DCFs that do not include AE-DCF functionality are found in clause 8.3.6.1 for IP and dual nodes, and in [ISO/IEC 10589] for OSI nodes.

B.3 Description of the AE-DCF

B.3.1 Introduction

Integrated IS-IS, as specified in [IETF RFC 1195], was originally designed to be able to route IP and CLNS using a single routing protocol, and a single shortest path first (SPF) algorithm. For this, it represents IPv4 addresses and subnet masks as a 64-bit number which is then treated by the SPF algorithm as if it were an OSI end system address. Integrated IS-IS nodes are required to have an IS-IS area address and a system identifier, which is treated in the same way as an NSAP address is in an OSI-only node. Integrated IS-IS nodes then form adjacencies and flood system identifiers and metrics throughout their Level-1 area (Level-1 routers) or their Level-2 subdomain (Level-2 routers) in the same way as OSI-only IS-IS nodes.

System identifiers (SIDs) and metrics to other SIDs are flooded throughout a Level-1 area or Level-2 subdomain using LS-PDUs (link state PDUs) that are common to both IS-IS and integrated IS-IS nodes. IP-specific information is then added to these LS-PDUs using TLV extensions that are understood only by IP-capable nodes. OSI-only routers cannot decode these TLVs but still flood them onwards to all of their adjacencies. In this way, an SPF tree can be built by any IS-IS or integrated IS-IS node whether it can route CLNS, IPv4 or IPv6. OSI-capable nodes will calculate the shortest paths to OSI end systems, IPv4-capable nodes will calculate the shortest paths to IPv4 addresses or prefixes, and IPv6-capable nodes will calculate the shortest paths to IPv6 addresses or prefixes.

One consequence of this is that an OSI-only node will calculate a shortest path to an OSI end system that goes through an IP-only node, even though that IP-only node cannot forward CLNS packets. Similarly, an IP-only node will calculate a shortest path to an IP destination that goes through an OSI-only node, even though the OSI-only node cannot forward IP packets. Thus, an OSI-only capable node must not be placed in a part of a network where there is any possibility of it being on the shortest path to IP destinations, and an IP-only node must not be placed in a part of the network where there is any possibility of it being on the shortest path to an OSI end system.

The integrated IS-IS algorithm can only use a single SPF algorithm for two or more network layer protocols due to an assumption that all network-layer protocols have access to the same resources; in other words, the same network with the same topology. Thus, integrated IS-IS requires any node in a Level-1 area or Level-2 subdomain to be able to route any network layer protocol that is present in the area or domain respectively.

For this reason, [IETF RFC 1195] places topological restrictions on networks that are routed by integrated IS-IS, requiring that all of the nodes support both IP and CLNS in an area that have both CLNS traffic and IP traffic present in them.

Consequently, according to [IETF RFC 1195], if one node is upgraded and forwards IP packets, then all of the others in the Level-1 area or Level-2 subdomain must also be upgraded.

The solution proposed here allows this topological restriction to be removed, and it automatically encapsulates CLNS packets inside IP packets for forwarding across IP-only nodes and encapsulates IP packets inside CLNS packets for forwarding across OSI-only nodes. The solution proposed here is fully compatible with existing OSI-only nodes, which will not require any upgrade. It places one requirement upon IPv4-only or IPv6-only nodes above those in [IETF RFC 1195], specifically the network-layer protocol aware adjacency creation function specified in clause 8.3.6.1.1.

B.3.2 Basic concept

This feature takes advantage of the fact that all integrated IS-IS and IS-IS nodes share basic topology information in the same way, and of the behaviour that OSI-only nodes will attempt to forward a packet across an IP-only node and vice versa, even though that node is incapable of actually forwarding the packet. Normally, this would result in packet loss, but an AE-DCF encapsulates packets before they are forwarded across incompatible nodes so that they are not lost.

When two islands of IP capable integrated IS-IS nodes are connected using a central network that supports only OSI, and if all of the nodes participate in the same area (for Level-1 nodes), then the IP capable nodes will receive the LS-PDUs from all of the other IP capable nodes, even those in the other island, as well as the LS-PDUs from all of the OSI-only nodes in the centre. Thus, they calculate shortest paths across the OSI-only nodes for all of the IP destinations in the island on the far side. It is only when an IP-capable node actually forwards an IP packet to an OSI-only node that things go wrong, and the packet is lost; hence, the topological restrictions in [IETF RFC 1195].

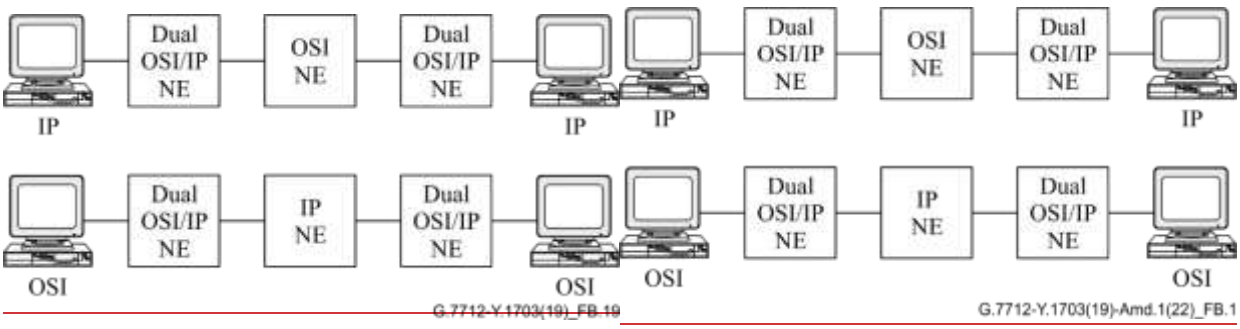


Figure B.1 – Illegal topologies

The above simple networks illustrated in Figure B.1 are illegal topologies according to [IETF RFC 1195]. In the top network IP packets will be routed from one side of the network to the other, but on arrival at the OSI-only node they will be discarded. Similarly, in the bottom network CLNS packets will be routed from one side of the network to the other, but on arrival at the IP-only node they will be discarded. An AE-DCF specified here corrects this behaviour.

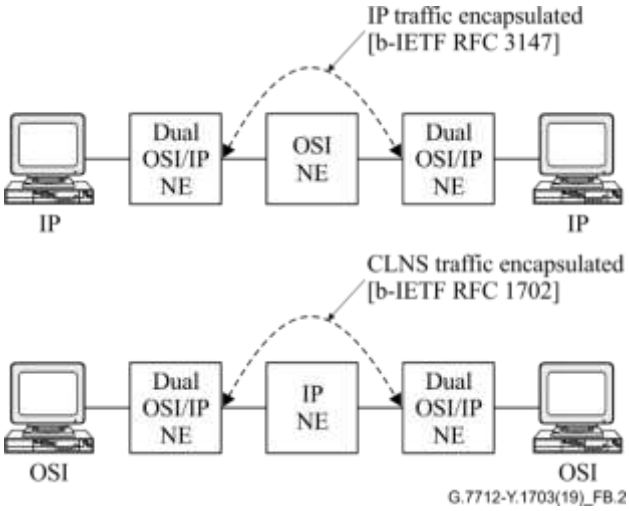


Figure B.2 – Encapsulation "repair"

The AE-DCF resides in dual nodes and enables them to recognize that a particular neighbour will discard certain traffic, and so to encapsulate it into a form that will not be discarded (see Figure B.2). This 'repairs' the network so that the part of network between the dual nodes acts as if it is comprised of all dual nodes when, in actual fact, one, or more of the nodes are not dual.

An AE-DCF does not alter the path that a packet will take across the network; any individual packet will still cross the network using the shortest path as calculated by the normal IS-IS SPF algorithm.

The network-layer protocol aware adjacency creation function specified in clause 8.3.6.1.1 forces traffic to go through nodes that support both IP and OSI whenever the shortest path takes traffic across a boundary between IP-capable and OSI-capable parts of an area. The AE-DCF then enables those dual nodes to encapsulate a packet if necessary, so that it can be forwarded by nodes that do not support that network layer protocol. This encapsulation takes place only when necessary, and thus these tunnels are automatically created and are dynamic. The resulting tunnels are not maintained in any way and exist only as entries in forwarding tables. The tunnels do not appear as a circuit or interface as far as the routing protocol is concerned. Thus, packets still cross the network along the shortest path that each node calculates normally, and there is no need for IS-IS packets to be encapsulated, only IP and CLNS traffic is encapsulated.

B.4 Requirements and limitations

B.4.1 Requirements for OSI-only nodes

In order to interwork with the AE-DCF, OSI-only nodes are required to be conformant to [ISO/IEC 10589].

B.4.2 Requirements for IP-capable nodes

In order to interwork with the AE-DCF, IP-only nodes are required to be conformant to [IETF RFC 1195].

In particular, IP-capable nodes are required to ignore the "protocol supported" TLV in LS-PDUs of nodes that they are considering as candidates for shortest paths when running the SPF algorithm.

An IP-capable node that only includes IP-capable nodes in its SPF calculation would not conform to [IETF RFC 1195], where it states:

– From page 26 of [IETF RFC 1195]: "The Dijkstra computation does not take into consideration whether a router is IP-only, OSI-only, or dual. The topological restrictions specified in section 1.4 ensure that IP packets will only be sent via IP-capable routers, and OSI packets will only be sent via OSI-capable routers."

The AE-DCF is compatible with [IETF RFC 1195] implementations that conform to the above statement. An implementation that only includes IP-capable nodes in its SPF calculation would not view paths through OSI-only nodes as being a suitable route, and so will not take advantage of the AE-DCF.

In order to interwork with the AE-DCF, IP nodes are required to conform to clause 8.3.6.1.1. The reason for this is stated below:

– This solution is dependent upon IP packets arriving at an OSI-only node, having first gone through an AE-DCF, and upon CLNS packets arriving at an IP-only node, having first gone through an AE-DCF. The AE-DCF is then responsible for encapsulating these packets so that they can be forwarded;

– Therefore, an IP-only node must never have an adjacency with an OSI-only node;

– If this solution is used to mix IPv4 and IPv6 nodes in the same Level-1 area or Level-2 subdomain, then similarly an IPv4-only node must never have an adjacency with an IPv6-only node;

– This requirement is met if all IP-capable nodes conforming to clause 8.3.6.1.1. Note that this requirement is not present in [IETF RFC 1195].

Alternatively, an operator may manually ensure that nodes that do not support a network layer protocol in common do not have adjacencies.

B.4.3 Requirements for automatically encapsulating dual or multilingual nodes

If this feature is to be used in a Level-1 area or Level-2 subdomain, then nodes that support more than one network layer protocol, but that do not support the AE-DCF, may be used with caution. A safer alternative is either to comply with the topological restrictions of [IETF RFC 1195], or to use only dual or multilingual nodes that contain the AE-DCF.

B.4.3.1 Encapsulation capability TLV

The AE-DCF will include a new TLV in LS-PDUs with LS-PDU number equal to zero. The new TLV will have the following structure:

Code: 16 (decimal)

Length: The length of the value

Value: A variable length part containing the following:

Sub-TLV type: 1

Sub-TLV length: 3 times the number of encapsulation modes in the sub-TLV

Sub-TLV value:

47 indicating that the next two bytes are a GRE encapsulation;

The NLPID of a packet that may be encapsulated (inner);

The NLPID of a packet that transports the encapsulated packet (outer);

Bytes 4, 5, 6: A second encapsulation mode (if needed);

Bytes 7, 8, 9: A third encapsulation mode (if needed);

etc.

The NLPIDs that are used shall be those as specified in [ITU-T X.263]. Nodes that transmit this TLV shall indicate the formats that a node can both receive and transmit. Nodes must be able to both automatically encapsulate and automatically unencapsulate the formats that are described in the TLV, so that traffic may be received, and so that traffic may return in the reverse direction.

It is recommended that dual nodes supporting an AE-DCF are able to encapsulate/unencapsulate A over B, and B over A (where A and B are the two supported network layer protocols) making two encapsulation modes in a typical dual node.

For example, the contents of the TLV for a typical OSI and IPv4 AE-DCF will be:

16: the code;

8: the value length (in this example);

1: sub-TLV type 1;

6: sub-TLV length (in this example);

47: next two bytes are a supported GRE mode;

129: Initial protocol identifier (IPI) for CLNP from [ITU-T X.263];

204: IPI for IPv4 from [ITU-T X.263];

47: next two bytes are a supported GRE mode;

204: IPI for IPv4 from [ITU-T X.263];

129 IPI for CLNP from [ITU-T X.263].

An OSI, IPv4, IPv6 AE-DCF will thus typically use six encapsulation modes to indicate CLNP over IPv4, CLNP over IPv6, IPv4 over CLNS, IPv4 over IPv6, IPv6 over CLNS, and IPv6 over IPv4, giving a value length of 20.

This TLV will not be included in pseudonode LS-PDUs.

An AE-DCF that does not have any IPv4 addresses must not place any encapsulation formats in its TLV of type equal 16 that include IPv4 as an encapsulation transport (outer) NLPID until such time as an IPv4 address is provisioned and advertised.

An AE-DCF that does not have any IPv6 addresses must not place any encapsulation formats in its TLV of type equal 16 that include IPv6 as an encapsulation transport (outer) NLPID until such time as an IPv6 address is provisioned and advertised.

B.4.3.2 Forwarding process

As the AE-DCF does not modify the path that a packet follows, an AE-DCF may calculate a shortest path for an IP packet that results in the next hop being an OSI-only node.

When this happens, the AE-DCF must not simply forward a packet to an adjacent node that does not support that type of network layer protocol. Instead, the AE-DCF must encapsulate the packet inside a new packet of a type that the next hop does support. The criteria for whether an adjacent node does or does not support a particular network layer protocol is whether that network layer protocol is listed in the "protocols supported" TLV in IS-IS Hello PDUs received from the node on the adjacency which is the next hop for that destination.

This new packet requires a network layer protocol, a destination address, and a source address to encapsulate the original packet:

– The network layer protocol of the new packet must be one that is supported by the next hop, as defined by the "protocols supported" TLV of Hello PDUs received from the next hop;

– The destination address of the new packet must be equal to the identity of the next node along the shortest path to the original destination that has transmitted an encapsulation mode that has both the type of network layer protocol that the original packet is as the encapsulated (inner) NLPID, and a network layer protocol that is supported by the next hop (as defined by the "protocols supported" TLV of Hello PDUs received from the next hop) as the encapsulation transport (outer) NLPID;

– This must be achieved by inspection of the new TLV of type equal to 16 from LS-PDUs received from each node in the path to the destination, until the first is found that meets the above requirement;
– When inspecting TLVs of type equal to 16, an AE-DCF shall ignore any sub-TLVs that it does not understand, and shall jump to the next sub-TLV and shall inspect that, either until it finds all of the encapsulation modes that it is looking for, or until it reaches the end of the TLV;
– The source address of the new packet must be equal to the identity of the AE-DCF that constructs the new encapsulation packet.

If an AE-DCF can forward a packet without encapsulation because the next hop supports that type of packet, then the AE-DCF must forward the packet without encapsulating it.

An AE-DCF might send LS-PDUs containing IP reachability from an IP-only node on to a split stack node, or vice versa, and consequently might then be required to encapsulate packets headed for a split stack node, or unencapsulate packets received from a split stack node.

Thus, an automatically encapsulating split stack node must also follow the same process of inspecting LS-PDUs of nodes between itself and the destination looking for a node that has a suitable encapsulation format.

Note that a split stack node might be capable of receiving an IPv4 packet only encapsulated inside CLNS, for example. In this case, the split stack node will transmit only "CLNS" in the "protocols supported" field of its Hello packets and will only include one encapsulation mode in its TLV of type equal 16 in its LS-PDUs. This single encapsulation mode will specify IPv4 as the encapsulated (inner) packet NLPID and CLNS as the encapsulation transport (outer) packet NLPID.

B.4.3.3 Receipt process

When an AE-DCF receives a packet that is destined for itself, it must inspect that packet to see if it has another packet encapsulated inside it. The resultant unencapsulated CLNS, IPv4 or IPv6 packet must then be forwarded as normal. If the resultant unencapsulated packet then contains another packet destined for this node, the process is repeated; this is because multiple layers of encapsulation may require unencapsulation at a single AE-DCF.

IS-IS packets are not compatible with IP packets and cannot be forwarded across the public Internet or other IP-only networks. This is a security advantage as it makes it difficult for a malicious entity to remotely launch IS-IS packets at IS-IS or integrated IS-IS nodes across the public Internet. In order not to remove this advantage, then, if an IS-IS or ES-IS packet arrives encapsulated inside another packet destined for an AE-DCF, then the AE-DCF must discard it unless it came from a node with which the AE-DCF has a manually provisioned tunnel with IS-IS provisioned to run across it. Optionally, an error report may be raised informing the network manager of information such that a packet was received and dropped, where it came from, or that it is a potential malicious event.

All packets must be encapsulated using GRE encapsulation as specified in clause 8.3.4.

B.4.3.4 MTU size and fragmentation requirements

The encapsulation of one packet inside another may result in a new packet that is longer than the MTU size of the link over which this new packet must be forwarded. This new GRE packet must not be discarded; therefore, these packets must not have the Don't Fragment bit set if they are IPv4 packets and must have the SP flag set if they are CLNS packets, as per clause 8.3.4.

The resultant encapsulation packets must then be fragmented before being forwarded if the packet is now longer than the MTU limit of the link.

It is not necessary to fragment a packet before encapsulating it, as the resultant encapsulation packet will be fragmented if necessary.

B.4.3.5 Requirements for AE-DCF with broadcast (LAN) interfaces

B.4.3.5.1 Pseudo-node election process

According to clause 8.3.6.1.1, IP-only nodes are not allowed to form an adjacency with OSI-only nodes, and IPv4-only nodes are not allowed to form an adjacency with IPv6-only nodes.

Therefore, when IP-only and OSI-only nodes are connected to the same LAN and in the same Level-1 area or Level-2 subdomain, then the IP-only nodes will form adjacencies with one another and will elect a pseudonode, whilst the OSI-only nodes will form separate adjacencies and will elect a different pseudonode. Therefore, there will be two separate pseudonodes on the LAN, one for the OSI-only nodes, and one for the IP-only nodes.

A similar thing may happen if IPv4-only and IPv6-only nodes are connected to the same LAN.

An AE-DCF must, therefore, take part in these separate pseudonode election processes independently for each network layer that it supports. A Level-1/Level-2 AE-DCF must take part in two pseudonode election processes for each network layer protocol that it supports (one for Level-1 and one for Level-2).

Each pseudonode on the LAN residing on a node of a network layer protocol compatible with the AE-DCF will have an adjacency with the AE-DCF. Thus, on an IP & OSI LAN, the AE-DCF will correctly be the one that has valid adjacencies both with the IP pseudonode and with the OSI pseudonode (if multiple pseudonodes are present on the LAN). The AE-DCF will have an adjacency with the IP pseudonode and with the OSI pseudonode, but the IP pseudonode will not have a direct adjacency with the OSI pseudonode, and vice versa, but will instead gain connectivity only through the AE-DCF, thus guaranteeing that CLNS packets are encapsulated by the AE-DCF before being forwarded to IP-only nodes, and that IP packets are encapsulated by the AE-DCF before being forwarded to OSI-only nodes.

An IP- and OSI-capable AE-DCF may be elected as the designated router by the IP-capable nodes on the LAN, but not by the OSI-capable nodes; in this case, the AE-DCF must create a pseudonode, but the pseudonode must declare adjacencies in its LS-PDUs only with the IP-capable nodes on the LAN.

Similarly, an IP- and OSI-capable AE-DCF may be elected as the designated router by the OSI-capable nodes on the LAN, but not by the IP-capable nodes; in this case, the AE-DCF must create a pseudonode, but the pseudonode must declare adjacencies in its LS-PDUs only with the OSI-capable nodes on the LAN.

An IP- and OSI-capable AE-DCF may be elected as the designated router both by the IP-capable and by the OSI-capable nodes on the LAN; in this case, the AE-DCF must create a pseudonode that declares adjacencies in its LS-PDUs to all of the nodes on the LAN.

In essence, an AE-DCF takes part in a separate election process for each network layer protocol that it supports, and if it wins any of the elections then it creates a pseudonode, but the pseudonode will declare adjacencies in its LS-PDUs only with the set, or sets, of nodes that elected it.

Consequently, OSI-only or IP-only nodes may receive LS-PDUs from a pseudonode that lists adjacencies to nodes on the LAN that they do not have adjacencies with. If a packet should need to be forwarded via such a node, then it should be sent to the designated IS as per [ISO/IEC 10589] section C.2.5 item "h", and as per [IETF RFC 1195] section C.1.4 step 0 clause 8 on page 73. Note that these clauses in [ISO/IEC 10589] and [IETF RFC 1195] are non-normative. It is possible that there are implementations that do not exhibit this behaviour. Such an implementation will drop packets rather than send traffic to an AE-DCF for automatic encapsulation, if the AE-DCF is the designated router, and if non-compatible nodes on the same LAN are on the shortest path.

Implementers and operators, therefore, have a choice to make; the choice is:

1) Set the priority of the AE-DCF to a high value. This results in a single pseudonode appearing on the LAN, supported by an AE-DCF. The disadvantage of this approach is that there is a

small chance that a legacy implementation exists on the LAN that does not forward traffic to an AE-DCF if a non-compatible node on the LAN is on the shortest path; or

2) Set the priority of the AE-DCF to a low value. This results in one pseudonode appearing on the LAN for every network-layer protocol supported, explicitly sending traffic for non-compatible nodes through an AE-DCF. This improves interoperability but doubles the amount of LS-PDUs transmitted onto the LAN, possibly reducing scalability.

It is recommended that the priority of an AE-DCF is operator configurable.

B.4.3.5.2 LS-PDU update process

[ISO/IEC 10589] states in section 7.3.15.1 that an LS-PDU received, which does not come from a valid adjacency, must be discarded. A strict OSI-only implementation will therefore reject LS-PDUs that are transmitted onto a LAN interface by an IP-only node, as the IP-only node has rejected the adjacency as per clause 8.3.6.1.1. Thus, the OSI-only node can receive such an LS-PDU only from an AE-DCF. Without modified behaviour, a dual node would only forward such an LS-PDU during periodic LS-PDU database synchronization.

An AE-DCF is, therefore, required to have modified LS-PDU flooding behaviour so that OSI-only or IP-only nodes do not need to wait for the next LS-PDU database synchronization event.

An AE-DCF must check incoming LS-PDUs that arrive on LAN interfaces to see if they come from a neighbour that supports all of the network layer protocols that the AE-DCF does. This must be achieved by inspection of the "protocols supported" TLV in Hello packets received from that neighbour.

If the LS-PDU is received from a neighbour that does support all of the network layer protocols that the AE-DCF supports, then the AE-DCF shall behave as per [ISO/IEC 10589] and unset the send routing message (SRM) flag for that LS-PDU on that LAN interface if it already has the LS-PDU, or shall flood it out of all other interfaces if it does not already have the LS-PDU.

If the LS-PDU is received from a neighbour that does not support all of the network layer protocols that the AE-DCF supports, and if it does not already have the LS-PDU, then the AE-DCF shall set the SRM flag for that LS-PDU on the LAN interface over which the LS-PDU was received, in addition to all other interfaces, resulting in the AE-DCF retransmitting the LS-PDU onto the LAN.

In this way, if an LS-PDU is transmitted onto the LAN by an IP-only node, then an AE-DCF will retransmit the LS-PDU, so that it may be received on a valid adjacency by OSI-only nodes on the LAN and vice versa.

B.4.3.5.3 Redirects

If an AE-DCF originates an ICMP redirect request, the request must not redirect IPv4 packets from an IPv4-capable node to a non-IPv4-capable node. Likewise, if an AE-DCF originates [ISO 9542] redirect PDUs, the redirect must not redirect CLNS packets from an OSI capable node to a non-OSI-capable node.

B.4.3.5.4 Mixing of dual [IETF RFC 1195] only and automatically encapsulating nodes on a LAN

A dual node that is conformant to [IETF RFC 1195], but that does not support an AE-DCF, must not reside on a LAN in the same Level-1 area or Level-2 subdomain as both IP-only and OSI-only nodes, as it may forward IP traffic to an OSI-only node, or CLNS traffic to an IP-only node, resulting in packet loss. This is a topological restriction of [IETF RFC 1195].

A dual node that is conformant to [IETF RFC 1195], but that does not support an AE-DCF, may reside on a LAN in the same Level-1 area or Level-2 subdomain as an AE-DCF.

Additionally, it may reside on a LAN with an OSI-only node if it can forward only CLNS traffic to that node, an IPv4-only node if it can forward only IPv4 traffic to that node, or an IPv6-only node if it can forward only IPv6 traffic to that node.

B.4.4 Requirements for automatically encapsulating split stack nodes

A split stack node initiates and terminates packets of a network-layer protocol type that it cannot forward natively in its DCC channels. Therefore, the only way that such a node may initiate or terminate such packets is if they are in an encapsulated form.

This solution is particularly useful for adding an IP card into a predominantly OSI node, or a node that will be installed into an existing OSI network, for example. It may also be easier to upgrade an OSI gateway NE to a split stack node, rather than to a dual AE-DCF, so that IP traffic can get in and out of the network for which the node is a gateway.

The split stack node must be able to internally route any packets that it receives that are of a network-layer protocol equal to one of those listed in the "protocols supports" TLVs of its' IS-IS LS-PDUs.

A split stack node must use the "protocols supported" TLV in IS-IS Hello PDUs to indicate only the network-layer protocols that it can receive and forward natively on any individual interface (or not support this TLV if it is an OSI-only interface).

That is, an IP-over-OSI node can route CLNS natively in its DCC channels, and can route IP traffic that arrives for it in IP-over-OSI GRE encapsulated packets, or possibly an Ethernet interface.

Thus, a split stack node may indicate one network layer protocol in the "protocols supported" TLV of Hello packets on one interface, and a different network layer protocol in the "protocols supported" TLV of Hello packets on another interface. Such a node would be able to route both network layer protocols internally, and so would advertise both in the "protocols supported" TLV of its LS-PDUs.

A split stack node must use IP reachability TLVs in IS-IS LS-PDUs to indicate the address range of encapsulated packets that it is able to terminate.

A split stack node might receive IP reachability extensions from an IP-only node, via a dual AE-DCF. Therefore, the split stack node must be able to send traffic to a destination via an AE-DCF, which it will use to unencapsulate its packets. To achieve this, a split stack node must search for the next node along the path to each destination capable of unencapsulation, or for a split stack destination, in exactly the same way that an AE-DCF does.

An automatically encapsulating split stack node shall advertise the encapsulation modes that it supports using encapsulation capability TLV as per clause B.4.3.1.

When a split stack node receives a packet that is destined for itself, it must inspect that packet to ascertain whether it has another packet encapsulated inside it. If so, then the packet will be processed internally, unless it is an IS-IS or ES-IS packet, in which case it must be discarded (unless a manually provisioned tunnel exists with IS-IS provisioned to run across it) in the same way as it would be by a dual AE-DCF.

In the same way as a dual AE-DCF, a split stack node must support GRE encapsulation as specified in clause 7.1.8.

B.4.5 Use of IP nodes that do not conform to clause 8.3.6.1.1 with the AE-DCF

IPv4-only or IPv6-only nodes that are conformant to [IETF RFC 1195], but that do not support the protocol aware adjacency creation function specified in clause 8.3.6.1.1, may be used in the same mixed Level-1 area or Level-2 subdomain as an AE-DCF, but the network manager must manually ensure that such a node does not have any adjacencies with other nodes that might forward packets to it that it does not support.

B.4.6 Use of dual nodes with no AE-DCF and dual nodes with AE-DCF in the same IS-IS area

Dual nodes that are conformant to [IETF RFC 1195], but that do not support an AE-DCF, may be used in mixed Level-1 areas or Level-2 subdomains with an AE-DCF with the restrictions below:

Integrated IS-IS nodes (or clusters of nodes) that support more than one network layer protocol but which do not support an AE-DCF are still subject to the topological restrictions of [IETF RFC 1195]. This means that the network manager must ensure that such a node cannot pass packets to a neighbouring node that cannot forward that type of packet.

That is, dual signifies a dual integrated IS-IS node that conforms to [IETF RFC 1195], but that does not contain an AE-DCF.

OSI-AEDCF-dual-AEDCF-IP is a safe combination;

OSI-AEDCF-dual-dual-dual-AEDCF-IP is a safe combination;

IPv4-AEDCF-dual IPv4&IPv6-AEDCF-IPv6 is a safe combination;

dual-AEDCF-OSI-AEDCF-dual is a safe combination;

OSI-IPv4&OSIAEDCF-dual IPv4&OSI-dual IPv4&IPv6-IPv4&IPv6 AEDCF-IPv6 is not a safe combination;

OSI-IPv4&OSIAEDCF-dual IPv4&OSI-IPv4&IPv6&OSI-dual IPv4&IPv6-IPv4&IPv6 AEDCF-IPv6 is not a safe combination.

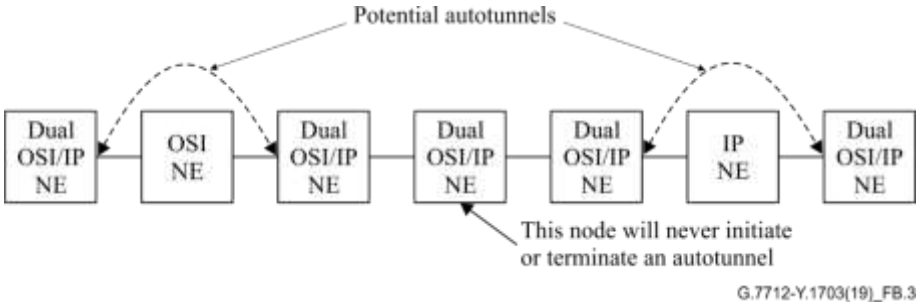


Figure B.3 – Topological requirements for IS-IS area dual nodes

B.4.7 Requirements for Level-1 and Level-2 nodes

It is recommended that nodes that support both Level-1 and Level-2 routing and are present in an area in which these AE-DCFs are used provide one of the following functions (mutually exclusive):

– To support all network layer protocols that are present in both the Level-1 and the Level-2 subdomain in which the node participates and support an AE-DCF; or

– To support all network layer protocols that are present in both the Level-1 and the Level-2 subdomain in which the node participates and be either directly connected to, or connected through, continuous strings of other nodes that support all network layer protocols in the area, to a node that supports an AE-DCF and that supports all of the network layer protocols in the area.

That is, dual signifies an Integrated IS-IS node that conforms to [IETF RFC 1195], but that does not support an AE-DCF:

L2_subdomain-dual_L1/L2-non_dual is safe (as per [IETF RFC 1195]);

L2_subdomain-dual_L1/L2-dual-dual-non_dual is safe (as per [IETF RFC 1195]);

L2_subdomain-dual_L1/L2-AE-DCF-mixted_network is safe;

L2_subdomain-dual_L1/L2-dual-dual-AE-DCF-mixted_network is safe;

L2_subdomain-dual_L1/L2-non_dual-dual is not safe (unless [IETF RFC 1195] restrictions are applied);

L2_subdomain-dual_L1/L2-non_dual-AE-DCF is not safe (unless [IETF RFC 1195] restrictions are applied).

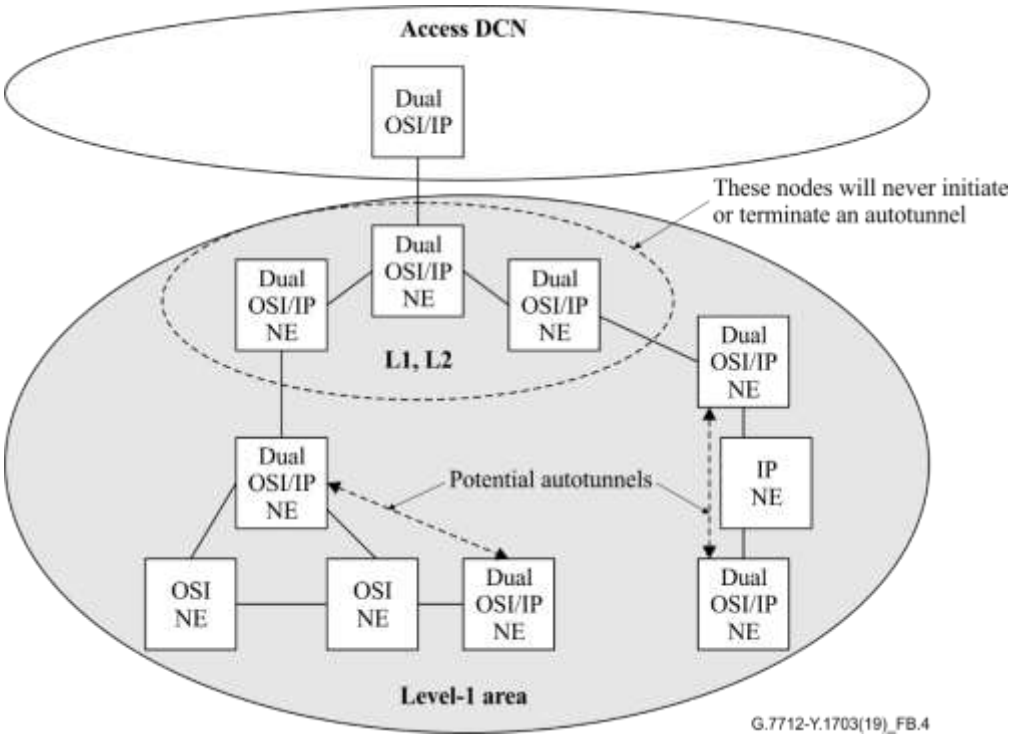


Figure B.4 – Requirements for Level-1, Level-2 nodes

However, it is understood that a gateway NE, and therefore a L1, L2 router, may be an existing OSI-only device. In this case, it is possible to have IP and automatic encapsulation in the area by using the following method, with care:

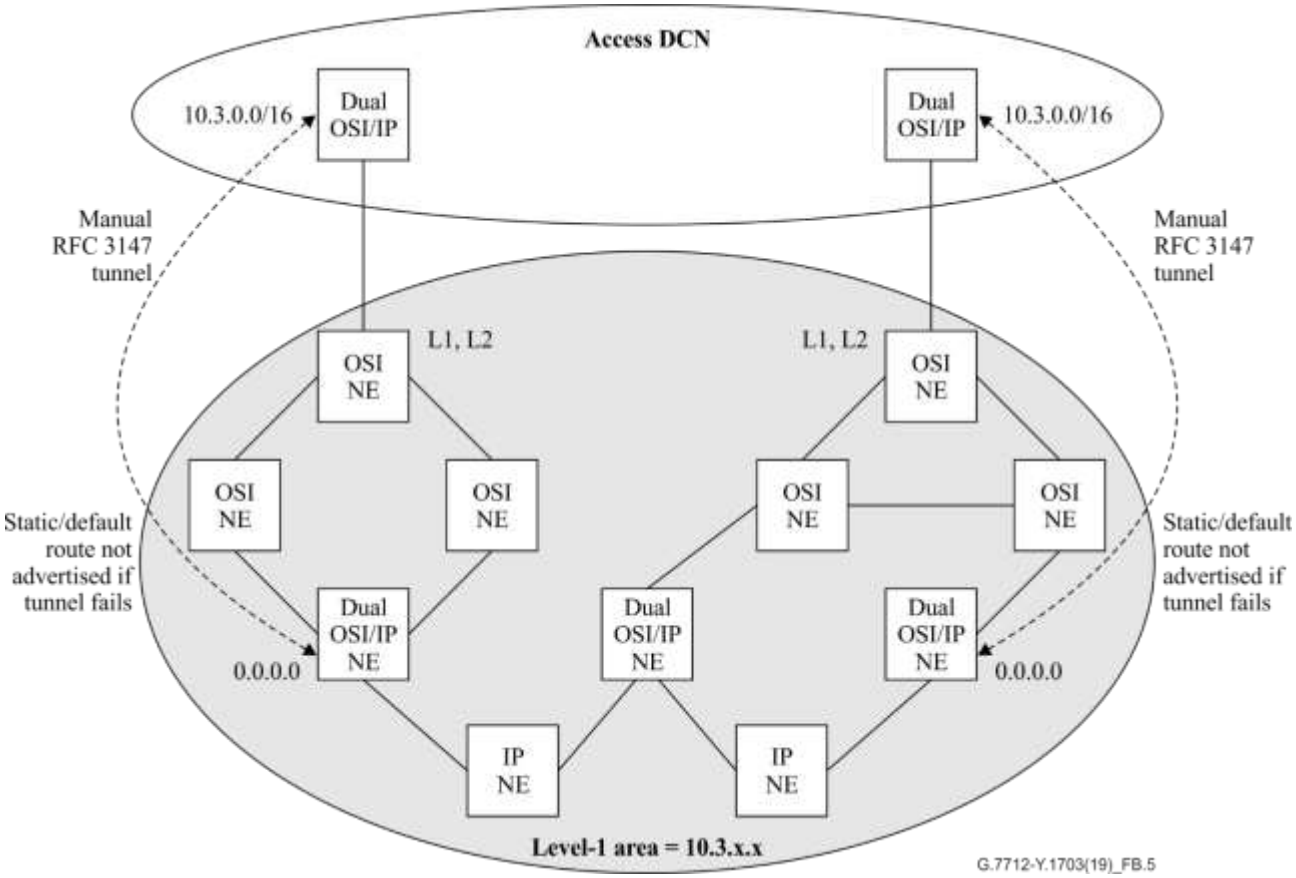


Figure B.5 – Use of an OSI-only device as a gateway

One or more dual nodes in the area may be chosen as gateways for IP packets. These nodes will be configured to advertise a default route (0.0.0.0) into the area to attract all "out of area" IP traffic to them. These nodes will then forward all "out of area" traffic across a manually provisioned GRE tunnel, which passes through the Level-1, Level-2 OSI-only node to another dual node outside of the area.

The dual node that is outside of the area must have a prefix manually provisioned into it to attract all IP traffic bound for the area to it and send it over the tunnel into the area. Optionally, a mechanism, such as an IP routing protocol, may be provisioned across the tunnel so that each end may see if the other is alive; however, if integrated IS-IS is used, then it must be a different routing instance to that used generally in the area, as it is effectively a different routing domain.

If such a mechanism is used, then if the far end disappears, the dual node inside the area should stop advertising a default route, and the dual node outside of the area should stop advertising the prefix that represents the nodes in the area. In this way, redundant IP gateways can be provisioned.

Note that [IETF RFC 1195] states that default routes should not be advertised within Level-1 LS-PDUs. This solution requires that this rule be broken. Normally a Level-1 [IETF RFC 1195] node would consider a Level-1, Level-2 node to be its default route. This solution requires that this behaviour be overwritten by receipt of a default route advertisement in a Level-1 LS-PDU. If this is not possible, then a work-around is for the IP gateway nodes to be configured with a selection of static routes that cover all possible "out of area" destinations that an IP stack in the area is likely to try to reach.

B.4.8 Requirements for the Level-2 subdomain

It is acceptable to route all protocols present natively in the Level-2 subdomain, as per [IETF RFC 1195], in which case, none of the Level-2 nodes need to support an AE-DCF, but all of them must support all of the network layer protocols present.

Alternatively, it is acceptable to use Level-2 nodes that support less than all of the network layer protocols present in the domain, in which case, the Level-2 dual or multilingual nodes will be required to support an AE-DCF so that packets may be automatically encapsulated in order to pass through such nodes.

Annex C

(This annex has been intentionally left blank.)

Annex D

OOB OCh-O and OTSiG-O protocol specification

(This annex forms an integral part of this Recommendation.)

D.1 Overview

The OOB OCh-O and optical tributary signal group – overhead (OTSiG-O) protocol supports an OCC carrying the status of OCh and optical tributary signal assembly (OTSiA) connections and signals over an OCN to systems that do not have direct access to the OSC. For deployment flexibility, the OCh-O and OTSiG-O protocol is defined independent of the specific DCN protocol in use (e.g., IPv4, IPv6). The details of how to adapt the characteristic information (CI) of this protocol to an IPv4 based DCN are provided at the end of the protocol definition.

The OOB OCh-O and OTSiG-O protocol requires configuration of a protocol adjacency between two OCh-O or OTSiG-O connection points (OCh-O CP, OTSiG-O_CP) located on the associated network equipment being connected by one or more optical physical section (OPS). Prior to both ends being configured, the status reporting behaviours driven by the protocol will not be operational. The adjacency is identified by using OPS as well as OCh identifiers and is carried by the DCN network.

The status messages carried by the OOB OCh-O and OTSiG-O protocol provide unidirectional state information for one or more OCh and/or OTSiA connections and signals. The messages include identifiers of the OPS trail and one or more OCh-P and/or OTSiG link connections carried by that trail that identify the OCh-P and/or OTSiG link connections for which status is being reported. The receiving NE correlates the received status message with a local OCh-P CP or OTSiG CP utilizing the configured OPS adjacency.

D.2 PDU format

The OOB OCh-O and OTSiG-O protocol is derived from the IETF's link management protocol (LMP) [b-IETF RFC 4204]. LMP uses a common format for the PDUs of all protocol messages as shown in Figure D.1.

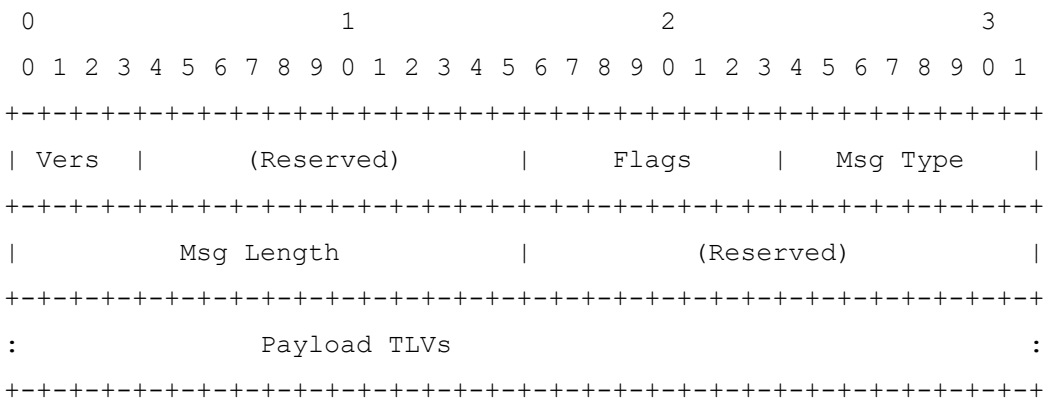


Figure D.1 – OOB OCh-O and OTSiG-O protocol message PDU format

Sub-protocols are used in the design of OOB OCh-O and OTSiG-O protocol. The value in the Msg Type field indicates which of the sub-protocols a PDU belongs to. TLV structure is used for the base PDU and payload TLV structures; in all cases the units of length are octets. The Msg Length provides the overall length of the PDU.

Payload TLVs all follow the format shown in Figure D.2.

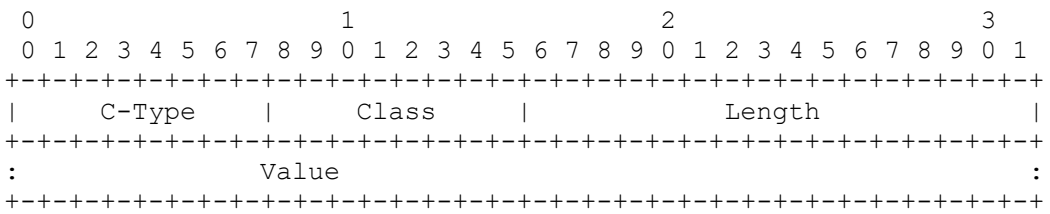


Figure D.2 – OOB OCh-O and OTSiG-O protocol payload TLV format

The C-Type and Class fields are defined by each sub-protocol. The Length field provides the overall length of the TLV inclusive of the C-Type, Class and Length fields.

The OOB OCh-O and OTSiG-O protocol shall exchange Hello PDUs and Status Reporting PDUs.

D.2.1 Hello sub-Protocol

The Hello Sub-protocol uses a message type of 4. Inside the message are Hello Sequence and Validity TLVs. The format of these TLVs is as follows:

D.2.1.1 Hello sequence TLV

The C-type is 7, Class is 1 and Length is 12. The Value field is formatted as shown in Figure D.3.

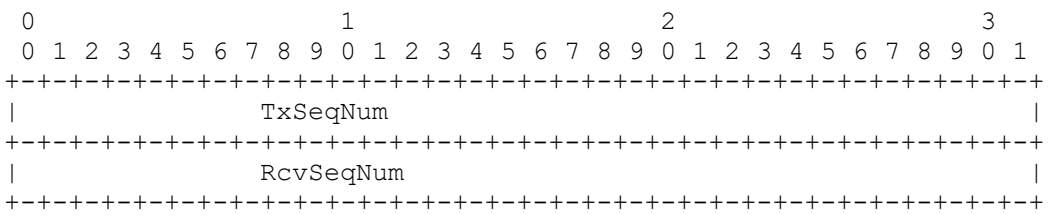


Figure D.3 – OOB OCh-O and OTSiG-O protocol Hello sequence format

The TxSeqNum is the sequence number of the Status Reporting message last transmitted by this adjacency endpoint. The RcvSeqNum is the sequence number of the Status Reporting message last received by this adjacency endpoint.

Initially the RcvSeqNum=0 and the TxSeqNum=1. The RcvSeqNum will be replaced with the TxSeqNum received from the peer when the first Hello message is received.

If a Hello message is received with a Hello sequence TLV containing a RcvSeqNum equal to 0, it is an indication that the peer endpoint has restarted and requires state information be sent for all OCh associated with this adjacency. The TxSeqNum may eventually exceed 2^32. When this occurs, the TxSeqNum will wrap to the value of 1.

D.2.1.2 Hello validity TLV

The C-type is 240, Class is 1 and length is 8. The value is formatted as shown in Figure D.4.

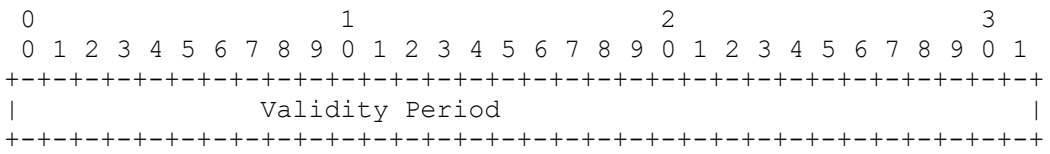


Figure D.4 – OOB OCh-O and OTSiG-O protocol Hello validity format

The Validity Period field describes the amount of time (in ms) before another Hello must be received for the adjacency to be considered up. A transmitter should send subsequent Hello messages prior to

the expiration of the validity period. The receiver of the Hello must update the expiration of the adjacency health timer upon receipt of a Hello PDU. If the validity period expires, the adjacency shall raise an alarm to the equipment management function (EMF). This alarm clears when the Hello protocol receives a Hello message from the peer starting a new validity period.

D.2.2 Status Reporting sub-protocol

Status Reporting PDUs are issued for one or more OCh and/or OTSiA connections and signals as state changes occur or initial state requests are received. These PDUs use message type 17. The PDUs each contains a Message ID TLV, an OPS Trail Identification TLV, along with one or more identifiers for one or more OCh-P and/or OTSiG link connections and one OCh and OTSiA Status TLVs.

It is possible for multiple OCh-P and/or OTSiG Link Connections that change state at the same time to be reported in a single status reporting PDU. In this case, all OCh-Ps and/or OTSiGs identified in the PDU will have the same status.

The format of these TLVs is as follows:

D.2.2.1 Message ID TLV

The Message ID TLV contains the TxSeqNum for this specific status reporting PDU. The class number is 5 and the C-Type 1. The TLV length is 8. The format is shown in Figure D.5.

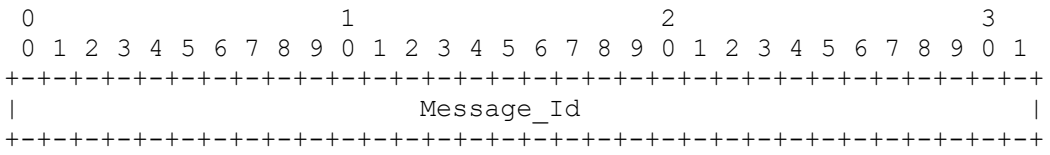


Figure D.5 – OOB OCh and OTSiA status reporting Message ID format

D.2.2.2 OPS Trail Identification TLV

The namespace used for OPS Trail identification is the TCP_ID namespace used by G.7714 neighbour discovery. Control ~~plane~~ domain names are not used as it is not guaranteed that a control ~~plane~~ domain is active on this link.

An OPS Trail Identification TLV has a C-type of 241 and Length of 16. The class uses the Format ID defined for each TCP-ID format in [ITU-T G.7714.1]. The Value field is formatted as shown in Figure D.6, Figure D.7 and Figure D.8 for TCP-ID Name, DCN Address format and DCN Name formats, respectively.

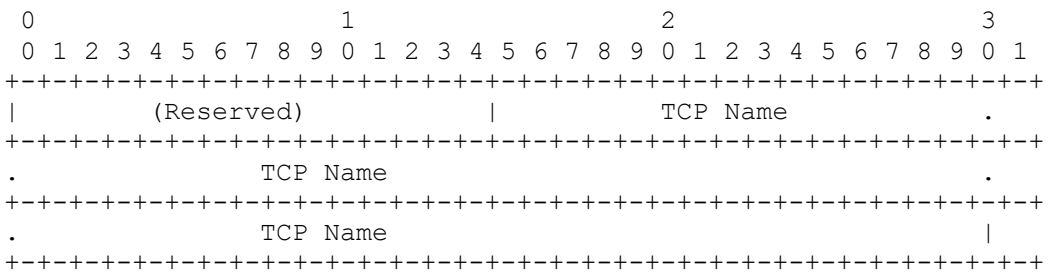


Figure D.6 – OOB OPS Trail and OCh-P and OTSiG Link Connection ID – TCP-ID Name format (Class=1)

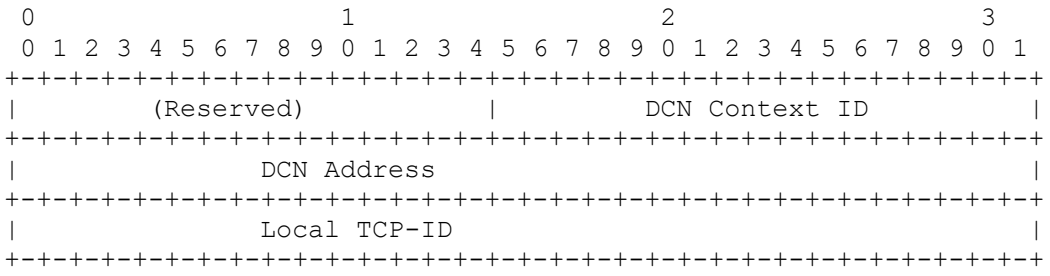


Figure D.7 – OOB OPS Trail and OCh-P and OTSiG Link Connection ID – DCN Address format (Class=2)

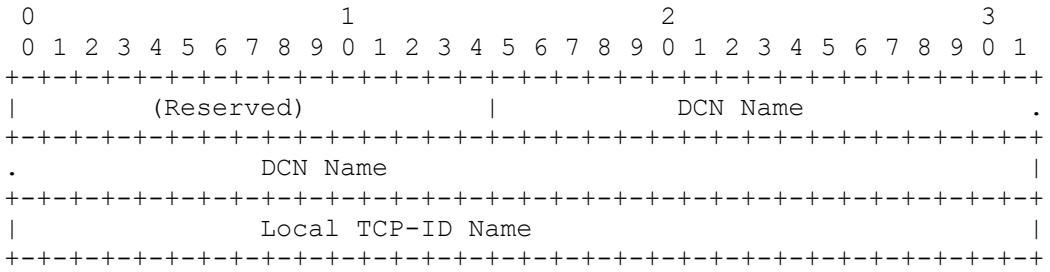


Figure D.8 – OOB OPS Trail and OCh-P and OTSiG Link Connection ID – DCN Name format (Class=3)

D.2.2.3 OCh-P and OTSiG Link Connection ID TLV

The OCh-P and OTSiG Link Connection ID TLV identifies an OCh-P or OTSiG instance carried by the OPS trail.

The namespace used for OCh-P and OTSiG Link connection ID is the TCP-ID namespace used by [ITU-T G.7714.1] neighbour discovery. Control ~~plane~~ domain names are not used as it is not guaranteed that a control ~~plane~~ domain is active on this link.

The format for the OCh-P and OTSiG Link Connection ID TLV is the same as the format for the OPS Trail ID TLV.

An OCh-P and OTSiG Link Connection ID TLV has a C-type of 244 and length of 16. The class uses the Format ID defined for each TCP-ID format in [ITU-T G.7714.1]. The Value field for the OCh-P and OTSiG Link Connection ID TLV is formatted as shown in Figure D.6, Figure D.7, and Figure D.8 for TCP-ID Name, DCN Address and DCN Name format, respectively.

Multiple Link Connection Identification TLVs may be carried in the same status update message. In this case, all OCh-P and/or OTSiG link connections in the message will have the same status.

D.2.2.4 OCh and OTSiG Status TLV

The OCh and OTSiG-O Status TLV is a bit vector providing status indication for one or more OCh-P and/or OTSiG link connections identified in the status reporting PDU. The Class number is 242 and the C-Type is 1. The TLV Length is 8. The format is shown in Figure D.9.

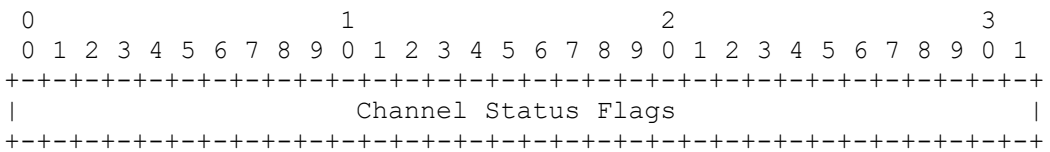


Figure D.9 – OCh and OTSiG Status TLV format

The flags in the Channel Status Flags field are defined as follows:

0x0000.0001: FDI-P

0x0000.0002: FDI-O

0x0000.0004: OCI

All remaining flags are reserved. Reserved flags are transmitted as zero (0) and ignored on reception.

D.2.3 Protocol adaptation to IPv4 DCN

The OOB OCh-O and OTSiG-O protocol is carried over IPv4 networks using unicast user datagram protocol (UDP) messages.

The OOB OCh-O and OTSiG-O PDUs are carried as payload within adaptation frames with one PDU in each frame. The adaptation uses the format in Figure D.10.

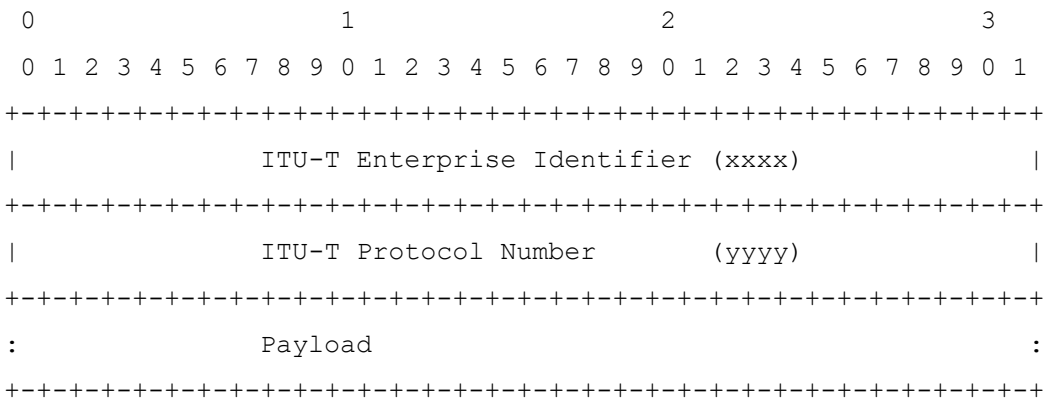


Figure D.10 – OOB OCh-O and OTSiG-O protocol UDP/IPv4 frame format

While the OOB OCh-O and OTSiG-O protocol does not have a byte-count limit on a PDU, they are to be carried within a single IPv4 PDU to the destination to avoid problems with complete message loss due to message fragmentation and loss of fragments. For this reason, the IPv4 DoNotFragment bit should be set and PDUs should be less than 1500 bytes (inclusive of IPv4, UDP and frame header overheads).

D.2.4 OTSiG-O TTI TLV

The TTI TLV is a string providing the TTI associated with the end-to-end OTSiA being reported. The class number is 243, the C-Type is 1 and the length is 68. The format is shown in Figure D.11.

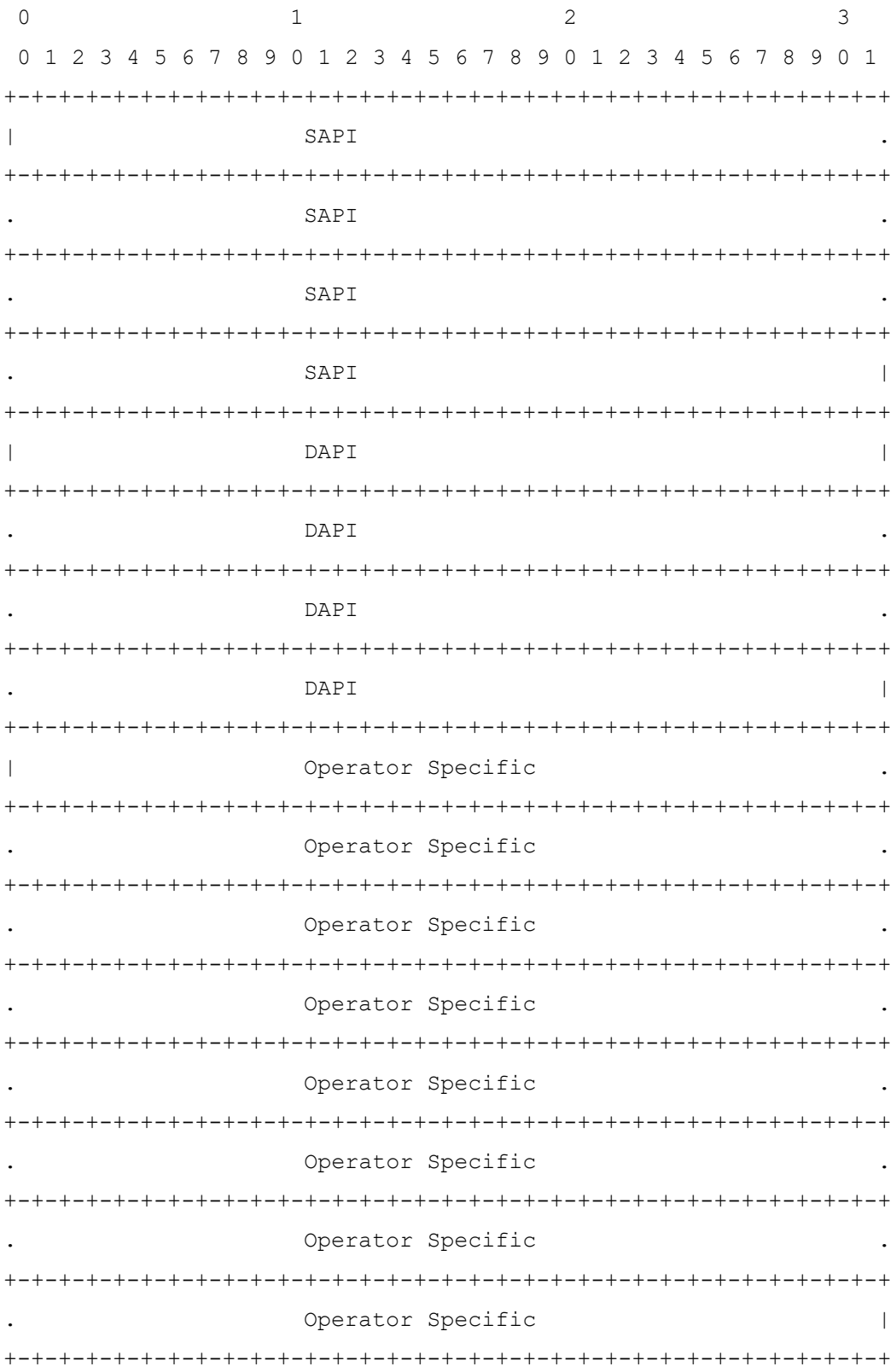


Figure D.11 – OOB OTSiG Status Reporting protocol TTI format

D.2.5 OTSiG-O BDI TLV

The backward defect indication (BDI) TLV is a string providing the BDI-P and BDI-O associated with the end-to-end OTSiA trail being reported. The class number is 245, the C-Type is 1 and the length is 8. The format is shown in Figure D.12.

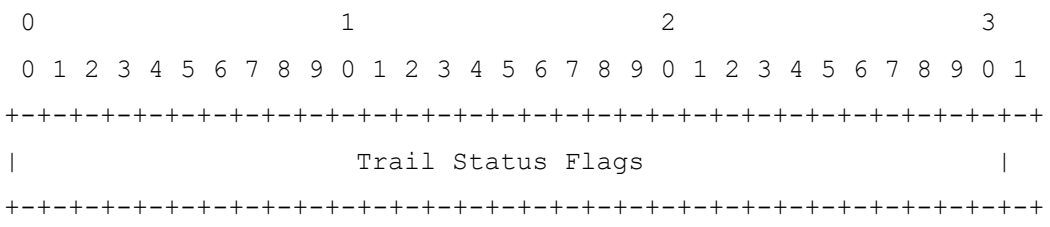


Figure D.12 – OTSiA Trail Status TLV format

The flags in the Trail Status Flags field are defined as follows:

0x0000.0001: BDI-P

0x0000.0002: BDI-O

All remaining flags are reserved. Reserved flags are transmitted as zero (0) and ignored on reception.

D.2.6 OTSi TSI TLV

The optical tributary signal (OTSi) TSI TLV is providing the OTSi TSI associated with one of the OTSi instances within the end-to-end OTSiG being reported. An OTSiG consisting of multiple OTSi will have multiple OTSi TLVs, one per OTSi. An OTSi TSI TLV contains a [ITU-T G.698.2] application code plus nominal central frequency. The class number is 246, the C-Type is 1 and the length is 16. The format is shown in Figure D.13. This format is based on the application code format as specified in [IETF RFC 7581] and wavelength ID format as specified in Appendix V of [ITU-T G.697].

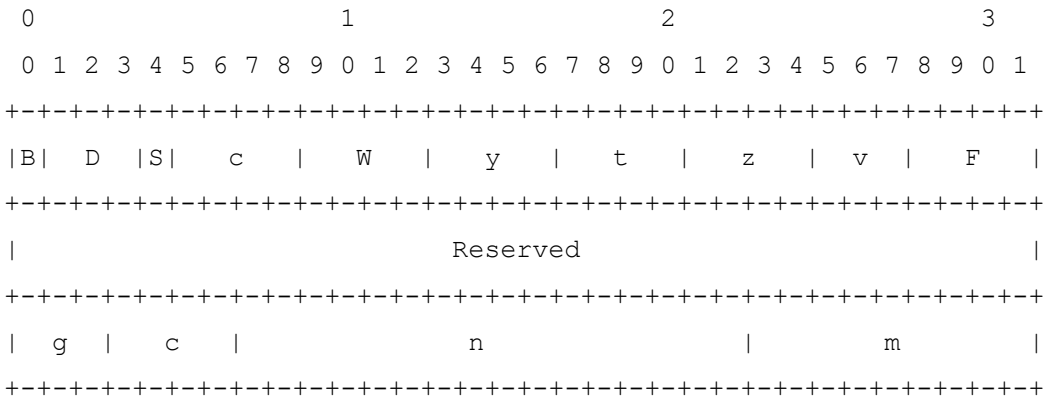


Figure D.13 – OTSi TSI TLV format

D.3 OCh_O and OTSiG-O communication channel adaptation function

D.3.1 OCh_O communication channel adaptation function (OCC/OCh-O_A)

The OCC/OCh-O_A function aggregates/de-aggregates OCh_CI_OH.

The specification of this function is for further study.

D.3.2 OCh_O and OTSiG-O communication channel adaptation function (OCC/OCh|OTSiG-O_A)

The OCC/OCh|OTSiG-O_A function aggregates/de-aggregates OCh_CI_OH and OTSiG_CI_OH.

The specification of this function is for further study.

D.4 OCh_O [and OTSiG-O] communication channel termination function (OCC_TT)

The OCC_TT functions are responsible for the end-to-end supervision of the OCC trail.

The specification of this function is for further study.

Appendix I

Constraints of the interworking functions in DCN

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

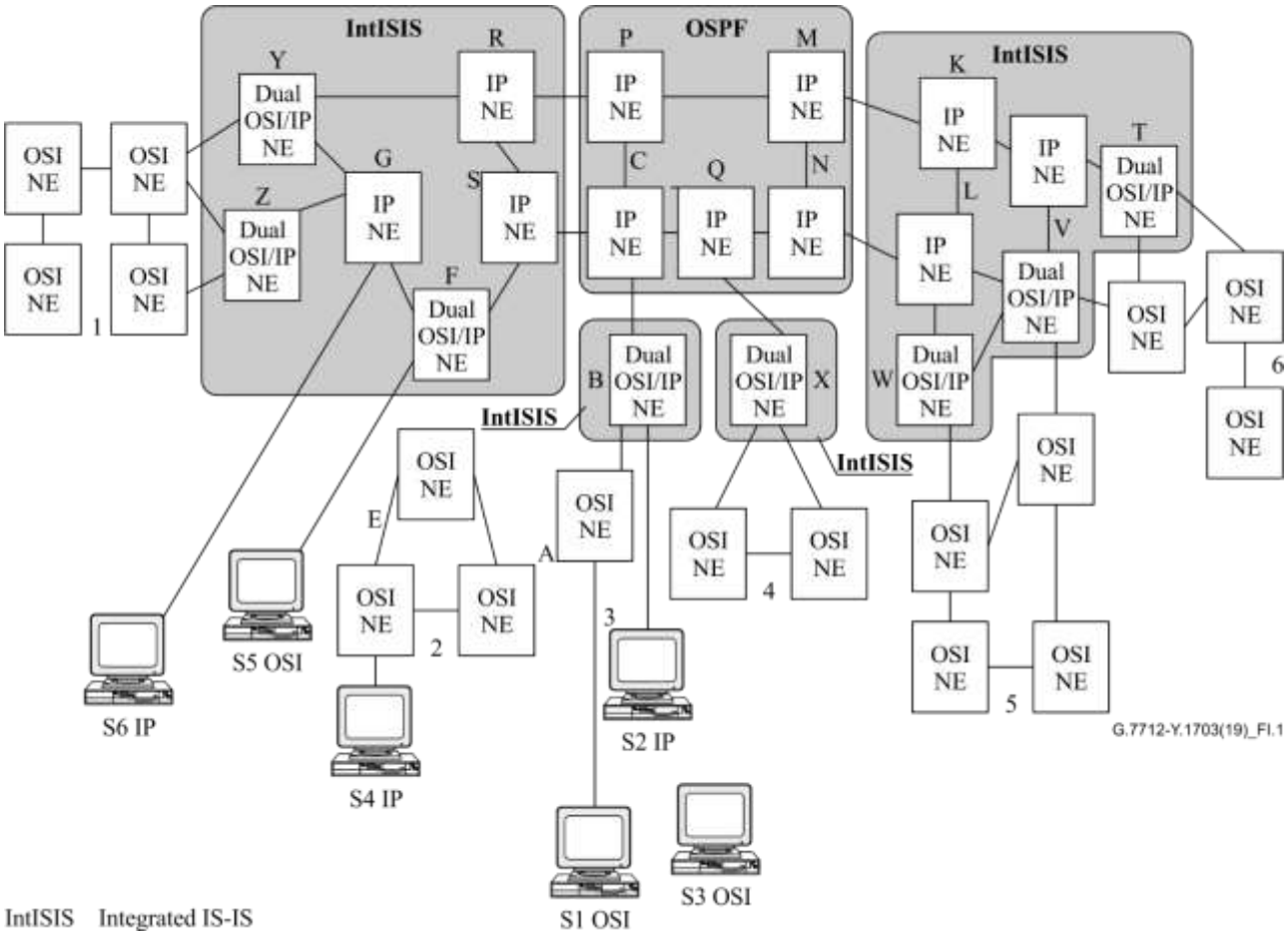


Figure I.1 – Interworking scenarios

I.1 General assumptions

DCN covers the IWF for Layer 2-3 of the IP-OSI stacks. Interworking mechanisms that apply to other layers are out of the scope of this Recommendation (i.e., mediation).

See clause 7.1.7 for a definition of interworking.

Tunnels are based on RFCs.

The IP-only NEs support IP routing and may contain redistribution between integrated IS-IS and OSPF.

I.2 Common to all scenarios

Dynamic routing is accomplished through the use of route redistribution of IP address information between OSPF and IS-IS NEs. Route redistribution is performed on the OSPF nodes between the pairs: (R,P), (S,C), (M,K), (N,L).

I.2.1 Scenario 1: OSI-based management system connected to node A

There must be at least one tunnel configured from B to one or more of Y or Z.

There must be a tunnel configured from B to X.

There must be a tunnel configured from B to F.

There must be at least one tunnel configured from B to one or more of W, V or T.

The above tunnels will probably have IS-IS running across them (inside the tunnel); however, inter-domain routing techniques is also a possibility. Under some conditions, some tunnels could become congested as a result of routing choices.

An OSI-based management system now has CLNS connectivity to any OSI-only or dual stack NE in the network, but does not have connectivity with IP-only NEs. Although an OSI-based manager will be able to send CLNS packets to a dual stack NE, it will not be able to manage it unless it is OSI manageable.

I.2.2 Scenario 2: IP-based management systems connected to node B

In this particular network, IP traffic can be forwarded from B to all IP NEs without requiring tunnels. OSPF NEs P, C, M, and N must support redistribution of IP routes into integrated IS-IS. Filters will have to be configured on OSPF nodes P, C, M, and N in order to stop routing loops from forming.

An IP-based management system now has IP connectivity to any IP-only or dual stack NE in the network but does not have connectivity with OSI-only NEs. Although an IP-based manager will be able to send IP packets to a dual stack NE, it will not be able to manage it unless it is IP manageable.

I.2.3 Scenario 3: OSI-based management systems connected to node C

NE C cannot provide OSI connectivity, and so CLNS packets cannot be forwarded; therefore, an OSI-based management system cannot function at this location.

I.2.4 Scenario 4: IP-based management systems connected to node E

NE E cannot provide IP connectivity, and so IP packets cannot be forwarded; therefore, an IP-based management system cannot function at this location.

I.2.5 Scenario 5: OSI-based management systems connected to node F

CLNS traffic can pass through NE F to OSI network 2 without requiring tunnels as NE F can forward CLNS packets natively.

There must be a tunnel configured from F to B.

There must be at least one tunnel configured from F to one or more of Z or Y.

There must be a tunnel configured from F to X.

There must be at least one tunnel configured from F to one or more of W, V or T.

The above tunnels will probably have IS-IS running across them (inside the tunnel); however, inter-domain routing techniques are also a possibility. Under some conditions, some tunnels could become congested as a result of routing choices.

An OSI-based management system now has CLNS connectivity to any OSI-only or dual stack NE in the network but does not have connectivity with IP-only NEs. Although an OSI-based manager will be able to send CLNS packets to a dual stack NE, it will not be able to manage it unless it is OSI manageable.

I.2.6 Scenario 6: IP-based management systems connected to node G

In this particular network, IP traffic can be forwarded from G to all IP NEs without requiring tunnels. OSPF NEs P, C, M, and N must support redistribution of IP routes into integrated IS-IS. Filters will have to be configured on each OSPF nodes P, C, M, and N in order to stop routing loops from forming.

An IP-based management system now has IP connectivity to any IP-only or dual stack NE in the network, but does not have connectivity with OSI-only NEs. Although an IP-based manager will be able to send IP packets to a dual stack NE, it will not be able to manage it unless it is IP manageable.

Appendix II

Example implementation of automatic encapsulation

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

II.1 Introduction

This appendix is not a requirement but gives brief example details on how a node may be implemented with respect to one aspect of the feature specified in this Recommendation.

The simplest way (but not the only way) for a node to calculate the next node along the shortest path to the final destination of a packet that can unencapsulate is to modify the SPF algorithm to achieve this.

The algorithm can be modified to find the next node along the shortest path to the destination that can accept IP over OSI encapsulated traffic, and the next node along the shortest path to the destination that can accept OSI over IP encapsulated traffic. Note that these two may be the same node, or may be two separate nodes. A modified Dijkstra algorithm is provided below that achieves this.

This additional process only needs to happen when the next hop does not support the network layer protocol of the type that corresponds to the destination address for that path. If the next hop does support that type of network layer protocol (as specified in the "protocols supported" TLV present in IS-IS Hello PDUs received from that node), then packets to that destination may simply be forwarded natively and forgotten, and so the search for a node along the path that can unencapsulate is not necessary.

The algorithm must then identify an IP address for this next unencapsulation node if the destination of the path is an OSI end system and must then identify an OSI address for this next unencapsulation node if the destination of the PATH is an IP address.

Failure to find an IP address for this next unencapsulation node indicates a configuration error in that node (no IP address); this may optionally result in an error message being sent to the network administrator. Packet loss will result if a CLNS packet requires tunnelling to that node over IP as, without an IP destination address, encapsulation may not be possible and the packet will be discarded instead.

Failure to find a node that can unencapsulate indicates a network design error, more specifically, a failure to conform to the topological restrictions stated in this Recommendation. This should result in a "destination unreachable" error report.

For each IP destination that requires encapsulation to get beyond the next hop, the node can then put a marker in the IP forwarding table indicating the OSI destination address that must be used to encapsulate all IP packets destined for that address.

For each OSI destination that requires encapsulation to get beyond the next hop, the node can then put a marker in the OSI forwarding table indicating the IP destination address that must be used to encapsulate all OSI packets destined for that address.

A node that supports IPv4, IPv6 and OSI may find two addresses (for example, an IPv4 address and an IPv6 address) that could be used to encapsulate. In this case, it may choose either as long as it results in a packet that is of a network layer protocol type that the next hop supports (as specified in the "protocols supported" TLV present in IS-IS Hello PDUs received from that node).

II.2 Updates to Dijkstra's algorithm

The following clauses contain the full Dijkstra's algorithm including extensions to support auto-tunnelling. It is based on the algorithm as specified in [IETF RFC 1195]. The algorithm shown is suitable for a dual IPv4 and CLNS automatically-encapsulating node. Changes to this algorithm are shown in ***Bold Italic***.

The algorithm produces a PATHS database containing, for each destination, the identity of the first node from S to N capable of unencapsulating IP over OSI, and the identity of the first node from S to N capable of unencapsulating OSI over IP.

For each IP destination, the first node from S to N capable of unencapsulating IP over OSI may have its OSI address loaded into the IP forwarding table as the destination address to be used in any CLNP packet used to encapsulate IP over OSI, if the next hop does not support IP.

For each OSI end system, the first node from S to N capable of unencapsulating OSI over IP may have one of its IP addresses loaded into the OSI forwarding table as the destination address to be used in any IP packet used to encapsulate OSI over IP, if the next hop does not support OSI.

II.2.1 Changes to database

The PATHS and TENTS database should be updated to contain an extension to the {Adj(N)}, element of the triple. The adjacency N element will contain two corresponding dual protocol support (IDP(N)-ODP(N)) entries which will represent the system ID of the first dual router on the path from S to N capable of de-encapsulating IP over OSI tunnelled packets (IDP(N)) and the system ID of the first dual router on that path from S to N capable of de-encapsulating OSI over IP tunnelled packets (ODP(N). If no *DP(N) router exists on the PATH, then this value will be set to zero. If multiple Adj(N) entries exist in either the TENTS or the PATHS database, then each adjacency will have corresponding *DP(N) entries. Thus, each triple will take the format <N,d(N),{Adj(N)-IDP(N)-ODP(N)}>.

If the value of IDP(N) is set to 0, then this means that no dual router exists on the path to the destination capable of de-encapsulating and encapsulating IP over OSI packets.

If the value of ODP(N) is set to 0, then this means that no dual router exists on the path to the destination capable of de-encapsulating and encapsulating OSI over IP packets.

II.2.2 Changes to algorithm

The SPF algorithm specified in section C.1.4 of [IETF RFC 1195] is amended to appear as follows:

Step 0: Initialize TENT and PATHS to empty. Initialize tentlength to
[internalmetric=0, externalmetric=0].

(tentlength is the pathlength of elements in TENT that we are examining.)

1) Add <SELF,0,W***-0-0***> to PATHS, where W is a special value indicating traffic to SELF is passed up to internal processes (rather than forwarded).

2) Now pre-load TENT with the local adjacency database (each entry made to TENT must be marked as being either an End System, or a router, to enable the check at the end of Step 2 to be made correctly – Note that each local IP reachability entry is

included as an adjacency, and is marked as being an End System).
For each adjacency Adj(N) (including level 1 OSI Manual
Adjacencies, or Level 2 OSI enabled reachable addresses, and
IP reachability entries) on enabled circuits, to system N of
SELF in state "Up" compute:

d(N) = cost of the parent circuit of the adjacency (N),
obtained from metric.k , where k = one of {default metric,
delay metric, monetary metric, error metric}

Adj(N)***-IDP(N)-ODP(N)*** = the adjacency number of the adjacency to N, ***the SID of the next-hop router along the path to the neighbour capable of de-encapsulating IP over OSI packets, and the SID of the next-hop router along the path to the neighbour capable of de-encapsulating OSI over IP packets.***

In this case, i.e., during initialization, both DP values will be set to 0

3) If a triple <N,x,{Adj(M)-***IDP(N)-ODP(N)***}> is in TENT, then:

If x = d(N), then {Adj(M)-***IDP(N)-ODP(N)***} <--- {Adj(M)-***IDP(M)-ODP(M)***}
U {Adj(N)-***IDP(N)-ODP(N)***}.

4) If N is a router or an OSI End System entry, and there are now
more adjacencies in {Adj(M)} than maximumPathSplits, then remove
excess adjacencies as described in Clause 7.2.7 of ISO/IEC 10589. If N
is an IP Reachability Entry, then excess adjacencies may be
removed as desired. This will not effect the correctness of
routing, but may eliminate the determinism for IP routes (i.e.,
IP packets still follow optimal routes within an area, but
where multiple equally good routes exist, will not necessarily
follow precisely the route that any one particular router
would have anticipated).

5) If x < d(N), do nothing.

6) If x > d(N), remove <N,x,{Adj(M)***-IDP(M)-ODP(M)***}> from TENT and add the
triple
<N,d(N),{Adj(N) ***-IDP(N)-ODP(N)***}>.

7) If no triple <N,x,{Adj(M)***-IDP(M)-ODP(M)*** }> is in TENT, then add
<N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}> to TENT.

8) Now add systems to which the local router does not have adjacencies,
but which are mentioned in neighbouring pseudonode LSPs. The

adjacency for such systems is set to that of the designated router. Note that this does not include IP reachability entries from neighbouring pseudonode LSPs. In particular, the pseudonode LSPs do not include IP reachability entries.

9) For all broadcast circuits in state "On", find the pseudonode LSP for that circuit (specifically, the LSP with number zero and with the first 7 octets of LSPID equal to LnCircuitID for that circuit, where n is 1 (for Level 1 routing) or 2 (Level 2 routing)). If it is present, for all the neighbours N reported in all the LSPs of this pseudonode which do not exist in TENT add an entry <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}> to TENT, where:

   d(N) = metric.k of the circuit.
   Adj(N) = the adjacency number of the adjacency to the DR.

10) Go to Step 2.

Step 1: Examine the zeroeth link state PDU of P, the system just placed on PATHS (i.e., the LSP with the same first 7 octets of LSPID as P, and LSP number zero).

1) If this LSP is present and the "Infinite Hippity Cost" bit is clear For each Adj(*) – IDP(*) – ODP(*) pair in the PATHS database for P. If this is not a pseudo-node LSP and if IDP(*) is equal to zero then check the unencapsulation capability field of the LSP, if it supports IP over OSI then set the IDP(P) value for this adjacency to be the system ID of P. if ODP(*) is equal to zero then check the unencapsulation capability field of the LSP, if it supports OSI over IP then set the IDP(P)value for this adjacency to be the system ID of P

2) If this LSP is present, and the "Infinite Hippity Cost" bit is clear, then for each LSP of P (i.e., all LSPs with the same first 7 octets of LSPID and P, irrespective of the value of SP number) compute:

   dist(P,N) = d(P) + metric.k(P,N)

for each neighbour N (both End System and router) of the system P. If the "Infinite Hippity Cost" bit is set, only consider the End System neighbours of the system P.

Note that the End Systems neighbours of the system P includes IP reachable address entries included in the LSPs from system P. Here, d(P) is the second element of the triple

<P,d(P),{Adj(P)***-IDP(P)-ODP(P)***}>

and metric.k(P,N) is the cost of the link from P to N as reported in P's link state PDU.

3) If dist(P,N) > MaxPathMetric, then do nothing.

4) If <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}> is in PATHS, then do nothing.

NOTE – d(N) must be less than dist(P,N), or else N would not have been put into PATHS. An additional sanity check may be done here to ensure that d(N) is in fact less than dist(P,N)

5) If a triple <N,x,{Adj(N)***-IDP(N)-ODP(N)***}> is in TENT, then:

a) If x = dist(P,N), then {Adj(N)***, IDP(N)-ODP(N)***} <-- {Adj(N)***-IDP(N)-ODP(N)***} U {Adj(P)***-IDP(P)-ODP(N)***}.
Note that even if the value of Adj(N) is equal to the value Adj(P) but the corresponding values of either IDP(P) or ODP(P) and IDP(N) or ODP(N) are different then this should be treated as a different adjacency and will represent a different path to the destination.

b) If N is a router or an OSI end system, and there are now more adjacencies in {Adj(N)} than maximumPath Splits, then remove excess adjacencies, as described in clause 7.2.7 of ISO/IEC 10589. For IP Reachability Entries, excess adjacencies may be removed as desired. This will not effect the correctness of routing, but may eliminate the determinism for IP routes (i.e., IP packets will still follow optimal routes within an area, but where multiple equally good routes exist, will not necessarily follow precisely the route that any one particular router would have anticipated).

c) if x < dist(P,N), do nothing.

d) if x > dist(P,N), remove <N,x,{Adj(N)***-IDP(N)-ODP(N)***}> from TENT, and add <N,dist(P,N),{Adj(P)***-IDP(P)-ODP(P)***}>

6) if no triple <N,x,{Adj(N)}> is in TENT, then add <N,dist(P,N),{Adj(P)}> to TENT.

Step 2: If TENT is empty, stop. Else:

1) Find the element <P,x,{Adj(P)***-IDP(P)-ODP(P)***}>, with minimal x as follows:

a) If an element <*,tentlength,*> remains in TENT in the list for tentlength, choose that element. If there are more than one elements in the list for tentlength, choose one of the elements (if any) for a system which is a pseudonode in preference to one for a non-pseudonode. If there are no more elements in the list for tentlength, increment tentlength and repeat Step 2.

b) Remove <P,tentlength,{Adj(P)***-IDP(P)-ODP(P)***}> from TENT.

c) Add <P,d(P),{Adj(P)***-IDP(P)-ODP(P)***}> to PATHS.

d) If this is the Level 2 Decision Process running, and the system just added to PATHS listed itself as Partition Designated Level 2 Intermediate system, then additionally add <AREA.P,d(P),{Adj(P)}> to PATHS, where AREA.P is the Network Entity Title of the other end of the Virtual Link, obtained by taking the first AREA listed in P's LSP and appending P's ID.

e) If the system just added to PATHS was an end system, go to step 2. Else go to Step 1.

NOTE – In the Level 2 context, the "End Systems" are the set of Reachable Address Prefixes (for OSI), the set of Area Addresses with zero cost (again, for OSI), plus the set of IP reachability entries (including both internal and external).

Appendix III

Commissioning guide for SDH NEs in dual [IETF RFC 1195] environment and impact of automatic encapsulation option

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

III.1 Introduction

This appendix provides guidance on installing Integrated IS-IS nodes in a dual IPv4 and OSI network, and on how to use the optional automatic encapsulation feature described in Annex B.

III.2 Integrated IS-IS without automatic encapsulation

III.2.1 Introduction and rules of [IETF RFC 1195]

Integrated IS-IS, as specified in [IETF RFC 1195], was originally written as a dual routing protocol. Specifically, it was written to be able to route both IPv4 and CLNP using a single SPF calculation, a single set of metrics for both IP and CLNP and a single set of Hellos and LS-PDUs.

More specifically, integrated IS-IS routers, conforming to [IETF RFC 1195], calculate shortest paths across a Level-1 area or Level-2 subdomain without considering whether any candidate router can actually forward a specific type of packet.

This is clearly stated in [IETF RFC 1195] in section 3.10:

– "The Dijkstra computation does not take into consideration whether a router is IP-only, OSI-only, or dual. The topological restrictions specified in section 1.4 ensure that IP packets will only be sent via IP-capable routers, and OSI packets will only be sent via OSI-capable routers."

With integrated IS-IS, a router is just a router. The assumption is that any router in the network can handle any type of packet that is thrown at it.

Therefore, integrated IS-IS routers calculate routes, and forward packets based on this assumption, and it is the responsibility of an operator to make sure that the assumption is actually true.

Thus, there are the topological restrictions of [IETF RFC 1195]. Failure to enforce the topological restrictions of [IETF RFC 1195] may result in packet loss, as packets disappear into the black-hole of a router that simply discards packets that it cannot forward, as it does not support them.

In a simple single Level-1 area network, the rules are quite simple. These are:

1) If IPv4 packets are to be forwarded in an area, then all of the routers in the area must be able to forward IPv4 packets;
2) If CLNP packets are to be forwarded in an area, then all of the routers in the area must be able to forward CLNP packets;
3) If both IPv4 and CLNP packets are to be forwarded in an area, then all of the routers in the area must be dual, i.e., able to forward both.

Thus, it is fairly easy to classify IS-IS Level-1 areas into the classes "OSI-only area", IP-only area", and "Dual area". This is shown in Figure III.1.

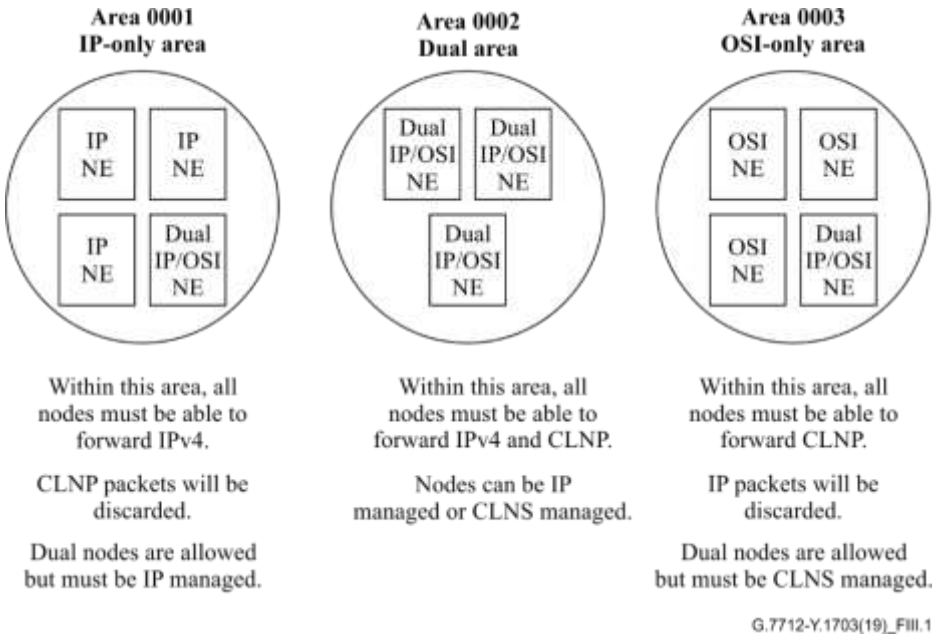


Figure III.1 – Classification of IS-IS Level-1 areas

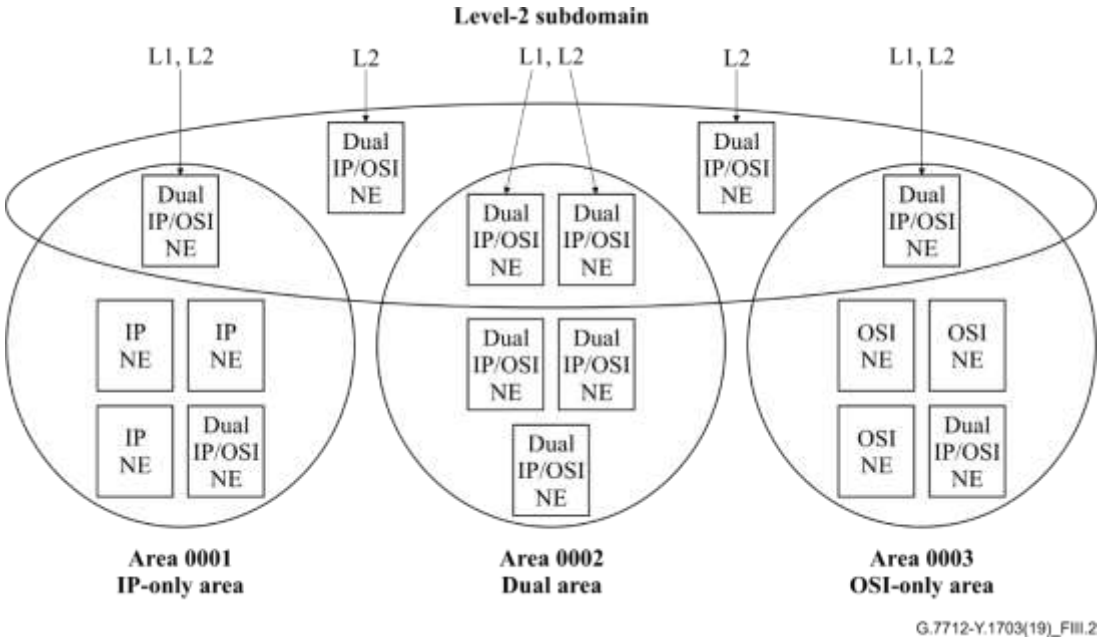
III.2.2 Level-2 subdomain

If a larger network is needed, requiring Level-2 routing, then the Level-2 subdomain forwards packets between the Level-1 areas, and thus must support all of the types of packets present in all of those Level-1 area. The rules for the Level-2 subdomain are:

1) If IPv4 packets are forwarded in any of the areas (IP-only or dual areas), then all of the routers in the Level-2 subdomain must be able to forward IPv4.

2) If CLNP packets are forwarded in any of the areas (OSI-only or dual areas), then all of the routers in the Level-2 subdomain must be able to forward CLNP.

Therefore, if any of the areas is dual, or if both OSI-only and IP-only areas exist, then the routers in the Level-2 subdomain must be dual. This is illustrated in Figure III.2.



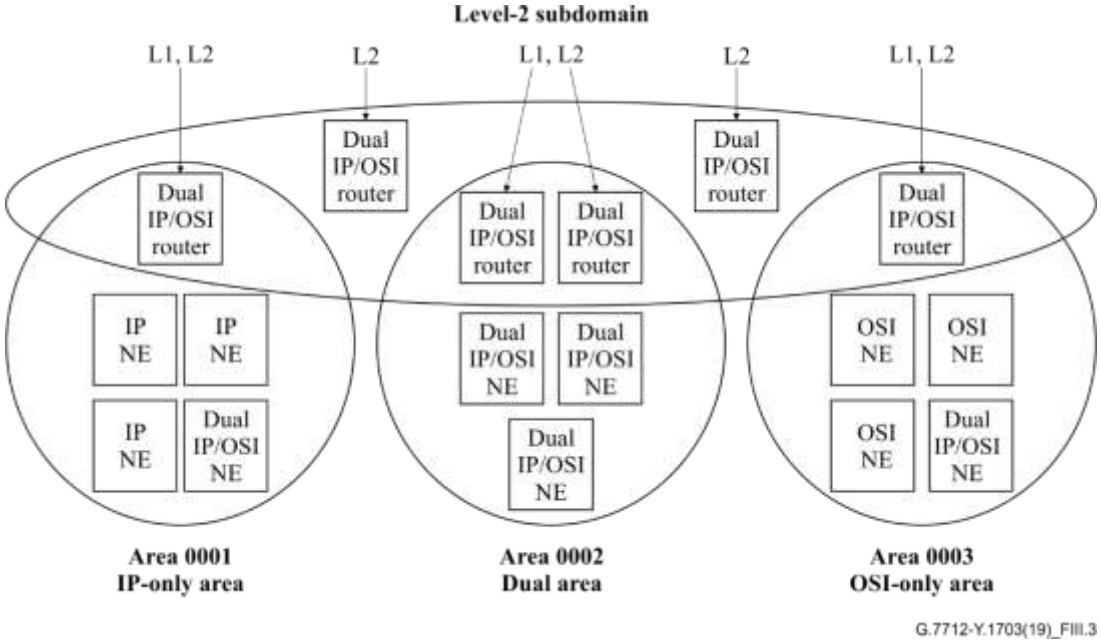
As both IPv4 and CLNP are forwarded within the Level-1 areas, all of the nodes in the Level-2 subdomain must be dual, even those present in IP-only or OSI-only areas. A node is in the Level-2 subdomain if it runs Level-2 routing.

Figure III.2 – Level-2 subdomain

III.2.3 Level-2 subdomain with external routers running integrated IS-IS

Many operators currently run Level-1 IS-IS routing in their OSI-only SDH NEs, and then link up multiple areas using Level-2 IS-IS routing in an external router network.

If an operator wishes to use a similar model for a dual network, then they can run Level-1 integrated IS-IS in each area, and Level-2 integrated IS-IS in an external router network. This gives a very similar network to the previous one, as shown in Figure III.3



As both IPv4 and CLNP are forwarded within the Level-1 areas, all of the routers in the Level-2 subdomain must be dual, even those present in IP-only or OSI-only areas.

Figure III.3 – Level-2 IS-IS routing in an external router network

III.2.4 External routers running OSPF or other IP routing protocols

Many operators currently run Level-2 IS-IS in their external routers, and OSPF, or other routing protocols, for IP. In this case, the external router must remain as the Level-2 router for the SDH NEs, and so, for a dual area, must be a dual integrated IS-IS router. However, the router may be configured to route all IP packets using OSPF by configuring redistribution of IP routes between IS-IS and OSPF. In this way, all IP packets will be OSPF routed, whilst CLNP packets continue to be Level-2 IS-IS routed. This is shown in Figure III.4.

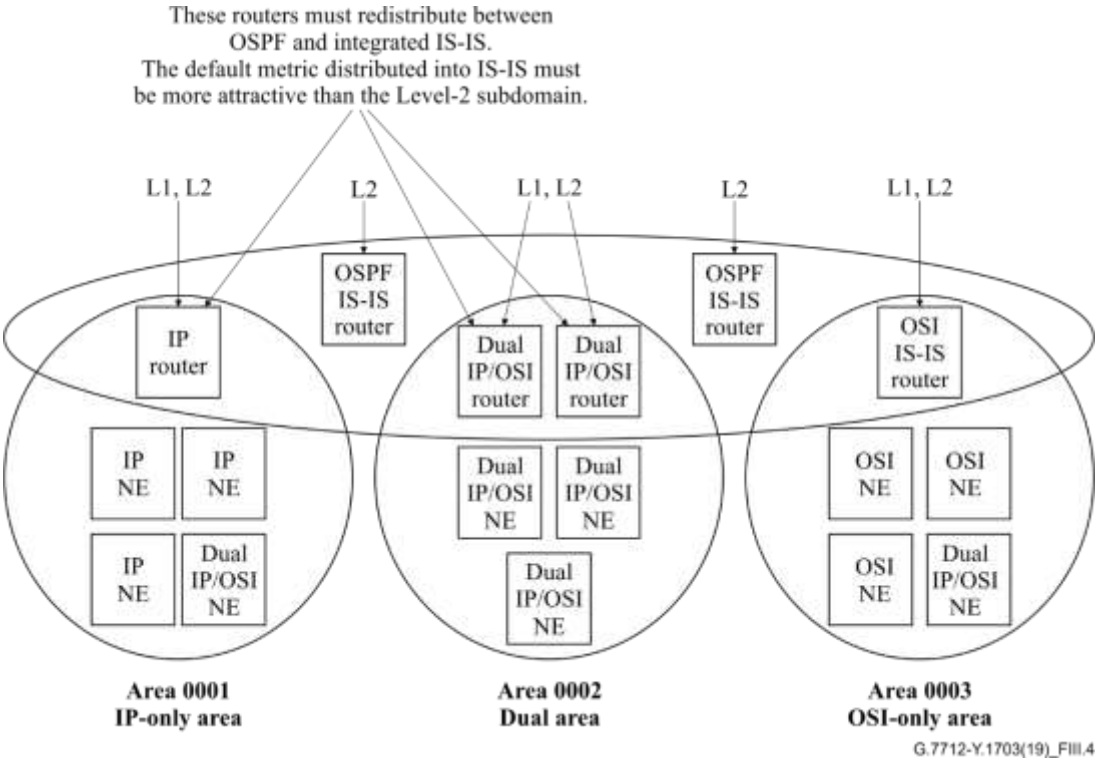


Figure III.4 – External routers running OSPF

Note that the integrated IS-IS stack in the external routers will not be aware that the Level-2 subdomain is meant only for CLNP packets. The OSPF learned routes must, therefore, be redistributed into integrated IS-IS with a low default metric, to make them more attractive to IP packets than the Level-2 subdomain.

III.3 Integrated IS-IS with automatic encapsulation

III.3.1 Introduction and effect on topological restrictions

The automatic encapsulation option allows the topological rules of [IETF RFC 1195] to be broken. Automatic encapsulation effectively makes a node, or group of nodes, appear to be able to forward packets that, intact, they cannot.

This is shown in Figure III.5.

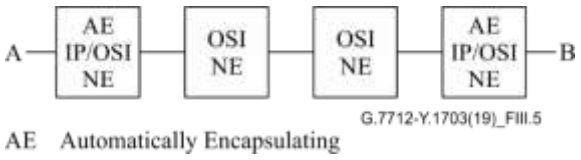


Figure III.5 – Group of nodes with automatic encapsulation

This group of nodes will now forward both IPv4 and CLNP packets, as long as the packets enter at point A or B, through one of the automatically encapsulating nodes.

The group of nodes may now safely be put into a dual area, or a dual Level-2 subdomain, as the pair of automatically encapsulating nodes will forward IPv4 packets by encapsulating them inside CLNP packets, so that they will be forwarded by the OSI-only NEs rather than being discarded.

A valid dual area may now appear as shown in Figure III.6.

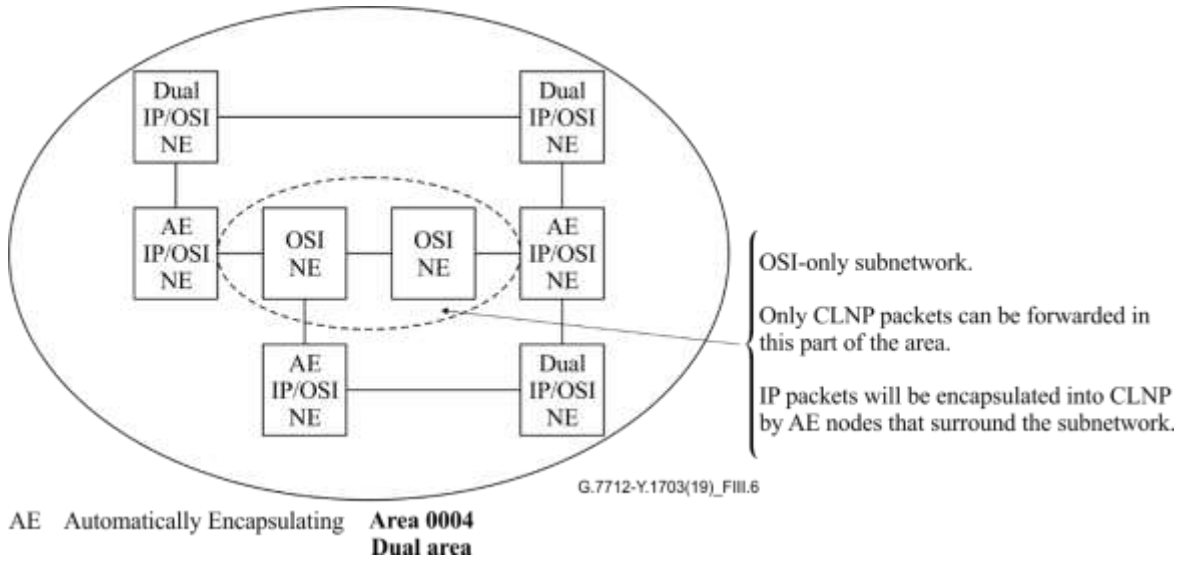


Figure III.6 – Example of a valid dual area

Note that the OSI-only nodes must not be directly connected to one of the dual nodes that do not have the automatic encapsulation option. It is only the presence of the automatic encapsulating nodes that prevent IPv4 packets from being sent to an OSI-only node.

A dual node may be connected directly to an OSI-only node if it is also treated as an OSI-only node, as shown in Figure III.7.

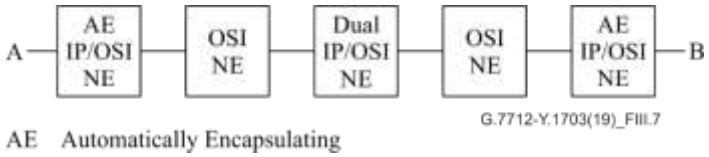


Figure III.7 – Connection of a dual node to an OSI-only node

In this case, the network acts as a dual network for packets going from point A to B, but IPv4 packets cannot reach the central dual node. This dual node is inside an OSI-only subnetwork. This dual node will be able to forward CLNP packets only and must be CLNS managed. There must be no other connections to the central dual node, as, if IPv4 packets were introduced at the central node, then they might be forwarded to an OSI-only node and be discarded.

III.3.2 Getting IP traffic in and out of the SDH embedded network

III.3.2.1 IP capable gateway NE

Both IP and CLNP packets must be able to enter and leave a dual area, whether or not automatic encapsulation is used. Normally traffic enters and leaves an IS-IS area via Level-1, Level-2 routers. These are routers that participate both in the Level-1 area and in the Level-2 subdomain.

The simplest way to build this is to ensure that any Level-1, Level-2 routers are dual, as shown in Figure III.8.

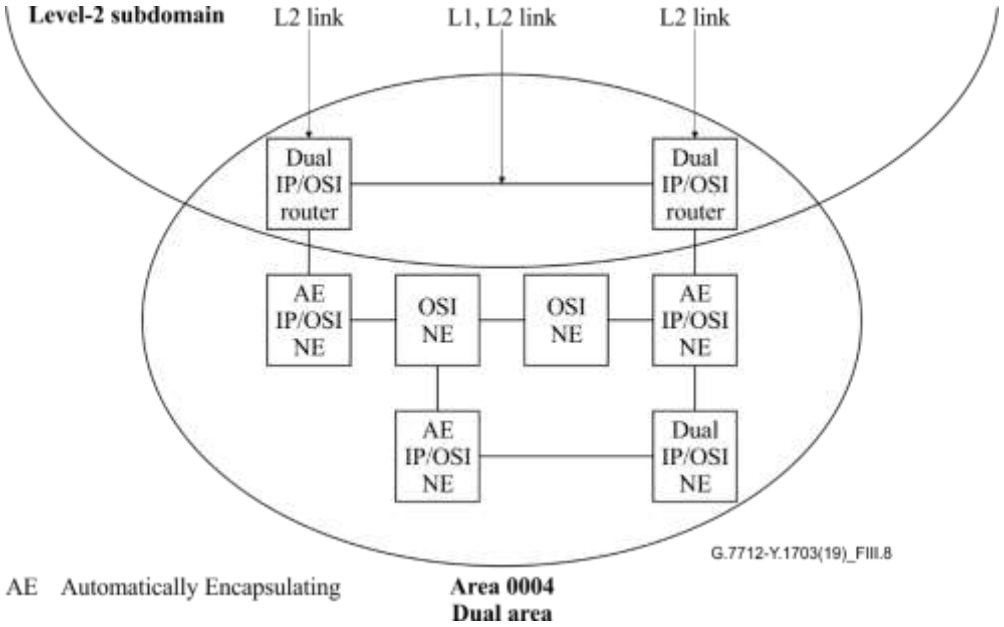


Figure III.8 – Dual gateway

III.3.2.2 OSI-only gateway NE

Occasionally, automatically encapsulating nodes will be used to upgrade an existing OSI-only area to make it effectively into a dual area. In this case, the gateway nodes may have to remain as OSI-only nodes. In such a case, a network can be built as shown in Figure III.9.

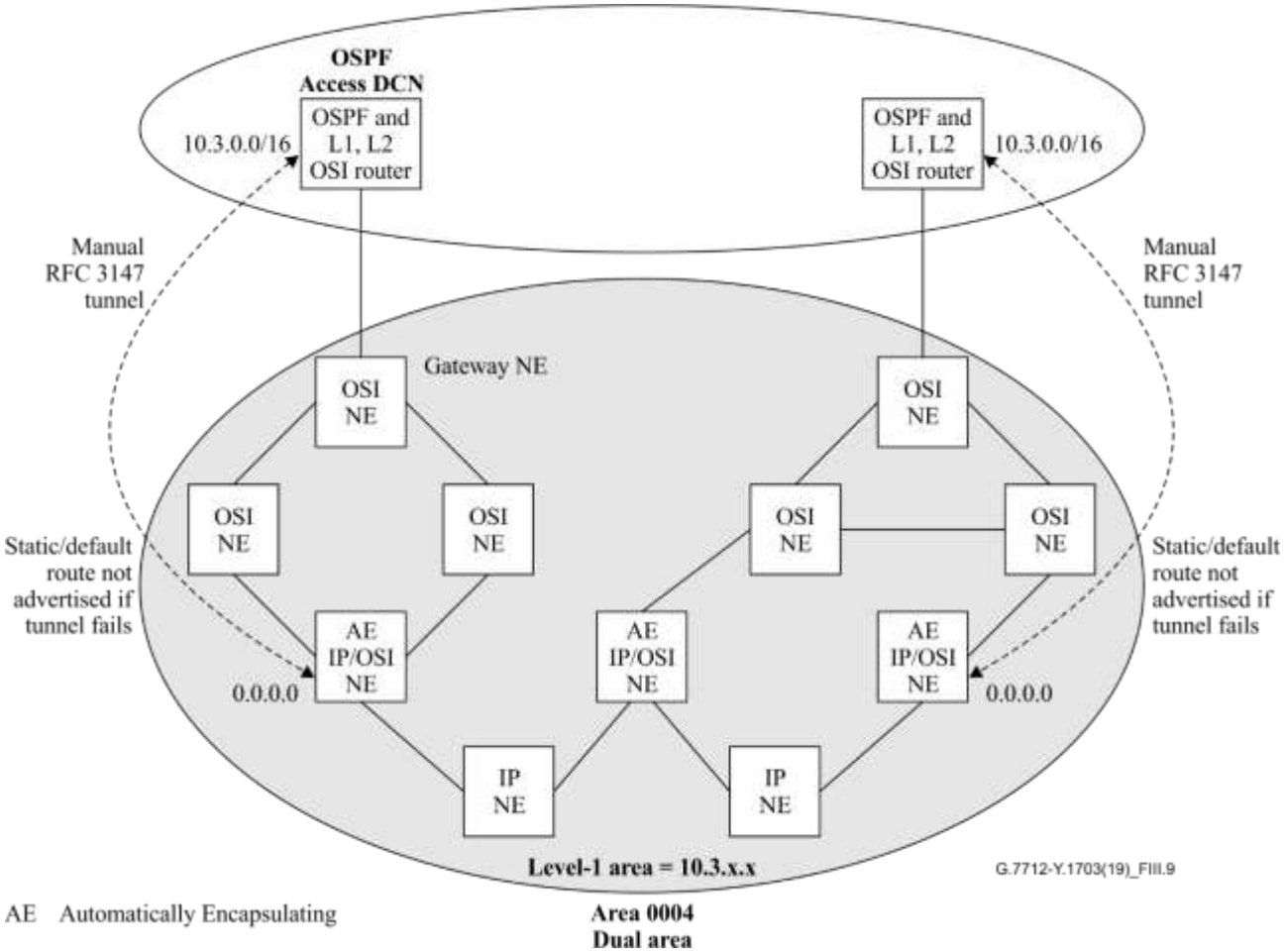


Figure III.9 – OSI-only gateway

In this network, the CLNP packets that need to leave the Level-1 area continue to go to the OSI Level-1, Level-2 router. The nodes that have a manual tunnel leading out of the Level-1 area advertise this as a default route. Consequently, the IP-capable nodes will all add an entry to the bottom of their routing table telling them to send all IPv4 packets to one of the nodes that has the manual tunnel, unless they have a more specific route. In this way, an IPv4 packet is never sent to a Level-1, Level-2 node, but is always sent across one of the manual tunnels.

The router in the access DCN that terminates the manual tunnel does not need to run integrated IS-IS. It may run any IP routing protocol that an operator wishes to use. In this way, an existing network that uses OSPF and Level-2 IS-IS in the access DCN, and Level-1 IS-IS in the SDH NEs, may have the Level-1 areas upgraded to dual areas with little impact on the existing OSI-only SDH NEs, or on the access DCN.

Appendix IV

Example illustration of packet 1+1 protection

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

IV.1 Packet 1+1 protection overview

Packet 1+1 path protection provides a packet level protection service similar in some respects to the conventional connection level 1+1 service, with several important distinctions. Packet level 1+1 allows selection of incoming packets from any connection, irrespective of the connection from which the last packet was selected. That is, packet 1+1 protection treats both connections as working connections, as opposed to designating one connection as working, and the other as the protection. In the latter, packets are selected from the working connection until a detection of failure on the working connection causes a switching to the protection connection. In contrast, packet 1+1 does not require explicit failure detection and protection switching. This allows the packet level 1+1 scheme to recover from any failure instantaneously and transparently. Similar to the connection level 1+1 protection, only edge nodes need to be service-aware, which makes interoperability easier.

To provide packet 1+1 protection service between two connection-oriented network edge nodes, a pair of connections is established along disjoint paths. Packets from an application flow subscribing to the service are dual-fed at the ingress node onto the two connections. Disjoint paths, in the simplest case, may be link or node disjoint but, in general, may involve more complicated notion such as shared risk groups. At the egress edge node, one of the two copies of the packets selected and forwarded from the two possible received copies, each traversing a disjoint path. Given this, any single failure in the network, other than the ingress or egress node itself, can affect at most one copy of each packet. This allows the service to withstand a single failure transparently. In terms of restoration time, this can be characterized as an instantaneous recovery from a failure since there is no need to detect, notify and switch to protection path explicitly. The scheme can be easily extended to protect against multiple failures by employing more than two disjoint paths.

IV.2 Packet 1+1 protection illustration

Figure IV.1 illustrates a realization of the service using sequence numbers as identifiers. After passing through the classifier, each packet that needs to be forwarded on the mated LSPs is assigned a distinct sequence number by the service-aware source edge node. This packet with the distinct identification is then duplicated and forwarded onto the two disjoint LSPs. The egress node shall only select one copy of the duplicated packet. For appropriately selecting the packet exactly once, the destination must be able to identify the duplicate packets and then select one, and handle all possible variations. This selection process at the packet level is non-trivial as the duplicate packets may not arrive at the same time (due to propagation delay and buffering) and also these packets may get lost (due to transmission errors and buffer overflows).

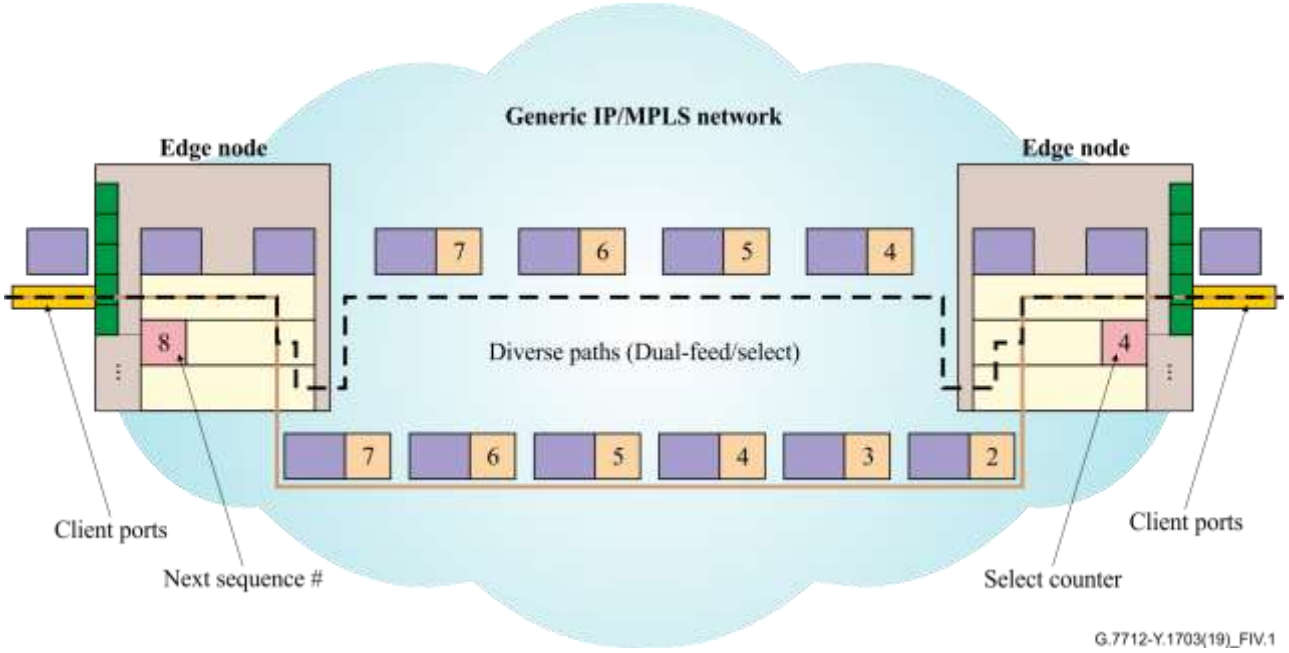


Figure IV.1 – 1+1 protection

The ingress node inserts the sequence number as defined in clause 7.1.19.2. The packet is then duplicated and transported over diverse LSPs. Due to the diversity of the LSPs, there will be a leading LSP and a trailing LSP. The leading LSP will deliver the packets to the egress node faster than the trailing LSP. Therefore, under non-failure conditions, the egress node will select the packets from the leading LSP. The packets received on the trailing LSP will be duplicate packets and will, therefore, be discarded.

The decision whether to accept or discard a received packet is based on the received packet's sequence number and a counter + sliding window at the egress node. The counter indicates the sequence number of the next packet it is expecting. The counter, plus sliding window, provides a window of acceptable sequence numbers. The sliding window is needed to properly accept and reject packets. If the received packet falls in the window, it is considered legitimate and can be accepted. Otherwise, it is rejected. The size of the window should be larger than the maximum number of consecutive packets a working (an alive) LSP can lose.

The sliding window is used to solve the problem of losing packets on the leading LSP when the leading LSP's sequence number is very close to the wrap around point. Figure IV.2 illustrates a leading LSP (LSP-1) that delivers a packet with sequence number 29. The packet is accepted and the counter is incremented to 30. If we assume that two consecutive packets are lost (i.e., packets with sequence numbers 30 and 31), the next received packet on LSP-1 will be 0. Without a sliding window, the egress node will reject the packet since $0 < 30$. By implementing a sliding window that is larger than the maximum number of consecutive packets a working (an alive) LSP can lose, this problem can be solved. For example, let us say that the maximum number of consecutive packets that a working LSP can lose is five, then a sliding window of six can be defined. Taking the same example as before, however, now using the sliding window, the egress node will accept packets in the range of {30, 31, 0, 1, 2, 3, 4}. Therefore, even if five packets are lost (i.e., the maximum number of consecutive packets that can be lost on a working LSP), the next packet received will have sequence number 3 and the packet will be accepted.

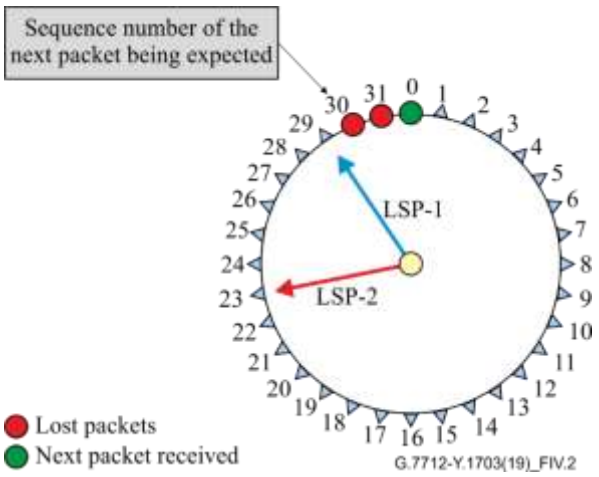


Figure IV.2 – Sliding window mechanism

Note that this idea of sliding window only works if the falling behind LSP cannot fall back in the sliding window range. If a packet with a sequence number in the range of the sliding window is received from the falling behind LSP, then it will be mistakenly accepted. A falling behind LSP can only receive a packet with a sequence number in the range of the sliding window if it falls back by more than (2^N – size of sliding window). Therefore, the number of bits "N" used for the sequence number must support the following equation:

$$2^N > \text{SlidingWindow} + \text{DelayWindow}$$

where:

SlidingWindow > maximum number of consecutive packets that can be lost on a LSP

and:

DelayWindow = maximum number of packets the trailing LSP can fall behind the leading LSP

Note that clause 7.1.19.2 defines a 4-byte field for carrying the sequence number. The 4-byte field provides a sequence of more than four-billion numbers which is large enough to accommodate worst-case consecutive packet losses and delay differentials.

One reasonable way of engineering the size of the sliding and delay windows is to make the size of the sliding window equal to the size of the delay window. (Note that it is assumed that the size of the delay window is generally larger than the size of the sliding window.) This guarantees selection of packets from the leading LSP in all scenarios after a failed LSP gets repaired. This point is further elaborated in the following clause which discusses various failure scenarios.

IV.3 Operation of selector algorithm under various failure scenarios

One way to view the operation of the selector algorithm is to picture a clock with 2^N intervals. Figure IV.3 illustrates an example where N = 4 (i.e., 4-bit sequence number) and, therefore, the sequence number ranges from 0 through 15.

In this example, the SlidingWindow is set equal to the DelayWindow, which is 5.

Figure IV.3 shows the leading LSP ahead of the trailing LSP by 3 sequence numbers. The leading LSP delivers a packet with sequence number = 1 and the counter is now set to 2.

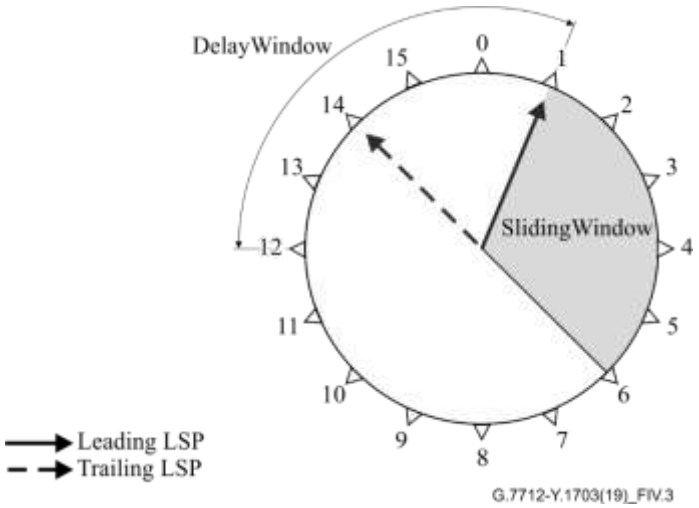


Figure IV.3 – Selector algorithm operation

Figure IV.4 shows that, prior to receiving a packet with a sequence number equal to 2 on the leading LSP, the leading LSP fails. Until the packet with sequence number equal to 2 is delivered from the trailing LSP, the egress node will not select any packets and the counter will remain equal to 2.

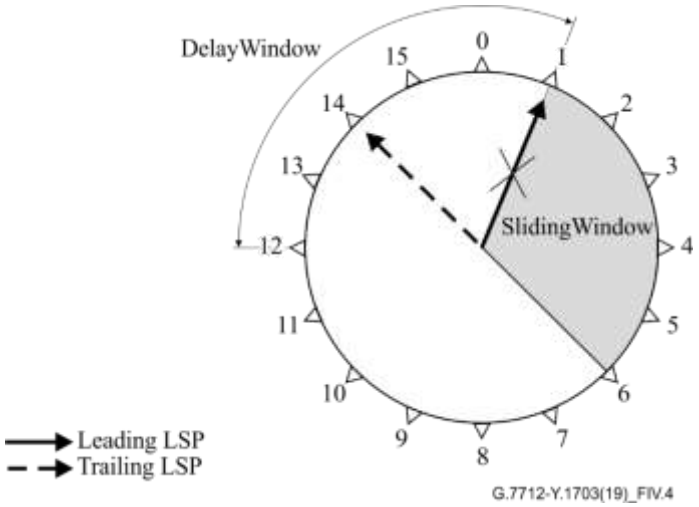


Figure IV.4 – Leading LSP failure

Figure IV.5 illustrates that, when the packet with a sequence number equal to 2 is received on the trailing LSP, the egress node increments the counter to 3 and the sliding window shifts so that a packet with a sequence number in the range of 3 through 7 can be accepted.

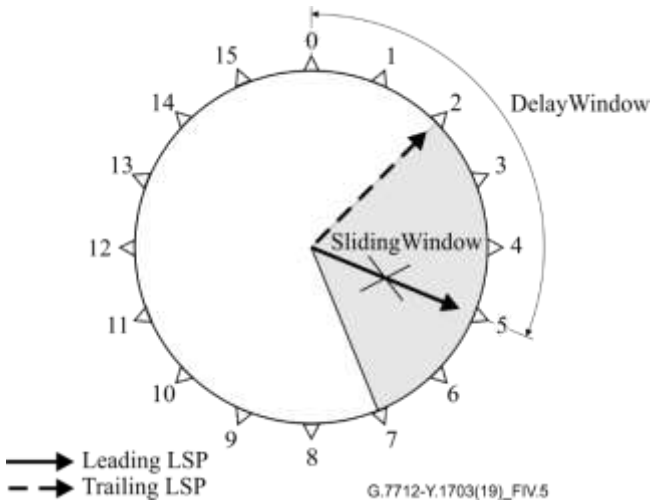


Figure IV.5 – Reception of packet 2 by trailing LSP

Figure IV.6 illustrates that, prior to receiving a packet with a sequence number equal to 3 from the trailing LSP, the leading LSP is repaired and a packet with a sequence number equal to 6 is received from the Leading LSP. Since 6 is within the sliding window range, the packet is accepted. Note that it is important that, so long as the leading LSP is working, packets are received from the leading LSP. Therefore, to ensure that, when the leading LSP is repaired, it delivers a packet with a sequence number value that is within the sliding window range, the SlidingWindow should be equal to or greater than the DelayWindow, which is the case for this example.

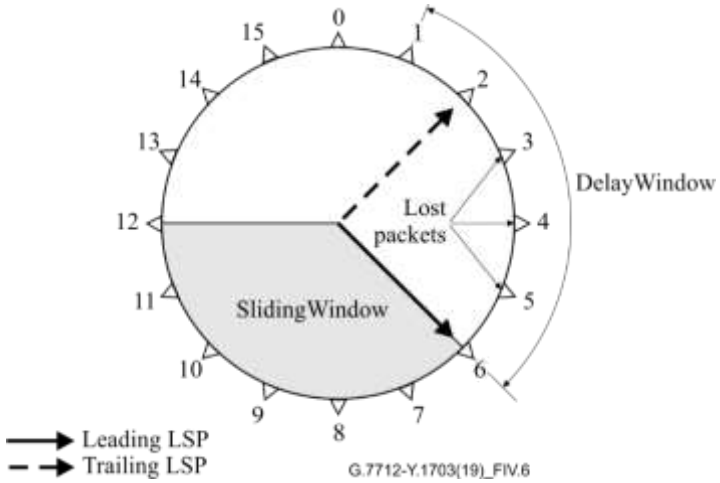


Figure IV.6 – Leading LSP repaired

Figures IV.7, IV.8 and IV.9 illustrate a problem if the SlidingWindow is set smaller than the DelayWindow. In this case, it is possible that, when the leading LSP is repaired, it delivers packets with sequence numbers that fall outside the SlidingWindow and, therefore, the egress node continues to accept packets from the trail LSP. If, at a later time, the trailing LSP fails, there is a potential to lose many packets (worst case would be 2^N – size_of_sliding_window, where N is the number of bits used for the sequence number).

Figure IV.7 shows an example where the SlidingWindow is set to 3, while the DelayWindow can be up to 7. In this example, the trailing LSP trails the leading LSP by 4 sequence numbers. Since the leading LSP has failed, the packets are selected from the trailing LSP.

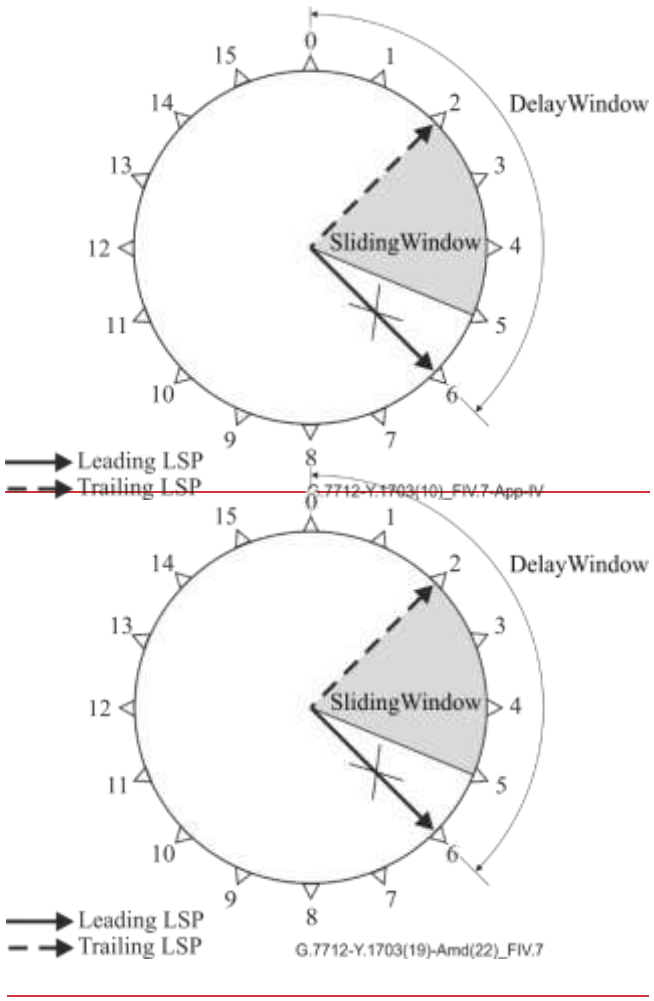


Figure IV.7 – Sliding window too small: packets selected from the trailing LSP

Figure IV.8 illustrates that, at the time when the leading LSP is repaired, it delivers a packet with a sequence number equal to 7 which is outside the SlidingWindow and, therefore, rejected. The packets continue to be selected from the trailing LSP.

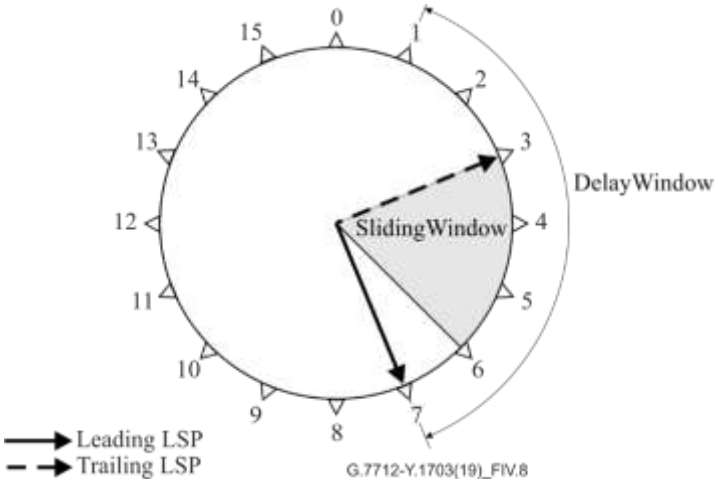


Figure IV.8 – Sliding window too small: rejection of packets delivered by the repaired leading LSP

Figure IV.9 illustrates a failure to the trailing LSP. Since the leading LSP delivers packets outside the SlidingWindow and, therefore, those packets are rejected, the egress node will not start accepting packets until the leading LSP comes all the way around and starts to deliver packets with a sequence number that falls within the SlidingWindow. This can result in a significant loss of packets. Therefore, to prevent such an occurrence, it is recommended that this type of selector algorithm set the SlidingWindow equal to the DelayWindow.

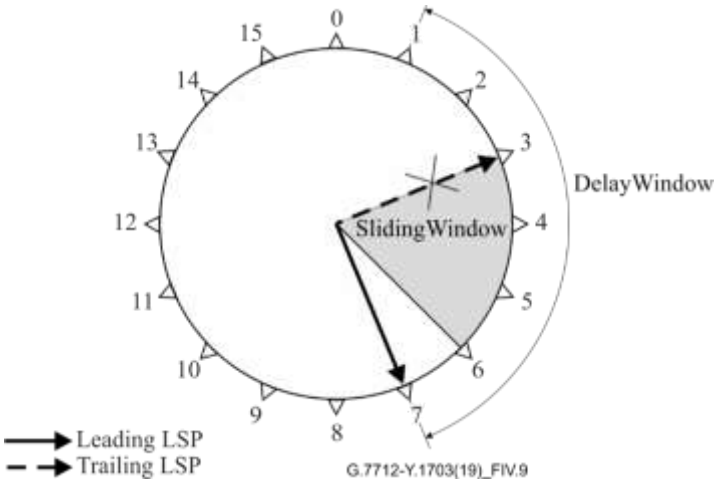


Figure IV.9 – Sliding window too small: effect of a failure for trailing LSP

Appendix V

Mapping version 4 and version 5 clause numbers

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

This appendix provides a mapping between clauses found in this version and those found in prior versions that have been changed due to restructuring.

Table V.1 – Mapping version 4 and version 5 clause numbers

Structure of clauses 6 and 7 in version 4	Corresponding structure in this version
6 DCN characteristics	6 DCN applications
6.1 TMN application 6.1.1 – 6.1.4	6.1 TMN application 6.1.1 – 6.1.4
6.2 Control plane application (ASON and MPLS-TP) 6.2.1 – 6.2.4	6.2 ASON[1] application 6.2.1 – 6.2.4
6.3 SDN application 6.3.1 – 6.3.4	6.3 SDN application 6.3.1 – 6.3.4
6.4 Other applications requiring communication networks 6.4.1 OTSiG|OCh non-association. overhead Comm. application	6.4 Other applications requiring communication networks 6.4.1 OTSiG|OCh non-association overhead Comm. application
6.5 Separation of various application	6.5 Separation of various application
7 DCN functional architecture and requirements	7 DCN functional architecture
7.1 Specification of data communication functions	8 Data communication function requirements
7.1.1 ECC access function	8.1 L1 Physical layer requirements
7.1.2 ECC data-link layer termination function	8.2 L2 Data Link layer requirements
7.1.2.1 SDH ECC data-link layer termination function	8.2.1 SDH ECC (DCC)
7.1.2.2 OTN ECC data-link layer termination function	8.2.2 OTN ECC (GCC)

[1] Possible future study: If there are lots of commonality between DCN for ASON application and DCN for SDN application, it might worth to consolidate the two applications. Furthermore, consolidate the TMN and Control plane applications into Management-Control-Continuum application.

Table V.1 – Mapping version 4 and version 5 clause numbers

Structure of clauses 6 and 7 in version 4	Corresponding structure in this version
	8.2.3 MPLS-TP ECC
7.1.2.3 MPLS-TP SCN; 7.1.2.5 MPLS-TP SCC	8.2.3.1 MPLS-TP SCN
7.1.2.4 MPLS-TP MCN; 7.1.2.6 MPLS-TP MCC	8.2.3.2 MPLS-TP MCN
	8.3 L3 Network layer requirements
7.1.3 "Network layer PDU into ECC data-link frame" encapsulation function	8.3.1 L3 into L2 encapsulation functions
7.1.3.1 "Network layer PDU into SDH ECC data-link frame" encapsulation function	8.3.1.1 L3 into SDH ECC data-link frame encapsulation function
7.1.3.2 "Network layer PDU into MPLS-TP SCC data-link frame" encapsulation function	8.3.1.2 L3 into MPLS-TP SCC data-link frame encapsulation function
7.1.3.3 "Network layer PDU into MPLS-TP MCC data-link frame" encapsulation function	8.3.1.3 L3 into MPLS-TP MCC data-link frame encapsulation function
7.1.3.4 "Network layer PDU into EoT MCC data-link frame" encapsulation function	8.3.1.4 L3 into EoT MCC data-link frame" encapsulation function
7.1.4 Ethernet LAN Physical termination function	*9.1 Ethernet LAN as L1&L2*
7.1.5 Network layer PDU into Ethernet frame	8.3.1.5 L3 into Ethernet frame encapsulation functions
7.1.6 Network layer PDU forwarding function	8.3.2 L3 forwarding function
7.1.7 Network layer PDU interworking function	8.3.3 L3 interworking function
7.1.8 Network layer PDU encapsulation function	8.3.4 L3 to L3 encapsulation function
7.1.9 Network layer PDU tunnelling function	8.3.5 L3 tunnelling function
7.1.10 Network layer routing function	8.3.6 L3 routing function
7.1.11 IP routing interworking function	8.3.7 L3 IP routing interworking function
7.1.12 "Applications to network layer" mapping function	8.3.8 Applications to L3 mapping function

Table V.1 – Mapping version 4 and version 5 clause numbers

Structure of clauses 6 and 7 in version 4	Corresponding structure in this version
	9 Specific DCN L3|L2|L1 Technology requirements
7.1.4 Ethernet LAN Physical termination function	9.1 Ethernet LAN as L1&L2
	9.2 Ethernet WAN as L1&L2
	9.3 Native MPLS as L3
7.1.13 "MPLS PDU into ECC data-link layer" encapsulation function	9.3.1 MPLS PDU into L2 encapsulation function
7.1.14 "MPLS PDU into Ethernet frame" encapsulation function	9.3.1.1 MPLS PDU into Ethernet frame encapsulation function
7.1.15 – 7.1.19 MPLS ….	9.3.2 – 9.3.6 ….
7.2 Provisioning requirements	*8.4.1 Provisioning requirements*
7.3 Security requirements	*8.4.2 Security requirements*
NOTE – *italicized* items are out of order or repeated.	

Bibliography

~~[b-IETF RFC 1702] IETF RFC 1702 (1994), *Generic Routing Encapsulation over IPv4 networks.*~~

[b-IETF RFC 2126] IETF RFC 2126 (1997), *ISO Transport Service on top of TCP (ITOT).*

[b-IETF RFC 2966] IETF RFC 2966 (2000), *Domain-wide Prefix Distribution with Two-Level IS-IS.*

[b-IETF RFC 3147] IETF RFC 3147 (2001), *Generic Routing Encapsulation of CLNS Networks*.

[b-IETF RFC 3373] IETF RFC 3373 (2002), *Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies*.

[b-IETF RFC 4204] IETF RFC 4204 (2005), *Link Management Protocol (LMP).*

~~[b-IETF RFC 5920] IETF RFC 5920 (2010), *Security Framework for MPLS and GMPLS Networks.*~~

[b-IETF RFC 5950] IETF RFC 5950 (2010), *Network Management Framework for MPLS-based Transport Networks*.

[b-ONF TR-529] Open Networking Foundation, Technical Recommendation 529 (2016), *Security Foundation Requirements for SDN Controllers*.
https://www.opennetworking.org/wp-content/uploads/2013/05/Security_Foundation_Requirements_for_SDN_Controllers.pdf

[b-ONF TR-530] Open Networking Foundation, Technical Recommendation 530 (2016), *Threat analysis for SDN architecture*.
https://www.opennetworking.org/wp-content/uploads/2014/10/Threat_Analysis_for_the_SDN_Architecture.pdf

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

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
Computing power networks	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.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022