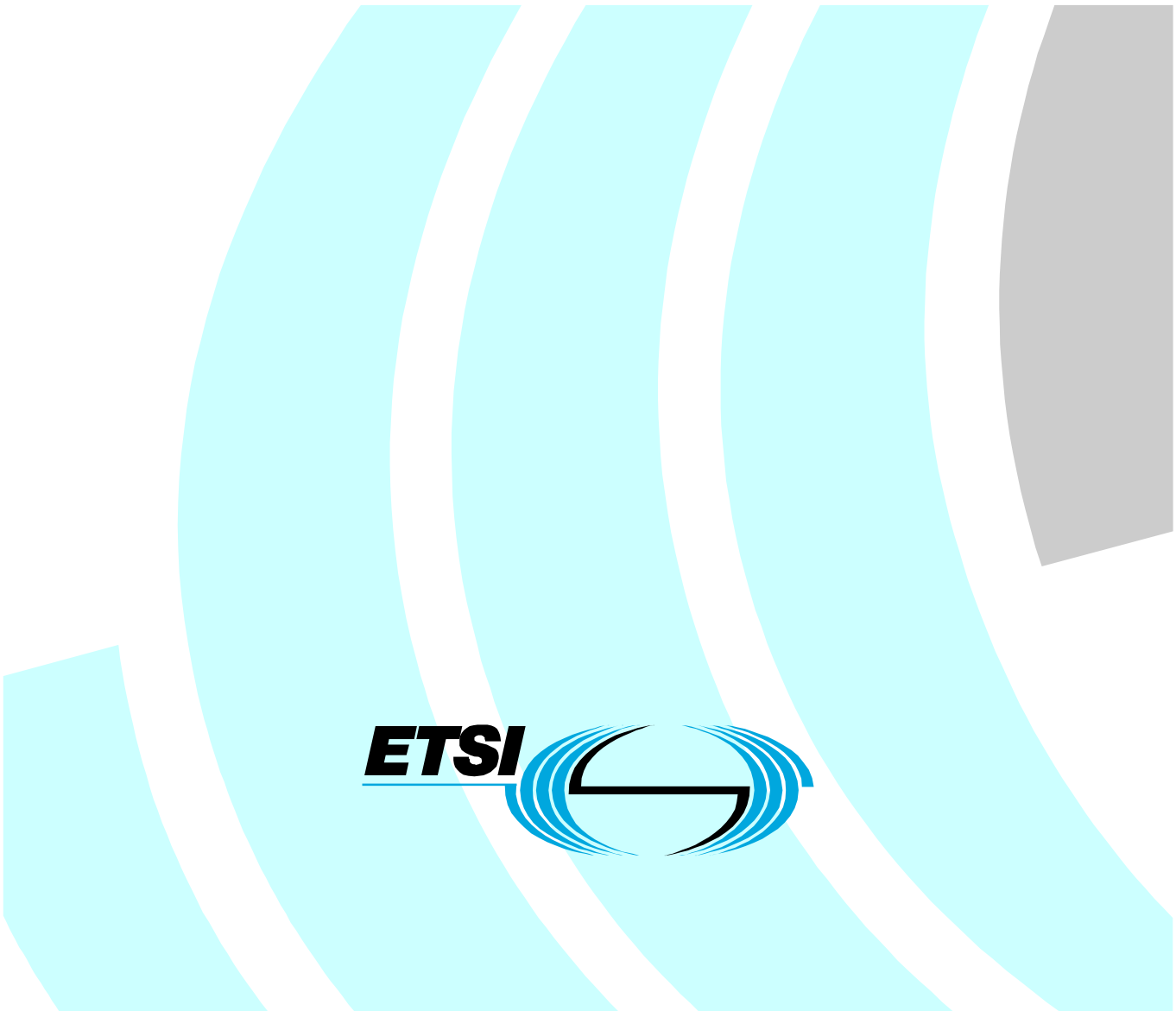
ETSI TR 102 198 V1.1.1 (2003-10)

Technical Report

Services and Protocols for Advanced Networks (SPAN); Preliminary analysis of migration to the Internet NGN



Reference
DTR/SPAN-130319

Keywords
IP, migration

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 6
Foreword 6
Introduction 6
1 Scope 7
2 References 7
3 Abbreviations 12
4 General considerations 13
4.1 QoS 14
4.1.1 Network performance 14
4.1.2 Unavailability 14
4.1.3 Security 14
4.2 Management 15
5 Harmonization between networks (TIPHON) 15
5.1 General 15
5.2 TIPHON abstract architecture and meta-protocol 16
6 Switched Circuit Networks (SCNs) 16
6.1 Access to networks 17
6.1.1 Analogue access 17
6.1.2 ISDN access 17
6.1.3 Mobile access 17
6.2 Architecture, Routeing and Signalling 18
6.2.1 Nodes 18
6.2.2 Signalling 19
6.3 Management and QoS of the signalling transport layer in SCN and ATM networks 19
6.3.1 Management 19
6.3.2 QoS of the transport layer 20
6.3.2.1 Availability 20
6.3.2.2 Performance 21
6.3.2.3 Security 21
7 IP networks 22
7.1 Subscriber Access Technologies 22
7.1.1 Analogue Modem 22
7.1.2 ISDN 22
7.1.3 xDSL 22
7.1.3.1 ADSL 22
7.2 Nodes, signalling and routeing 23
7.2.1 Network architecture 23
7.2.2 Signalling Transport 24
7.2.2.1 Network layer protocol IPv6 and ICMPv6 24
7.2.2.1.1 IPv6 addressing 25
7.2.2.1.2 Neighbour Discovery 25
7.2.2.1.3 Routeing of packets 25
7.2.2.2 MPLS 26
7.2.2.3 SCTP 26
7.2.2.4 TCP 26
7.2.2.4.1 Operation 27
7.2.2.5 RSVP 28
7.2.2.6 Differentiated services (Diffserv) 28
7.2.3 Call and bearer control 28
7.2.3.1 Session Initiation Protocol (SIP) 28
7.2.3.2 H.323 29

7.2.3.3 H.248 & Megaco 29
7.2.3.4 BICC Bearer Independent Call Control 29
7.3 Management, QoS of the signalling transport in the network 29
7.3.1 Management 29
7.3.2 QoS and security 30

8 Interconnection between networks 30
8.1 Edge nodes, interworking and using legacy applications 30
8.1.1 Edge nodes 30
8.1.2 Interworking between the SCN and the IP network 32
8.1.3 Using SS7 applications in or through a Managed IP network 33
8.1.3.1 Protocols 33
8.1.4 All IP path 34
8.2 Joint management of the networks and QoS for the signalling transport layers 34
8.2.1 Management 34
8.2.2 QoS 34
8.2.2.1 Availability and reliability 35
8.2.2.2 Performance 35
8.2.2.3 Security 35

9 Addressing and naming issues 36

10 Transition to IPv6 in Managed IP networks 36

11 Standardization in the IETF 36

12 Identification of the standards areas concerned and the gaps 37
12.1 Signallings, interworkings and other items 37
12.2 IPv6 and IPv4 interconnection issues 37
12.3 Management 37
12.4 Possible areas of further investigation in addition to the above 38

Annex A: Security generalities 39

Annex B: SCN details 41

B.1 Routeing in switched circuit networks 41

B.2 Signalling protocol stacks in a Time Division Multiplex SCN 41
B.3 ATM packet network instead of TDM 42

B.4 Management and QoS of the signalling transport layer in SCN and ATM networks 44
B.4.1 Management 44
B.4.1.2 OMAP management categories 44
B.4.1.2.1 Fault management for OMAP 44
B.4.1.2.2 Configuration management 44
B.4.1.2.3 Performance management 44
B.4.2 QoS and congestion 48
B.4.2.1 Congestion 48
B.4.2.2 QoS 48

Annex C: IP network details 51

C.1 Design 51

C.2 IPv6 details 51
C.2.1 Neighbour discovery 51
C.2.2 Routeing of packets 52
C.2.2.1 IPv6 headers and extension headers 52

C.3 SCTP details 54
C.3.1 Architectural View of SCTP 54
C.3.2 Functional view of SCTP 54
C.3.3 Association startup and takedown 54
C.3.4 Sequenced delivery within streams 55
C.3.5 User data fragmentation 55

C.3.6 Acknowledgement and congestion avoidance 55
C.3.7 Chunk bundling 55
C.3.8 Packet validation 55
C.3.9 Path management 56

C.4 TCP details 56
C.4.1 Communication using TCP 56
C.4.2 Connection establishment and clearing 56
C.4.3 Data communication 57
C.4.4 Precedence and security 58

C.5 Routeing in IP networks 58
C.5.1 Routeing in the public Internet 58
C.5.2 Managed IP networks 58

C.6 The Internet 58
C.6.1 Firewalls and NATS 58
C.6.1.1 Firewalls 58
C.6.1.2 NATS 59

ANNEX D: Using SS7 applications in or through a Managed IP network 60

D.1 General 60

D.2 Architecture for SIGTRAN protocols 60

D.3 Models for SIGTRAN 62
D.3.1 M3UA models 63
D.3.1.1 MTP/M3UA users homed on SG 63
D.3.1.1.1 MTP management 63
D.3.1.1.2 Message routeing 64
D.3.1.2 MTP/M3UA Users at AS/ASPs with own point codes 64
D.3.1.2.1 MTP network management 64
D.3.1.2.2 Message routeing 65
D.3.2 SUA Models 65
D.3.2.1 SCCP/SUA Users homed on SG 65
D.3.2.1.1 SCCP management 65
D.3.2.1.2 Message routeing 66
D.3.2.2 SCCP/SUA Users at AS/ASPs with own addresses 66
D.3.2.2.1 SCCP management 66
D.3.2.2.2 Message routeing 67

Annex E (informative): Bibliography 68

History 73

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

Introduction

COM(2002) 96 [1] is a policy document which the STF examined in the context of ETSI. The Commission proposed a set of actions in COM(2002) 96 [1] to ensure that the EU maintains the initiative and leadership in the upgrading of the capabilities of the Internet, providing for an efficient transition to the Next Generation Internet based on IPv6.

The present document gives a brief overview of the properties of existing SCNs, gives a brief description of managed IP networks and the public Internet, and examines methods to interconnect them using NGN nodes and SIGTRAN signalling protocols carrying call and bearer control information.

The issues pertinent to ETSI are listed, the outstanding one is the large number of protocols involved. The introduction of the large number of protocols could delay the migration to IP telephony. The present document identifies some possible protocol choices.

1 Scope

The present document is an analysis of technical requirements for the support and deployment of Telecommunication Services in Europe using IPv6, to progress toward the enhancement of signalling transport protocol standards.

The aims are to evaluate the requirements for standardization, existing standards, and to identify standardization gaps with respect to recommendations made by the Communication "Next Generation Internet priorities for action in migrating to the new Internet Protocol Ipv6" [COM(2002) 96 final] (reference [COM 96]).

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] COM(2002) 96 final: "Next Generation Internet - priorities for action in migrating to the new Internet protocol IPv6", Brussels 21.2.2002.

[2] ITU-T Recommendation E.721: "Network grade of service parameters and target values for circuit-switched services in the evolving ISDN".

[3] ITU-T Recommendation E.723: "Grade-of-service parameters for Signalling System No.7 networks".

[4] ITU-T Recommendation E.733: "Methods for dimensioning resources in Signalling System No.7 networks".

[5] ETSI EN 301 007-1: "Integrated Services Digital Network (ISDN); Signalling System No.7; Operations, Maintenance and Administration Part (OMAP); Part 1: Protocol specification".

[6] ETSI EN 301 007-2: "Integrated Services Digital Network (ISDN); Signalling System No.7; Operations, Maintenance and Administration Part (OMAP); Part 2: Protocol Implementation Conformance Statment (PICS) proforma specification".

[7] ETSI EN 301 848: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); Bearer Independent Call Control (BICC); Signalling procedures in an ATM/IP/.. backbone network; Capability Set 1 (CS1); Part 1: Protocol specification [ITU-T Recommendations Q.1901 and Q.765.5, modified]".

[8] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".

[9] ETSI TS 101 315: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Functional entities, information flow and reference point definitions; Guidelines for application of TIPHON functional architecture to inter-domain services".

[10] ETSI TS 101 882: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 1: Meta-protocol design rules, development method, and mapping guideline".

[11] ETSI TS 101 885: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Technology Mapping of TIPHON reference point N to H.248/MEGACO protocol".

[12] ETSI TS 101 883: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using H.323".

[13] ETSI TS 101 909-12: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 12: Internet Signalling Transport Protocol (ISTP)".

[14] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[15] ETSI TS 101 884: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Technology Mapping; Implementation of TIPHON architecture using SIP".

[16] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3 (3GPP TS 24.229 version 5.3.0 Release 5)".

[17] ETSI TR 101 308: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; SIP and H.323 Interworking".

[18] ETSI TR 101 771: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent requirements definition; Threat Analysis".

[19] ITU-T Recommendation G.1000: "Communications quality of service: A framework and definitions".

[20] GTS GSM 01.02: "Digital cellular telecommunications system (Phase 2+) (GSM); General description of a GSM Public Land Mobile Network (PLMN) (GSM 01.02)".

[21] GTS 03.02: "Digital cellular telecommunications system (Phase 2+) (GSM); Network architecture (GSM 03.02)".

[22] GTS GSM 03.04: "Digital cellular telecommunications system; Signalling requirements relating to routeing of calls to mobile subscribers (GSM 03.04)".

[23] GTS GSM 08.06: "Digital cellular telecommunications system (Phase 2+) (GSM); Signalling transport mechanism specification for the Base Station System - Mobile-services Switching Centre (BSS - MSC) interface".

[24] GTS 09.02: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Application Part (MAP) specification (GSM 09.02)".

[25] GTS GSM 09.03: "Digital cellular telecommunications system; Signalling requirements on interworking between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN) (GSM 09.03)".

[26] GTS GSM 09.08: "Digital cellular telecommunications system (Phase 2+) (GSM); Application of the Base Station System Application Part (BSSAP) on the E-interface (GSM 09.08)".

[27] GTS 11.31: "European digital cellular telecommunications system (Phase 1); Home Location Register Specification (GSM 11.31)".

[28] GTS 11.32: "European digital cellular telecommunications system (Phase 1); Visitor Location Register Specification (GSM 11.32)".

[29] L.Kleinrock, Wiley Interscience: "Queueing Systems", Volume 1, 1975.

[30] ITU-T Recommendation M.3100: "Generic network information model".

[31] ITU-T Recommendation M.3010: "Principles for a Telecommunications management network".

[32] ITU-T Recommendation Q.1901: "Bearer Independent Call Control protocol".

[33] ITU-T Recommendation Q.2150.0: "Generic signalling transport service".

[34] ITU-T Recommendation Q.701: "Functional description of the message transfer part (MTP) of Signalling System No. 7".

[35] ITU-T Recommendation Q.702: "Signalling data link".

[36] ITU-T Recommendation Q.703: "Signalling link".

[37] ITU-T Recommendation Q.704: "Signalling network functions and messages".

[38] ITU-T Recommendation COM 11-R 6 January 2001: "Implementors' Guide (12/2000) for Recommendation Q.704 (07/96)".

[39] ITU-T Recommendation Q.2210: "Message transfer part level 3 functions and messages using the services of ITU-T Recommendation Q.2140".

[40] ITU-T Recommendation Q.705: "Signalling network structure".

[41] ITU-T Recommendation Q.706: "Message Transfer Part signalling performance".

[42] ITU-T Recommendation COM 11-R 205-E: "Implementors' Guide (12/99) for Recommendation Q.706 (03/93)".

[43] ITU-T Recommendation Q.707: "Testing and maintenance".

[44] ITU-T Recommendation Q.708: "Assignment procedures for international signalling point codes".

[45] ITU-T Recommendation Q.709: "Hypothetical Signalling Reference Connection".

[46] ITU-T Recommendation Q.711: "Functional description of the signalling connection control part".

[47] ITU-T Recommendation Q.712: "Definition and function of signalling connection control part messages".

[48] ITU-T Recommendation Q.713: "Signalling connection control part formats and codes".

[49] ITU-T Recommendation Q.714: "Signalling connection control part procedures".

[50] ITU-T Recommendation Q.715: "Signalling connection control part user guide".

[51] ITU-T Recommendation Q.716: "Signalling System No.7 - Signalling connection control part (SCCP) performance".

[52] ITU-T Recommendation Q.750: "Overview of Signalling System No. 7 management".

[53] ITU-T Recommendation Q.751.1: "Network element management information model for the Message Transfer Part (MTP)".

[54] ITU-T Recommendation Q.751.2: " Network element management information model for the Signalling Connection Control Part".

[55] ITU-T Recommendation Q.752: "Monitoring and measurements for Signalling System No. 7 networks".

[56] ITU-T Recommendation Q.753: " Signalling System No. 7 management functions MRVT, SRVT and CVT and definition of the OMASE-user".

[57] ITU-T Recommendation Q.754: " Signalling System No. 7 management Application Service Element (ASE) definitions.

[58] ITU-T Recommendation Q.761: " Signalling System No. 7 - ISDN User Part functional description.

[59] ITU-T Recommendation Q.762: " Signalling System No. 7 - ISDN User Part general functions of messages and signals.

[60] ITU-T Recommendation Q.763: " Signalling System No. 7 - ISDN User Part formats and codes".

[61] ITU-T Recommendation Q.764: "Signalling System No. 7 - ISDN User Part signalling procedures".

[62] ITU-T Recommendation Q.766: "Performance objectives in the integrated services digital network application".

[63] ITU-T Recommendation Q.771: "Functional description of transaction capabilities".

[64] ITU-T Recommendation Q.772: "Transaction capabilities information element definitions".

[65] ITU-T Recommendation Q.773: "Transaction capabilities formats and encoding".

[66] ITU-T Recommendation Q.774: "Transaction capabilities procedures".

[67] ITU-T Recommendation Q.775: "Guidelines for using transaction capabilities".

[68] ITU-T Recommendation Q.921: "ISDN user-network interface - Data link layer specification".

[69] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".

[70] Q.Sup.41: "ITU-T Technical Report TRQ.2003: Roadmap to the BICC protocol Recommendations, BICC interworking Recommendations, and BICC requirement supplements".

[71] ITU-T Recommendation X.700: "Management framework for Open Systems Interconnection (OSI) for CCITT applications".

[72] ITU-T Recommendation X.701: "Information technology - Open Systems Interconnection - Systems management overview".

[73] ITU-T Recommendation X.731: "Information technology - Open Systems Interconnection - Systems management: State management function".

[74] ETSI TS 102 141: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN (Transport of SS7 over IP); Message transfer part 2 User Adaptation layer (M2UA) [Endorsement of RFC 3331 (2002), modified]".

[75] ETSI TS 102 142: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN (Message of SS7 over IP); Message transfer part 3 User Adaptation layer (M3UA) [Endorsement of RFC 3332 (2002), modified]".

[76] ETSI TS 102 144: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN (Transport of SS7 over IP); Stream Control Transmission Protocol (SCTP) [Endorsement of RFC 2960 and RFC 3309, modified]".

[77] IETF RFC 2960: "Stream Control Transmission Protocol", R. Stewart., Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson.

[78] IETF RFC 3309: "Stream Control Transmission Protocol (SCTP) Checksum Change", J. Stone, R. Stewart, D. Otis.

[79] IETF RFC 3436: "Transport Layer Security over Stream Control Transmission Protocol", A. Jungmaier, E. Rescorla, M. Tüxen.

[80] IETF RFC 3257: "Stream Control Transmission Protocol Applicability Statement", by L.Coene, April 2002.

[81] ETSI TS 102 143: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN (Transport of SS7 over IP); Signalling connection control part User Adaptation layer (SUA) [Endorsement of SIGTRAN-SUA-14 (December 2002), modified]".

[82] IETF RFC 2638: "A Two-bit Differentiated Services Architecture for the Internet", by K. Nichols, V. Jacobson and L. Zhang, July 1999.

[83] IETF RFC 2474 (Obsoletes: 1455, 1349): "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", by K. Nichols, S. Blake, F. Baker and D. Black, December 1998.

[84] IETF RFC 2475 (Informational): "An Architecture for Differentiated Service", by S. Blake, D. Black, M. Carlson, E. Davies and Z. Wang, W. Weiss, December 1998.

[85] IETF RFC 2373 (Obsoletes 1884): "IP Version 6 Addressing Architecture", by R. Hinden and S. Deering, July 1998.

[86] IETF RFC 2460 (Obsoletes 1883): "Internet Protocol, Version 6 (IPv6) Specification", by S. Deering and R. Hinden, December 1998.

[87] IETF RFC 2461 (Obsoletes 1970): "Neighbor Discovery for IP Version 6 (IPv6)", by T. Narten, E. Nordmark and W. Simpson, December 1998.

[88] IETF RFC 2463 (Obsoletes 1885): "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", by A. Conta and S. Deering, December 1998.

[89] IETF RFC 3031: "Multiprotocol Label Switching Architecture", by E. Rosen, A. Viswanathan and R. Callon, January 2001.

[90] IETF RFC 3270, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", by F. Le Faucheur (Editor), L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval and J. Heinanen, May 2002.

[91] IETF RFC 2205: "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification", by R. Braden (Ed.), L. Zhang, S. Berson, S. Herzog and S. Jamin, September 1997.

[92] IETF RFC 2207: "RSVP Extensions for IPSEC Data Flows", by L. Berger and T. O'Malley, September 1997.

[93] IETF RFC 2368: "The mailto URL scheme".

[94] IETF RFC 2750 (Updates 2205): "RSVP Extensions for Policy Control", by S. Herzog, January 2000.

[95] IETF RFC 2246: "The TLS Protocol Version 1.0", by T. Dierks and C. Allen, January 1999.

[96] IETF RFC 2401 (Obsoletes 1825): "Security Architecture for the Internet Protocol", by S. Kent and R. Atkinson, November 1998.

[97] IETF RFC 2404: "The Use of HMAC-SHA-1-96 within ESP and AH", by C. Madson and R. Glenn, November 1998.

[98] IETF RFC 2406 (Obsoletes 1827): "IP Encapsulating Security Payload (ESP)", by S. Kent and R. Atkinson, November 1998.

[99] IETF RFC 2407: "The Internet IP Security Domain of Interpretation for ISAKMP", by D. Piper, November 1998.

[100] IETF RFC 2409: "The Internet Key Exchange (IKE)", by D. Harkins and D. Carrel, November 1998.

[101] FIPS PUB 46-3: "DATA ENCRYPTION STANDARD (DES)", from the Federal Information Processing Standards, 1999 October 25.

[102] FIPS PUB 180-2: "Secure Hash Signature Standard (SHS) (FIPS PUB 180-2)", from the Federal Information Processing Standards, 2002 August 1. To be found at: http://csrc.nist.gov/publications/.

[103] IETF RFC 3057: "ISDN Q.921-User Adaptation Layer", by K.Morneault, S.Rengasami, M.Kalla and G.Sidebottom, February 2001.

[104] IETF RFC 3261 (Obsoletes 2543): "SIP: Session Initiation Protocol", by J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, June 2002.

[105] IETF RFC 3410: "Introduction and Applicability Statements for Internet Standard Management Framework", by J.Case, R.Mundy, D.Partain and B.Stewart, December 2002. Also its references (RFCs 3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418, 2578, 2579, 2580).

[106] IETF RFC 793: "Transmission Control Protocol", by J Postel (Editor), September 1981.

[107] ETSI TR 101 303: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Requirements definition study; Introduction to service and network management".

[108] ETSI ES 202 915-1: "Open Service Access (OSA); Application Programming Interface (API); Part 1: Overview".

[109] ETSI TS 129 202: "Universal Mobile Telecommunications System (UMTS); SS7 signalling transport in Core Network; Stage 3 (3GPP TS 29.202 Release 4)".

[110] ITU-T Recommendation Y.1541: "Revised Appendix VI: Applicability of the Y.1221 transfer capabilities and IETF Differentiated Services to IP QoS classes".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ADSL	Asymmetric Digital Subscriber Line
AE	Application Entity
AMF	Address Mapping Function
AMI	Application Management Interface
AS	Application Server
ASE	Application Service Element
ASP	Application Server Process
ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
BSS	Base Station System
BSSAP	Base Station System Application Part
CBC	Cipher Block Chaining
CIC	Circuit Identification Code
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DPC	Destination Point Code
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GT	Global Title
GTT	Global Title Translation
HLR	Home Location Register
IETF	Internet Engineering Task Force
IN	Intelligent Network
INAP	Intelligent Network Application Part
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LAN	Local Area Network
LME	Level Management Entity
LMI	Level Management Interface
M2PA	MTP level 2 Peer-to-Peer Adaptation Layer
M2UA	MTP level 2 User Adaptation Layer
M3UA	MTP level 3 User Adaptation Layer
MAP	Mobile Application Part
MGC	Media Gateway Controller
MGW	Media GateWay
MIB	Management Information Base
MIS	Management Information Service
MPLS	Multi Protocol Label Switching
MSC	Mobile-services Switching Centre
MSU	Message Signal Unit
MT	MTP Tester
MTP	Message Transfer Part
NAT	Network Address Translator
NGN	Next Generation Network
OMAP	Operations, Management and Administration Part
OMASE	OMAP ASE

OPC	Origin PC
OSF	Operations Systems Function
OSI	Open Systems Interconnection
PC	Point Code
PLMN	Public Land Mobile Network
QoS	Quality of Service
RFC	Request For Comments
RSA	Rivest Shamir Adleman (public key asymmetric cryptosystem)
RTP	Real Time Protocol
SCCP	Signalling Connection Control Part
SCN	Switched Circuit Network
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SEP	Signalling End Point
SG	Signalling Gateway
SI	Service Indicator
SIGTRAN	Signalling Transport (group of the IETF)
SIO	SI Octet
SIP	Session Initiation Protocol
SLS	Signalling Link Selection (field)
SMSI	System Management Service Interface
SNMP	Simple Network Management Protocol
SRP	SCCP Relay Point
SS7	Signalling System No.7
SSN	Subsystem Number
ST	SCCP Tester
STP	Signalling Transfer Point
SU	Signal Unit
SUA	SCCP User Adaptation Layer
TC	Transaction Capabilities
TC	Transaction Capabilities
TCP	Transmission Control Protocol
TF	Transformation Function
TIPHON	Telecommunication and Internet Protocol Harmonization over Networks
TMN	Telecommunications Management Network
TSP	Telcommunication Service Provider
TT	TC Test responder
TUP	Telephony User Part
UDP	User Datagram Protocol
VLR	Visitor Location Register
VoIP	Voice over IP
VPI/VCI	Virtual Path/Virtual Channel Combination

4 General considerations

Telecommunications Service Providers (TSPs) have realized in the past few years that the cost of providing new services and expansion of capacity might be reduced by the use of packet switching rather than their traditional circuit switching technologies.

The exponential growth in popularity of the Internet causes TSPs (who provide access to the Internet via their own networks) to believe that new capacity should be provided using IP technology for packet switching.

In parallel with the growth in Internet access, there has been enormous growth within Europe and Asia of wireless networks, using e.g. GSM, to provide mobile communication services.

Both the legacy fixed and mobile networks use circuit switching, although the General Packet Radio Service (GPRS) extension of GSM uses packet switching.

In order for telecommunications service subscribers to accept changes, the evolution from switched circuit networks (SCNs) to managed IP networks via Next Generation Networks (NGNs) should be as seamless as possible, and in particular the Quality of Service (QoS) subscribers observe at present should be retained, or improved, during the evolution.

The cost of the transition can be minimized only if the cost of its management and the cost of NGN management can be minimized. Legacy networks, and their management systems, are liable to persist for some years. If NGN management can be integrated into existing management systems, the cost of retraining staff and the cost of extension of the systems will be reduced.

The present document is concerned with analysing the requirements of signalling transport in the evolution towards NGNs. To do this, it considers the signalling transport characteristics of the SCN, the many and varied protocols in the Internet and managed IP network for signalling, and possible ways of providing for signalling transport requirements in the NGN.

It also identifies areas where clarification and extension of standards are required.

4.1 QoS

Quality of Service is a phrase that has many different interpretations. The present document uses ITU-T Recommendation G.1000 [19] as a basis, and for signalling transport within networks considers just its network performance (listed as speed and accuracy in figure 1/G.1000 [19]), availability, reliability and security aspects. See also DTR/STQ-00037 (bibliography).

4.1.1 Network performance

The performance standards for the Next Generation Networks should be at least as good as those of the SCN. The objectives for SS7 signalling transport layers at a node are in ITU-T Recommendations Q.706 [41] for the MTP and Q.716 [51] for the SCCP. The Implementors' Guide (1999) for Q.706 (03/93) (see ITU-T Recommendation Q.706 IG [42]) gives further information on message delay in SS7 MTP, dependent on message length, link loading, bit error rate and signalling loop delay.

ITU-T Recommendation Y.1541 [110] gives performance objectives for IP-based services, table 1/Y.1541 [110] gives provisional values for IP packet transfer delay, packet delay variation, packet loss ratio and packet error ratio for its six QoS class definitions. Table 2/Y.1541 [110] gives guidance into which classes example applications should be placed.

In order to compare SCN performance with IP-based networks, it might be helpful to estimate using ITU-T Recommendations Q.706 [41] and Q.716 [51] for typical SS7 network architectures the equivalent statistics for a "signalling transport" QoS class to those given in ITU-T Recommendation Y.1541 [110].

Various techniques to achieve the "signalling transport" QoS for each type of signalling transport (e.g. M3UA from SG to MGC) need to be investigated by ETSI, and guidance given.

4.1.2 Unavailability

According to ITU-T Recommendation Q.706 [41], the unavailability of signalling between an origin and a destination should be no more than 10 min. per year (i.e. probability of unavailability better than $1{,}9 \times 10^{-5}$).

Preferred architectures need to be defined in ETSI to achieve similar figures for NGNs. A Work Item has been agreed to examine the architecture of networks using the SIGTRAN protocols, this WI should also consider availability and reliability characteristics.

4.1.3 Security

The definitions commonly used for security concepts are:

- **confidentiality:** the avoidance of the disclosure of information without the permission of its owner.
- **integrity:** the property that data has not been altered or destroyed in an unauthorized manner.

- **accountability:** the principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation.
- **availability:** the property of being accessible and usable upon demand by an authorized entity.
- **non-repudiation:** a property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.

Of these, the ones applicable to signalling transport are confidentiality, integrity and availability.

Threats to security can be characterized as:

- Denial of service.
- Eavesdropping.
- Masquerade.
- Unauthorized access.
- Loss of information.
- Corruption of information.
- Repudiation.

The Switched Circuit Network is usually physically secure from break-in, masquerade attacks etc. Denial of service is also not a known problem. Confidentially of data is usually not a problem (encryption is enabled across radio link from handset to base station for mobile calls. There is the possibility of encryption on signalling links if required.)

New networks are vulnerable because of their physical characteristics, and because they might well connect to the Internet to provide some services. Their arrangements should be such as to provide at least as good security as that of SCNs.

4.2 Management

Management of the SCN has been defined using TMN concepts (see ITU-T Recommendation M.3010 [31], also ITU-T Recommendation M.3100 [30]), which refers to OSI management (see ITU-T Recommendation X.700 [71]). Signalling transport within SS7 networks uses OMAP (see ITU-T Recommendations X.700 [71] and Q.751.1 [53], Q.751.2 [54] and Q.752 [55]). IP networks use SNMP (see RFC 3410 [105] and its references). Only the latest version 3 of SNMP defines security and administration. As yet, for carrying SS7 over IP, only drafts exist for the management information bases (MIBs) for SCTP and for M3UA. M2UA, M2PA and SUA have no defined MIBs.

If costs are to be kept down, some integration of management between SCN and IP networks is desirable, particularly for nodes such as an SG and MGCs (ASs) that have an appearance in both networks. This implies that harmonization of management systems is needed between the SCN and IP networks, and that managed entities visible in both networks should have a common definition. The possibility of defining a TMN transformation function (TF, see ITU-T Recommendation M.3010 [31]) for the management entities defined using SNMP in the IP network should be examined.

5 Harmonization between networks (TIPHON)

5.1 General

Tiphon was set up to harmonize existing (SCN) and managed IP networks, including providing interworking definitions for services which are supported currently (and in the future) by networks.

5.2 TIPHON abstract architecture and meta-protocol

The scope of this architecture is shown in figure 5.1, taken from TS 101 314 [8], TS 101 315 [9], TS 101 882 [10], TR 101 303 [107], and ES 202 915-1 [108].

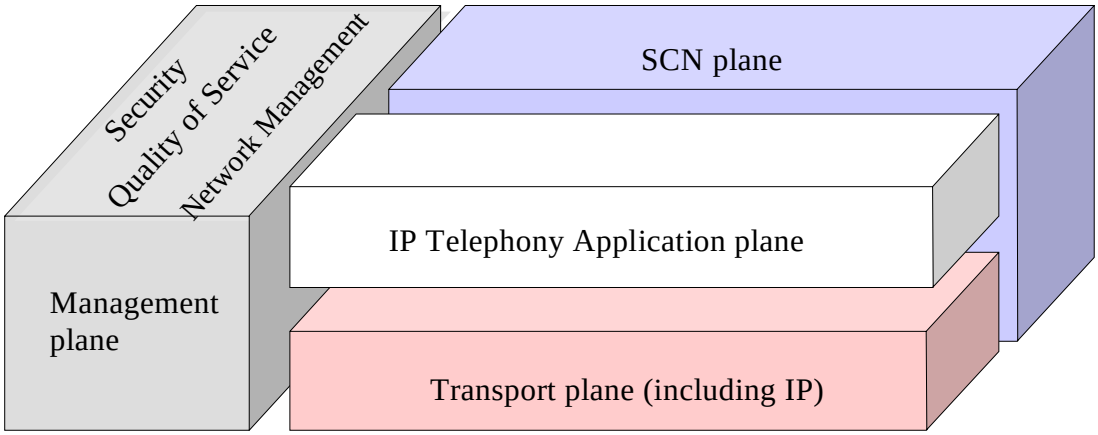


Figure 5.1: TIPHON scope

From this it can be seen that TIPHON implicitly regards it as important to blend legacy and NGN management (at least functionally). But savings could only be made if they are blended in practice.

The Transport plane and its management are of interest in the present document.

TIPHON has the functional layers shown in figure 5.2.

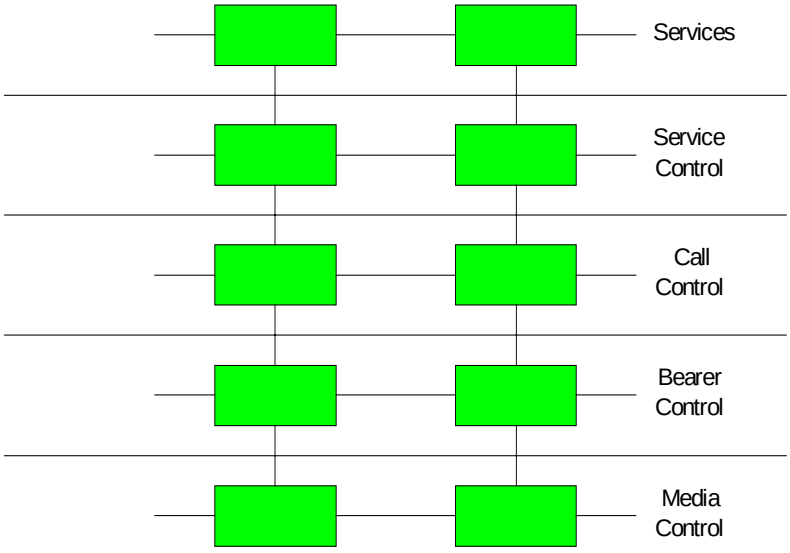


Figure 5.2: TIPHON Functional layers

Signalling transport affects the call control, bearer control and to some extent the media control layers of this model.

Reference is made to Tiphon throughout the present document, and its work has been incorporated in places.

6 Switched Circuit Networks (SCNs)

In the present document, the term Switched Circuit Network is taken to include PSTN, ISDN and mobile networks such as GSM.

Trunk signalling transport layers are defined in MTP ITU-T Recommendations Q.701 [34] and Q.709 [45] and for the SCCP in ITU-T Recommendations Q.711 [46] and Q.715 [50]. Transaction Capabilities for circuit unrelated signalling is defined in ITU-T Recommendations Q.771 to ITU-T Recommendation Q.775 [67] ISDN call related signalling is defined in ITU-T ISUP Recommendations Q.761 [58] to Q.766. [62]

ISDN access signalling is defined in ITU-T Recommendations Q.921 [68] and Q.931 series [69].

6.1 Access to networks

6.1.1 Analogue access

Nearly all users currently have analogue access.

There is a variety of signalling systems, the most common information signalling uses DTMF 2 out of ~5 voice frequency tones.

6.1.2 ISDN access

Some users have ISDN access which offers speeds of up to 128 kbit/s using both B channels.

6.1.3 Mobile access

See for example the GSM series of standards in GTS GSM 01.02 [20] to GTS 11.32 [28].

The GSM service is taken as the example for this description.

A GSM subscriber's Mobile Station (MS) communicates with a node called a base station (BS). The subscriber registers and sets up calls to the nearest base station (BS) of his/her GSM serving network for the cell in which he/she is currently situated, using the wireless "air interface".

A mobile station roaming to a Mobile-services Switching Centre (MSC) area is controlled by the Visitor Location Register (VLR) of this area. When a Mobile Station (MS) enters a new location area it starts a registration procedure via its nearest BS. The MSC in charge of that area notices this registration and transfers to the Visitor Location Register the identity of the location area where the MS is situated. If this MS is not yet known to the MSC, the VLR and the Home location register (HLR) exchange information to allow the proper handling of calls involving the MS.

The HLR is located within the country of the subscriber's subscription network, so if the subscriber is roaming, the HLR could be in another service provider's domain, possibly in another country. In that case, there needs to exist an agreement between the subscriber's service provider and the provider of the roaming service at the subscriber's current location (i.e. between the subscriber's home network and his/her serving network).

A call set up request is routed to the BS's mobile switching centre, and the MSC signals to its Visitor Location register (if the subscriber is visiting this serving network), or to the subscriber's home location register for the subscription details. The call is then completed.

Calls are set up from the mobile subscriber's own network (if the caller is roaming in a serving network, from that network to the subscriber's home network), and from there to the called person in her/his home network (or, if the called person is roaming, to her/his serving network via her/his home network).

Messages between BS and MSC use the SS7 BSSAP application over Connection Oriented SCCP over MTP. For signalling between MSCs and HLRs, and between HLRs and VLRs within the PLMN, MAP over TC over connectionless SCCP over the MTP is used.

The mobile network is connected to the fixed part of the SCN via Public Land Mobile Network (PLMN) Gateway MSCs, using the transmission and call signalling appropriate for the SCN interconnect agreement (e.g. TDM or ATM for bearers, SS7 MTP and ISUP for call control, and MTP, connectionless SCCP, TC and the appropriate application for information signalling).

6.2 Architecture, Routeing and Signalling

For the fixed network, nodes are Local Exchanges (LEs) or Trunk Exchanges (TEs). Signalling within the SCN is based on ITU-T SS7, and uses paths in the network which are distinct from those used for the media. Hence signalling information does not have to compete for its QoS with the media it controls. Signalling nodes are signalling end points (SEPs) or signalling transfer points (STPs). SEPs terminate SS7 voice/data circuits and contain the ISDN User Part or Telephony User Part, or contain other MTP Users such as the SCCP and possibly data base applications. STPs act as routers for SS7 messages between SEPs.

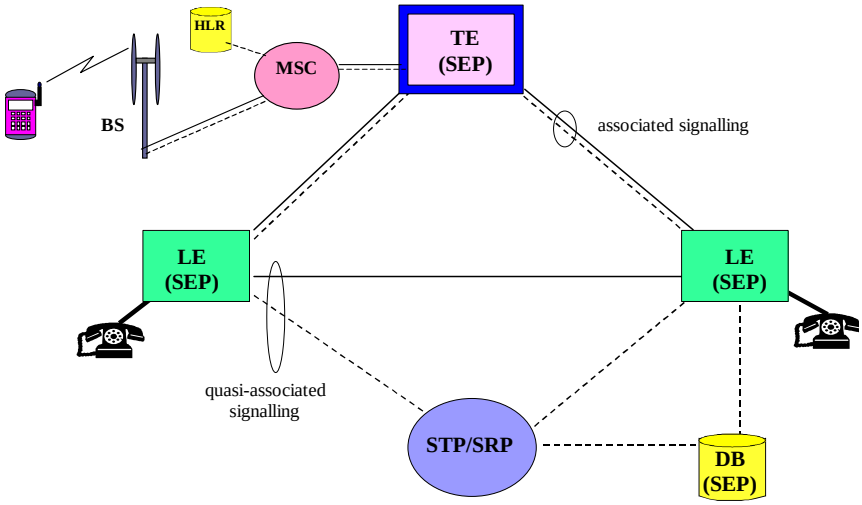
The transport layer physical layers are TDM with PCM multiplexes, or SDH + ATM for broad band and TDM replacement.

In a circuit switched network such as an ISDN, calls are routed from switch to switch, following the voice/data circuits used. In the circuit-associated case, the signalling and the transmission circuit follow the same path and each switch decides to which subsequent switch to route the call. The routeing decisions may be made using number analysis based on routeing tables stored within the switch, possibly with additional information from a database (intelligent network databases may be used for number portability or other services such as freephone calls). For simple calls the depth of analysis of the called party number tends to increase the closer the call gets to the called party. ISUP uses E.164 addresses, call routeing converts this to circuit identification code (CIC) + destination point code (DPC) (+originating point code (OPC) and network identity) for the circuit selected. The circuit's origin is at the exchange (and signalling end point) identified by the OPC, its termination is at the exchange identified by the DPC.

The MTP uses the DPC for routeing messages. At the message destination denoted by the DPC, the MTP distributes each message to the appropriate MTP User (e.g. ISUP) according to the value of the Service Indicator in the message's SIO field.

See annex B for more details.

6.2.1 Nodes



Key:
BS Base Station
DB Data Base
HLR Home Location register
LE Local exchange
MSC Mobile Switching Centre
SEP Signalling end point
SRP SCCP Signalling Relay Point
STP Signalling transfer point (MTP
TE Trunk exchange

voice/data path
signalling path

Figure 6.2.1: Nodes and signalling in ISDN and PLMN

6.2.2 Signalling

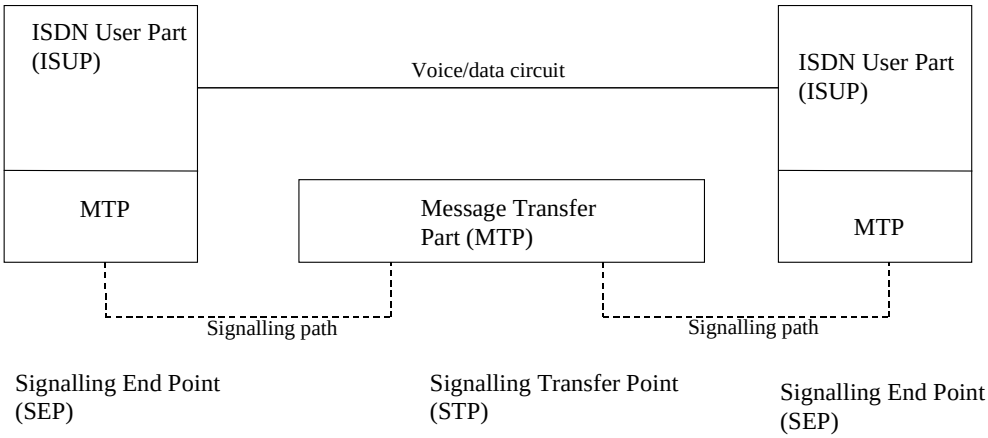


Figure 6.2.2: Typical SS7 stacks for ISUP call control

Of these stacks, the MTP layer is used for signalling transport. See annex B for more details.

6.3 Management and QoS of the signalling transport layer in SCN and ATM networks

6.3.1 Management

See ITU-T Recommendations Q.750 [52], M.3100 [30], Q.751.1 [53], Q.751.2 [54], Q.752 [55] and EN 301 007 [5].

Operations, Administration and Management (OMAP) of the signalling transport layers of an SS7 network are defined in the ITU-T series of Recommendations Q.75x and EN 301 007-1 [5], and an overview is given in ITU-T Recommendation Q.750 [52].

The management functions of SS7 are divided into three main parts:

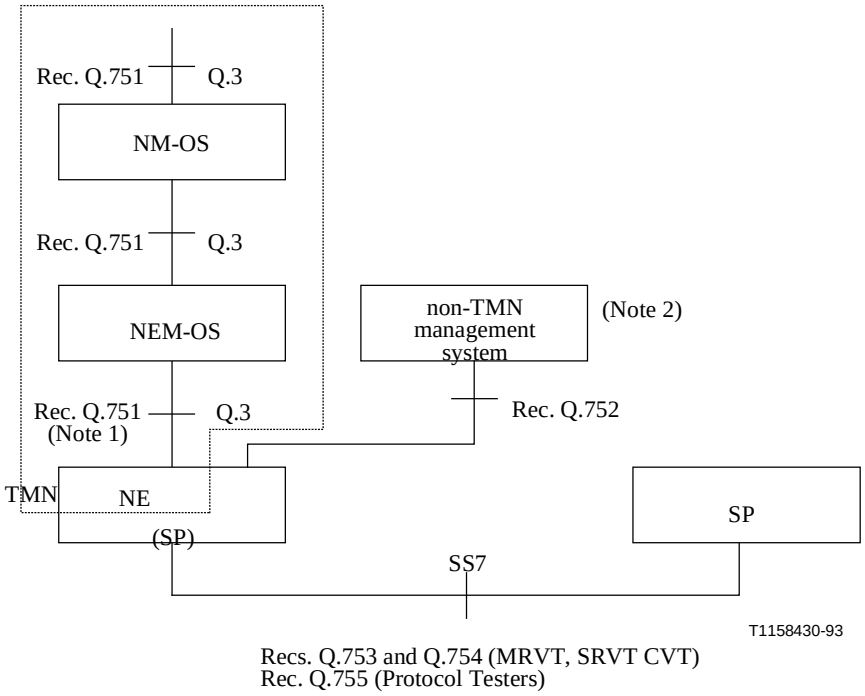
a) Management functions located in the Telecommunications Management Network (TMN) (which means the Network Element Functions (NEFs) and the Operations System Functions (OSF) (see ITU-T Recommendation M.3010 [31]). These functions include measurement collection and cover TMN-to-TMN interactions; such management functions are modelled as managed objects at the interface between network elements and operations systems, or between operations systems.

b) Management functions within the SS No. 7 protocol itself (e.g. changeover, forced rerouting, sub-system management, etc.).

c) Management functions defined to enable verification and validation of routing tables, CICs, etc. These functions may require communication within the signalling network, and for this a separate protocol is defined. Such management functions are modelled as managed objects at the interface between the network elements and an operations system.

Of the three sets of management functions defined above, OMAP provides a) and c). Set b) can be modelled as existing within the "Layer Management Entities" of SS No. 7, and the functions are defined in the Recommendations pertinent to those layers.

Figure 6.3.1 (which is the same as figure A.1/Q.750 [52]) is copied below and shows the relationship between TMN, SS7 management and the OMAP Recommendations.



NM-OS Network Management Operations System (OS)
NEM-OS Network Element Management OS
NE Network Element
SP Signalling Point
- - - Within this line is the TMN domain

NOTE 1 – Recommendation Q.751 references Recommendation Q.752 for measurements.
NOTE 2 – This is an implementation dependent system.

Figure 6.3.1: TMN, SS No. 7 management and OMAP Recommendations

The definition of TMN is concerned with five layers in management, namely business management, service management, network management, network element management, and the elements in the network that are managed.

Of these, OMAP is not concerned with business management, and interacts with other TMN parts to provide service management. For example, this latter interaction occurs if ISDN services require to be added so that subscribers at one exchange can use these services to subscribers at another exchange.

The top management level proper of OMAP is network management, which provides the functions and resources to allow Administrations (possibly via a set of administration managed objects) to control the SS7 network. Management functions and resources are provided by OMAP to allow management within the SS7 signalling points.

The definitions of both network management and network element management functions and resources utilize the TMN and OSI managed object approach, and allow changes to be coordinated within OMAP.

See clause B.4 for more information.

EN 301 007-1 [5] and EN 301 007-2 are the ETSI standards for OMAP, endorsing and constraining the ITU-T Recommendations.

6.3.2 QoS of the transport layer

6.3.2.1 Availability

There is an allowance of 10 min/yr for signalling route set outage (a probability of $1{,}9 \times 10^{-5}$.) See ITU-T Recommendation Q.706 [41].

At the link level (MTP level 2), signalling points are connected by linksets. A linkset is a load sharing collection of signalling links, where, if a link fails, changeover occurs, and the link's message traffic is automatically shared on to the remaining working links in the set.

At network level (MTP level 3), a signalling point routes messages towards their destination using a routeset. A routeset is a collection of alternative routes towards an MTP destination. At a node, a route is viewed as a linkset. Routes are arranged in priority order (and two or more routes may have the same priority, in which case the associated linksets at a node are termed a combined linkset). If a route currently carrying message traffic towards a destination fails (i.e. the last working link in the linkset fails), forced rerouteing occurs and the message traffic is automatically diverted to the next highest priority alternative route.

If a routeset fails, the application above the MTP (e.g. ISUP) might itself use alternative routeing.

All of these mechanisms provide for a high availability of service in the network. See ITU-T Recommendation Q.766 [62] for more details.

6.3.2.2 Performance

ITU-T Recommendation Q.706 [41] gives the probability for message loss in the MTP as 1 in 10^7, a 1 in 10^{10} probability for message duplication, and a 1 in 10^{10} probability for missequencing.

ITU-T Recommendation Q.706 IG [42] provides in figure 5 and figure 6 values for the mean and standard deviation of the total queueing delay for each channel of traffic on a signalling link against the signalling link loading, for a number of MSU total (i.e. level 2) sizes between 15 and 279 octets, for MSU error probabilities of 0 and 0,001, and for the signal unit error probability of 0,004 at which a signalling link will fail. The details of the calculations are shown in its annex B. Table 5/Q.706 [41] provides objectives for the transfer times through an STP, and ITU-T Recommendation Q.716 [51] provides objectives for transfer times through an SCCP relay point. ITU-T Recommendation Q.766 [62] provides objectives for the cross office transit time of call control processing intensive and processing non-intensive messages. Message delays and delay variation in an SS7 network can be estimated from these (see e.g. ITU-T Recommendations E.733 [4], E.721 [2] and E.723] [3]).

6.3.2.3 Security

An SS7 network is usually physically secure from break-in, masquerade attacks, etc. Denial of service is not a known problem. Confidentially of data is usually not a problem (encryption may be enabled across the radio link between handset and base station for mobile calls).

1) SS7 link level:
   links are either fixed point to point between Signalling Points which would require physical access in order to interfere with them; or they are radio links on which encryption could be used. Access to the links themselves would be required to insert a protocol analyser for eavesdropping or insertion of false messages.
   A break of more than 128 ms. in transmission in a TDM network would cause the link to fail, but then it would automatically attempt to realign itself. Before the link can go into service again at MTP level 3, it needs to pass a signalling link test, which checks the consistency of the link's OPC, DPC and signalling link code at each end (sending messages over the link), for which continuity in the signalling path is required. In addition, the signalling link test message contains an implementation-dependent field which must be reflected back to the test-sending end (this could be a timestamp, which could if necessary measure any extra delay inserted by an analyser). Thus, the physical access could be spotted either by the link failure, or by its extra round trip delay, or both. In addition, all link failures are monitored according to ITU-Recommendation
   ITU-T Recommendation Q.752 [55]

2) Network level:
   STP Gateways have a message screening function. ITU-T Recommendation Q.705 [40] section 8 defines a number of parameters in the MTP label which can be screened to ensure authorized signalling relations only are allowed, the most detailed screening is to allow messages only between particular combinations of OPC and DPC for particular MTP User Parts (denoted by their SI values).
   ITU-T Recommendation Q.752 [55] contains measurements for messages discarded because of screening.

3) SCCP level:
SCCP Relay Points have a screening function to allow messages only for certain combinations of certain parts of messages' calling party address and called party address, for certain SCCP users (denoted by their SSN values). This screening function is not defined by the ITU, but is by some standards bodies in some regions (e.g. Telcordia).

7 IP networks

There are Internet and only a few managed IP networks at present.

7.1 Subscriber Access Technologies

7.1.1 Analogue Modem

Typically, this is a 56 Kb/s V.90 modem attached to or bundled with a PC, using ordinary copper telephone cable.

Its download speed is typically 14 Kb/s, depending on the ISP and congestion conditions.

Internet access is usually differentiated by specific dialled E.164 numbers.

7.1.2 ISDN

Access to IP networks is as per ISDN network access, again differentiated according to called address.

Speeds of up to 128 kbit/s are possible using both B channels. The main advantage of ISDN compared to analogue modems is the very greatly reduced time between initiating the access and being able to send or receive useful data. For ISDN this time can be reduced to less than 1 second compared to 5 seconds to 15 seconds for a modem.

7.1.3 xDSL

A range of Digital Subscriber Line (DSL) technologies are available, the technologies are summarized in table 7.1.

These currently are mostly used for access to the Internet, rather than to a particular Operator's managed IP network.

Table 7.1: xDSL technologies

DSL type	Data rates	Pairs used	Analogue access on same pair	Range	Main current application
ADSL (Asymmetric DSL)	< 8 Mbit/s to the home < 512 kbit/s from the home	1	Yes	< 4 km	High speed Internet access and delivery of video-on-demand
HDSL (High speed DSL)	2 Mbit/s symmetric	1 to 3	No	< 4 km	Services to small businesses
VDSL (Very high speed DSL)	> 2 Mbit/s	1	No	< 500 m	Short connections of user premises to cabinets in the street served by fibre

7.1.3.1 ADSL

ADSL enables high speed Internet access to be provided in parallel with continued use of an exchange line by an analogue telephone. The Internet access can also be used for the various forms of VoIP.

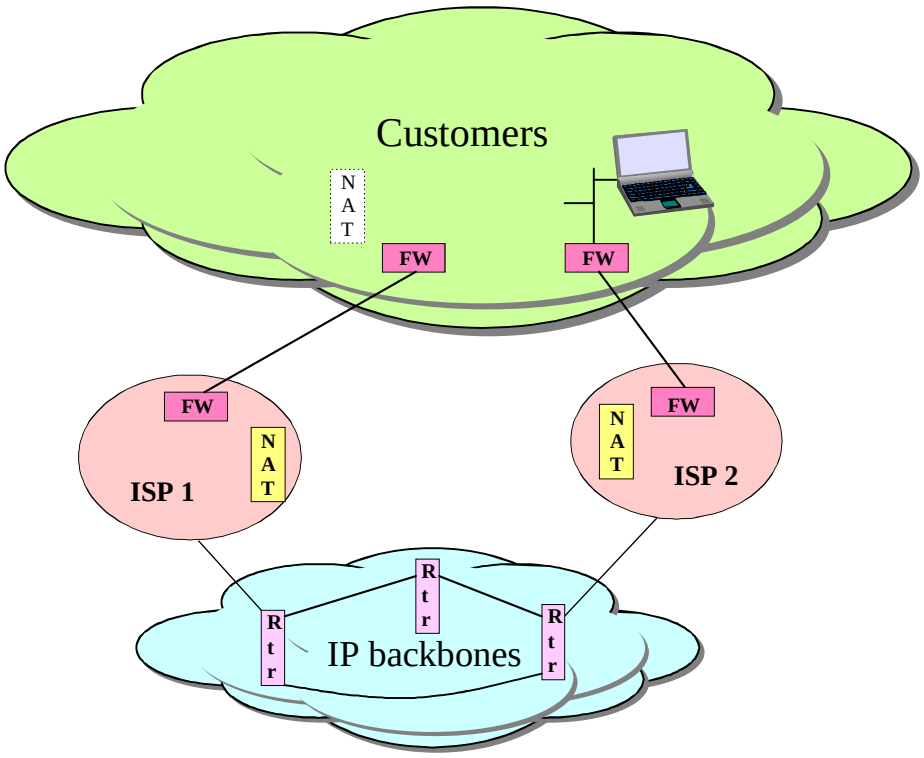
With ADSL the network termination point for IP network access would be either a LAN connection or a USB interface. IP packets are normally carried on ATM across a network owned by the access provider with each customer having a permanent virtual circuit (PVC) to their Internet service provider.

7.2 Nodes, signalling and routeing

There is a variety of layer 2 technologies used for IP networks (e.g. ATM, frame relay, etc.).

TCP, SCTP or RTP over UDP, or UDP, are used over IP to carry applications. IP addresses are used in some Application layers as well as at the network layer (i.e. IP layer). Restrictions can be experienced for IPv6 addresses to be carried in IPv4 infrastructure - Network Address Translators (NATs) are concerned with IP addresses at the IP layer, but Application Layer Gateways (NAT-ALGs) are involved if the Application also deals with IP addresses.

7.2.1 Network architecture



Key:
FW Firewall (and Gateway)
NAT Network Address Translator
ISP Internet Service Provider
Rtr Router

Figure 7.2.1: Internet and Managed IP network architecture

IP networks use IP routers at their edges or access points to route incoming and outgoing packets. Inside the network, however, they either have other IP routers or ATM routers to create a mesh of virtual connections between the IP routers at the edge. Where the service is sensitive to packet delay (e.g. for VoIP), the service's packets can be allocated a high priority, and techniques such as MPLS (see later) may be used within the IP network to ensure a sufficient Quality of Service.

Service Providers and their customers each tend to have Firewalls established to screen their IP network access, these are sometimes combined with Network Address Translators which determine IP addresses from names or URLs. See annex C for more information.

7.2.2 Signalling Transport

The following figure shows a sample of the different protocols used in IP networks from the Application layer down to the physical layer (the V.34 and V.90 modem protocols usually use PPP to access the Internet). The protocols used by signalling transport with which the present document is particularly concerned are RSVP, TCP, SCTP, IPv4 and IPv6, MPLS.

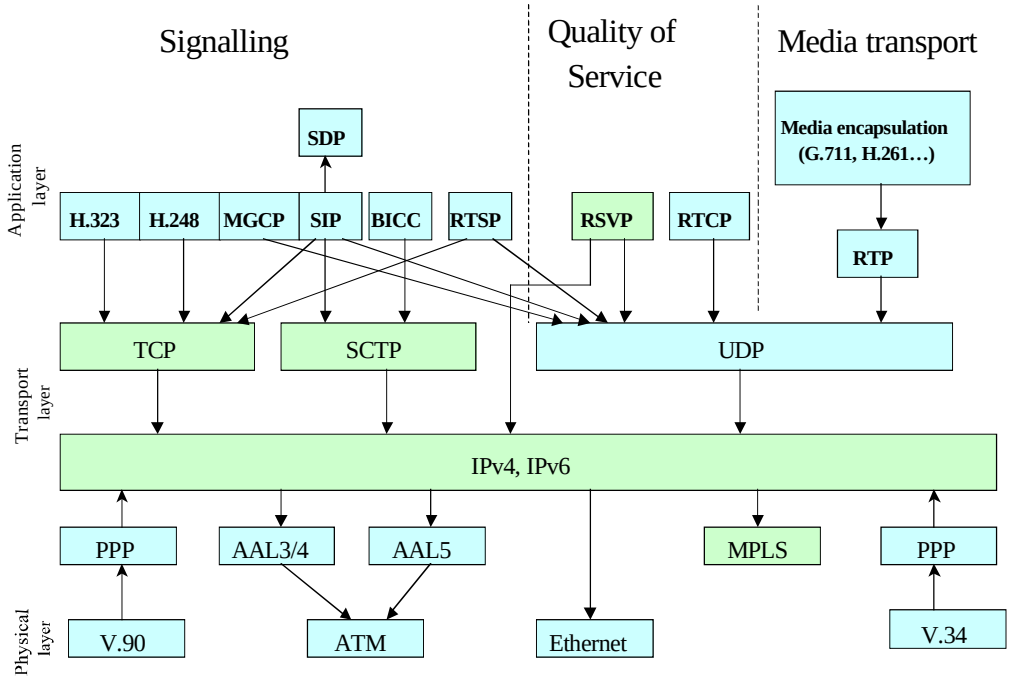


Figure 7.2.2: Collection of some of the protocols used in IP networks

The signalling transport layer within the managed IP network contains a choice of TCP or SCTP or UDP over IPv4 or IPv6 over the physical layer. MPLS may be used above or below the IP layer to provide some form of QoS assurance. BICC has a signalling transport adaptation layer between it and the transport layer. In addition to the protocols shown, ISUP or BICC call control messages may be tunnelled in the SIP protocol, and ISUP or BICC may be carried over the SIGTRAN M3UA protocol over SCTP, or over MTP layer 3, over either M2PA or M2UA, over SCTP.

7.2.2.1 Network layer protocol IPv6 and ICMPv6

See RFC 2373 [85], RFC 2460 [86], RFC 2463 [88], and RFC 2461 [87].

IP is the network layer protocol of the IP network, and serves to route message packets from a source node (host) to a sink node (another host), if necessary using intermediate router nodes.

IPv6 was defined since IPv4 address space is limited. Address space limitations led to dynamic assignment of IPv4 addresses by a server when an IP session is started.

The IPv6 specification is well covered by IETF, ETSI needs to standardize it (i.e. endorse it).

The Internet Message Control Protocol version 6 (ICMPv6) is used by IPv6 nodes to report errors encountered in processing packets, and to perform other internet-layer functions, such as diagnostics (ICMPv6 "ping"). ICMPv6 is an integral part of IPv6 and must be fully implemented by every IPv6 node.

7.2.2.1.1 IPv6 addressing

IPv6 addresses are 128 bits long, which should ensure address space exhaustion does not occur.

The type of address are:

1) Unicast, which is an identifier for a single interface. A unicast address or a set of unicast addresses may be assigned to multiple physical interfaces for load sharing over these physical interfaces.

2) Anycast, which is an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).

3) Multicast, which is an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

An IPv6 address is preferably represented as a text string in the form: x:x:x:x:x:x:x:x, where each x is the hexadecimal value of its one eighth 16-bit piece. An example is FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

A long string of bits whose value is zero may be shortened within the address by use of "::", but only one such use is permitted in one address. Examples are 1080:0:0:0:8:800:200C:417A which may be written 1080::8:800:200C:417A, and FF01:0:0:0:0:0:0:101 which may be written FF01::101.

Another representation may be used when IPv4 addresses are to be written as IPv6 addresses. This is of the form x:x:x:x:x:x:d.d.d.d, where x has the same meaning as before, and d is the decimal value of the IPv4 low-order 8-bit piece. An example is the IPv4 address 13.1.68.3 which could perhaps be given the IPv6 value 0:0:0:0:0:0:13.1.68.3, or ::13.1.68.3.

Address prefixes are written in the form iPv6Address/prefixLength, where iPv6Address has any of the notations above for IPv6 addresses, and prefixLength is the number in decimal of the left-most contiguous bits forming the prefix in the address. An example for the 60 bit prefix whose hexadecimal value is 12AB00000000CD3 in the address 12AB:0:0:CD30:: is 12AB:0:0:CD30::/60. Here it should be noted that leading zeroes may be dropped within a 16 bit chunk of an address, but trailing zeroes must not be.

7.2.2.1.2 Neighbour Discovery

Nodes within the IPv6 network make use of a set of procedures called Neighbor Discovery (see RFC 2461 [87]), which allow routeing tables within host and router nodes to be updated.

For more information see annex C.

7.2.2.1.3 Routeing of packets

Routeing information is held in Destination cache, Prefix list and Neighbour cache entries and used at a node until the cached information is suspected to be in error. At a host, each time that an upper layer protocol hands a message packet to the IP layer, the IP layer examines its Destination cache to see if an entry exists for that destination. If not, the next hop is determined by comparing the packet's address against the Prefix list to match the longest prefix there. If the destination is on-link, the next hop is the packet's destination. If not, the router to use is selected from the Default router list for this destination. The next hop information is then written into the cache. Having obtained the IP address of the next hop, if it is of type unicast, the Neighbour cache is examined for the link-layer information of the neighbour (e.g. its physical link identity). Address resolution is required if there is no neighbour information for this IP address. The message is sent once the link is determined.

The IP layer uses information from some of its higher layers (e.g. TCP) that its addresses are still reachable. IP sends a Neighbor Solicitation message if it suspects that a neighbour is unreachable, and a Neighbor Advertisement message is expected in reply. Nodal parameters are defined as to the frequency of this test, in the absence of higher layer assurance.

For more information see annex C.

7.2.2.2 MPLS

Multi-Protocol Label Switching (MPLS) (see RFC 3031 [89]) is used by IP routers at the edges of a network to attach locally defined labels to IP packets. These labels define a Forwarding Equivalence Class (FEC) which can be used to distinguish between different types of traffic (e.g. real time application versus non-real time), and also to define a complete route through the network.

The use of labels reduces the processing load on the router because the label can be analysed more easily and quickly than the IP address. The three main advantages of adding label switching to an IP core network are:

- The reduction in delay;
- The addition of source route control;
- The introduction of different quality classes.

Where the internal routers are ATM rather than IP, the label is carried in the ATM header instead of the virtual path – virtual channel identifier (VPI/VCI).

7.2.2.3 SCTP

See RFC 2960 [77], RFC 3309 [78] and TS 102 144 [76].

SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users:

- acknowledged error-free non-duplicated transfer of user data;
- data fragmentation to conform to discovered path maximum packet (MTU) size;
- sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages;
- optional bundling of multiple user messages into a single SCTP packet; and
- network-level fault tolerance through support of multi-homing at either or both ends of an association.

The design of SCTP includes congestion avoidance behaviour and resistance to flooding and masquerade attacks.

SCTP has advantages over TCP in that it provides multiple streams per SCTP association, thus minimizing "head of line" (HOL) blocking of one traffic stream by another. It is packet-based, rather than byte (plus segment) based, and allows multi-homing. Its congestion control technique is similar to TCP's.

For more information, see annex C.

7.2.2.4 TCP

See RFC 793 [106].

TCP is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP provides for reliable inter-process communication between pairs of processes in host computers attached to distinct but interconnected computer communication networks. TCP assumes it can obtain a simple, potentially unreliable datagram service from the lower level protocols.

TCP fits into a layered protocol architecture just above the Internet Protocol (see e.g. [IPv6]) which provides a way for TCP to send and receive variable-length segments of information enclosed in datagram "envelopes". The datagram provides a means for addressing source and destination TCPs in different networks. The internet protocol also deals with any fragmentation or reassembly of the TCP segments required to achieve transport and delivery through multiple networks and interconnecting gateways. The internet protocol also carries information on the precedence, security classification and compartmentation of the TCP segments, so this information can be communicated end-to-end across multiple networks.

7.2.2.4.1 Operation

The primary purpose of TCP is to provide reliable, securable logical circuit or connection service between pairs of processes. To provide this service on top of a less reliable internet communication system requires facilities in the following areas:

- Basic Data Transfer;
- Reliability;
- Flow Control;
- Multiplexing;
- Connections;
- Precedence and Security.

7.2.2.4.1.1 Basic data transfer

TCP transfers a continuous stream of octets in each direction between its users by packaging a number of octets into segments for transmission. Each TCP decides when to block and forward data at its own convenience.

Sometimes users need to be sure that all the data they have submitted to the TCP has been transmitted. For this purpose a push function is defined. To assure that data submitted to a TCP is actually transmitted, the sending user indicates that it should be pushed through to the receiving user. A push causes the TCPs promptly to forward and deliver outstanding data to the receiver. The exact push point might not be visible to the receiving user and the push function does not supply a record boundary marker.

7.2.2.4.1.2 Reliability

TCP recovers from data that is damaged, lost, duplicated, or delivered out of order by the underlying system, by assigning a sequence number to each octet transmitted, and by requiring a positive acknowledgment (ACK) from the receiving TCP. If an ACK is not received within a timeout interval, the data is retransmitted. At the receiver, the sequence numbers are used to order correctly segments that may be received out of order and to eliminate duplicates. A checksum is added to each segment transmitted, which is checked at the receiver. Segments with an incorrect checksum are discarded.

7.2.2.4.1.3 Flow control

TCP provides a means for the receiver to govern the amount of data sent by the sender. This is achieved by returning a "window" with every ACK indicating a range of acceptable sequence numbers beyond the last segment successfully received. The window indicates an allowed number of octets that the sender may transmit before receiving further permission.

7.2.2.4.1.4 Multiplexing

TCP provides a set of addresses or ports within each host to allow for many processes within a single Host to use TCP communication facilities simultaneously. This set of ports, when concatenated with the network and host addresses from the internet communication layer, forms a socket. A pair of sockets uniquely identifies each connection. That is, a socket may be simultaneously used in multiple connections.

The binding of ports to processes is handled independently by each Host. However, it proves useful to attach frequently used processes (e.g. a "logger" or timesharing service) to fixed sockets which are made known to the public. These services can then be accessed through the known addresses.

7.2.2.4.1.5 Connections

TCPs are required to initialize and maintain certain status information for each data stream. The combination of this information, including sockets, sequence numbers, and window sizes, is called a connection. Each connection is uniquely specified by a pair of sockets identifying its two sides.

When two processes wish to communicate, their TCPs must first establish a connection (initialize the status information on each side). When their communication is complete, the connection is terminated or closed to free the resources for other uses.
Since connections must be established between unreliable hosts and over the unreliable internet communication system, a handshake mechanism with clock-based sequence numbers is used to avoid erroneous initialization of connections.

7.2.2.4.1.6 Precedence and Security

The users of TCP may indicate the security and precedence of their communication. Provision is made for default values to be used when these features are not needed.

For more information on TCP, see annex C.

7.2.2.5 RSVP

See RFC 2205 [91] and Jun Diffserv (see bibliography). RSVP is a protocol that is used by an application to request reservation of resources by routers. Source and destination hosts exchange RSVP signalling messages, this causes the RSVP- enabled routers along the flow path of the application's packets to keep a state machine for each RSVP flow.

Two main types of service can be requested - guaranteed or controlled load.

7.2.2.6 Differentiated services (Diffserv)

See RFC 2475 [84], RFC 2368 [93], RFC 2474 [83] and Jun Diffserv. Diffserv enables the segregation into classes of traffic entering a network, the class is denoted by the IPv6 Traffic Class octet. Diffserv can also condition traffic flow at the edges of the network. Per hop behaviour (PHB) is defined for each traffic class within a "Diffserv domain" consisting of a set of contiguous Diffserv routers with the same service provisioning policies and PHB group definitions.

Two PHB groups have been defined - expedited forwarding (providing low loss, low delay, low jitter and assured bandwidth) and assured forwarding (containing four traffic classes, each giving a high probability of packet delivery, providing that the aggregate traffic in the class does not exceed the prescribed rate. Packets within each class can be differentiated further as to the relative probability of dropping them under network congestion).

7.2.3 Call and bearer control

7.2.3.1 Session Initiation Protocol (SIP)

See RFC 3261 [104], also TS 101 884 [15], TS 124 229 [16] and ITU BICC/SIP (see bibliography).

SIP normally uses TCP as its underlying transport layer, but work has been done to allow the use of SCTP instead.

SIP is a protocol defined by the IETF for initiating, modifying and terminating end-to-end sessions of communications. These sessions can include Internet multimedia conferences, Internet telephone calls and multimedia distribution. SIP's key functions are to determine the called party's current address and to match communication capabilities and preferences between all parties in the session. SIP messages encapsulate SDP information to control a call.

The original aim in using SIP for telecommunications was for it to open the session, and then higher layers would establish and control the call. SIP is hence a relatively simple protocol. The 3GPP project has defined its multimedia call control protocol based on SIP and SDP, in places it has defined extensions to them.

SIP is being studied by the ITU for use over managed IP networks, this variant is called SIP-I.

SIP is an alternative protocol to H.323.

A possible area of further investigation in the domain of SIP may be to consider the selection of a compatible subset signalling protocol profile to facilitate interoperability.

7.2.3.2 H.323

See ITU-T Recommendation H.323 and TS 101 883 [12].

H.323 is ITU-T's standard for "Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service". H.323 defines the components of the system and the signalling, but it does not define the LAN or transport layer, hence it can be used for voice and multi-media over IP.

The H.323 functional components are:

1) Terminals (TEs);
2) Gateways (GWs);
3) Gatekeepers GKs);
4) Multipoint Control Units (MCUs).

The call control signalling in H.323 is based on ISDN access signalling (ITU-T Recommendation Q.931 [69]).

7.2.3.3 H.248 & Megaco

H.248 is an ITU-T standard for the Media Gateway Control Protocol. This is a protocol to provide remote control of media gateways. The standard was developed originally by the Megaco group in IETF and offered to ITU-T for publication as H.248. It probably does not need to be standardized for Europe, since it is unlikely that an MGC would control an MGW across an administrative domain. boundary. See also TS 101 885 [11].

7.2.3.4 BICC Bearer Independent Call Control

See EN 301 848 [7], ETSI BICC and ITU-T Recommendation Q.1901 [32].

BICC is a standard developed in ITU-T and ETSI for signalling. It is heavily based on ISUP.

BICC uses a signalling transport service adaptation layer (see ITU-T Recommendation Q.2150.0 [33]) directly underneath it, so it can use various signalling transport layers without modification to BICC itself. These transport layers include SCTP, or M3UA over SCTP (utilizing the work done for MTP3b within the SCN) for an IP network.

BICC has been standardized within Europe for European-standardized services, ETSI have a work item for completing this for all ETSI-standardized ISUP services.

7.3 Management, QoS of the signalling transport in the network

7.3.1 Management

See RFC 3410 [105] and its references, also TR 101 303 [107] and ES 202 915-1 [108].

SNMP is the management framework supported by the IETF for the Internet. There are a number of versions.

Version 3 is the latest, and the first to define security and administration.

If use of IP networks (of whatever type) intensifies greatly, it will become important to simplify management as much as possible. If different vendors are used by an operator for the same network, standardization of management information would be worthwhile.

A draft M3UA MIB has been written, also one for SCTP. See the bibliography on MIBs for references (draft-ietf-sigtran-sctp-mib-09 (using SMIv2, RFC 2578, RFC 2579 and RFC 2580), draft-ietf-sigtran-m3ua-mib-04 (using SMIv2, RFC 1902, RFC 1903, RFC 1904; SNMPv3, RFC 1906, RFC 2272, RFC 2574; SNMPv2PO, RFC 1905; SNMPv3APP, RFC 2273; SNMPv3VACM, RFC 2572). But see RFC 3410 [105]). These MIBs contain a few managed objects for performance measurements as well as managed objects to set up state and routeing tables.

No MIBs have yet been agreed for M2UA, M2PA or SUA.

7.3.2 QoS and security

ITU-T Recommendation Y.1541 [110] and G.1000 [19], RFC 2386, RFC 2676, Jun IPdep, Jun TE, also FIPS PUB 46-3 [101] and FIPS PUB 180-2 [102].

The QoS for signalling transport within IP networks is of concern, since signalling packets have to be conveyed in the network along with media packets. Differentiating flows requiring treatment other than "best effort" routeing according to delay, jitter and loss characteristics is at an early stage.

ETSI should provide guidance on means of assuring signalling transport QoS.

Signalling paths using SCTP will probably need a low probability of packet drop, fairly low delay, not much jitter (although this could be higher than that for VoIP packets), assured bandwidth and low congestion. If signalling uses Diffserv (with possibly MPLS) under SCTP and over IPv6, then at least Assured Forwarding per hop behaviour (PHB) may be required.

The managed part of a managed IP network can be made as secure as an ISDN. But if the managed IP network is connected to the Internet, attacks popular in the Internet could well be made in the managed IP network part. This may lead to investigations whether and how security could be specified end to end. See RFC 2401 [96].

8 Interconnection between networks

See Annex D for more details, also ETSI ISTP.

8.1 Edge nodes, interworking and using legacy applications

8.1.1 Edge nodes

Figure 8.1.1 shows the basic architecture of a next generation network switch.

Access from the SCN is usually over PCM bearers from the TDM network, or by ATM bearers over SDH. These bearers physically terminate at the Media Gateway (MGW), SCN SS7 signalling links terminate logically at the Signalling Gateway (SG).

Subscriber access can be from modems, or ISDN, or xDSL. A variety of access systems connects into the managed IP network (or ATM network) to carry call control information to the MGC, and media streams to the MGW. ISDN access from the SG to the MGC can use the ISDN Q.921 User Adaptation layer (IUA) over SCTP over IP (see RFC 3057 [103]), a V5.2 adaptation layer is being defined.

Call and bearer control is performed in the Media Gateway Controller (MGC). Communication between this and the MGW and SG is over the managed network in which the NGN node resides. If this managed network uses IP, between the MGC and SG the IETF protocols M2UA over SCTP over IP (v6 or v4), or M3UA over SCTP over IP can be used, or BICC over SCTP over IP. If M2UA is used it "backhauls" the SS7 signalling links from the SG to the MG, and then the MGC is viewed as a signalling point from within the SS7 network. Use of M3UA means that the SG itself is viewed as a signalling point (and then the MGC could be "homed" on the SG, using the same point code, or it could have its own point code and use the SG as an STP).

Note that the 3GPP consortium have specified the use of M3UA for SS7 signalling transport within their IP-based core network. See TS 129 202 [109].

For communication between the MGC and MGW, H.248 (MEGACO) or MGCP have been defined.

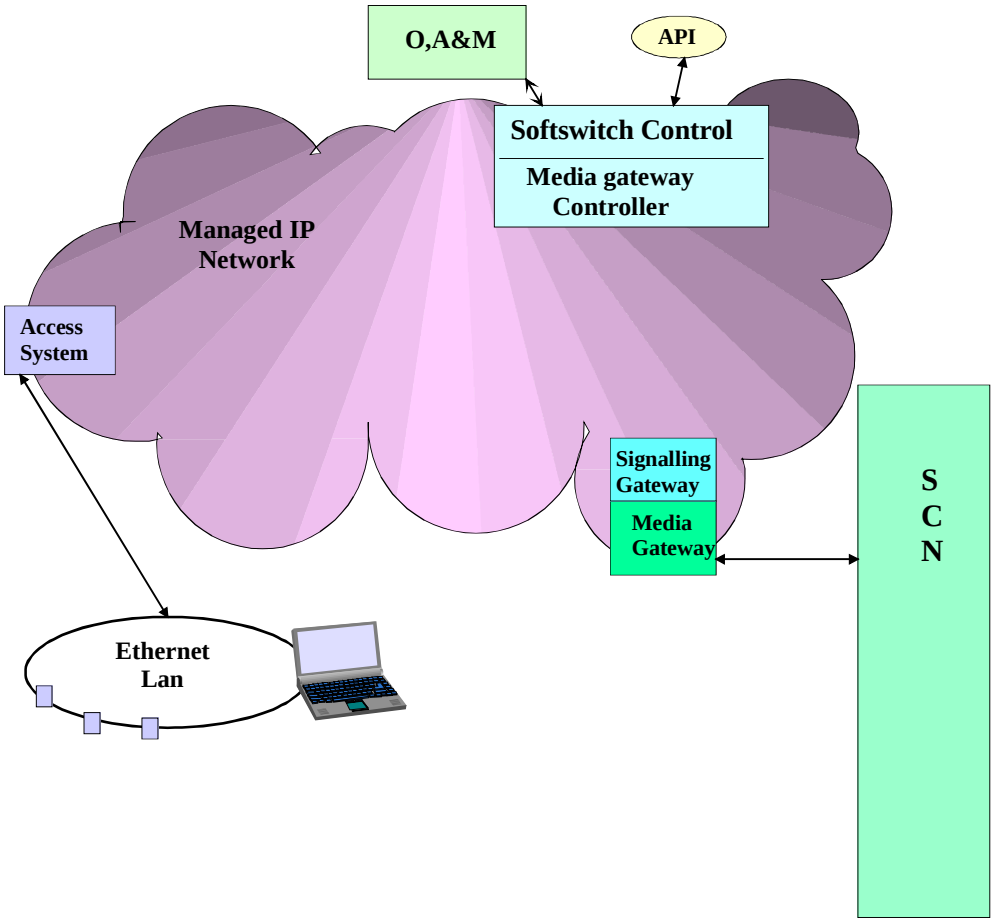


Figure 8.1.1: Schematic of a Softswitch NGN node

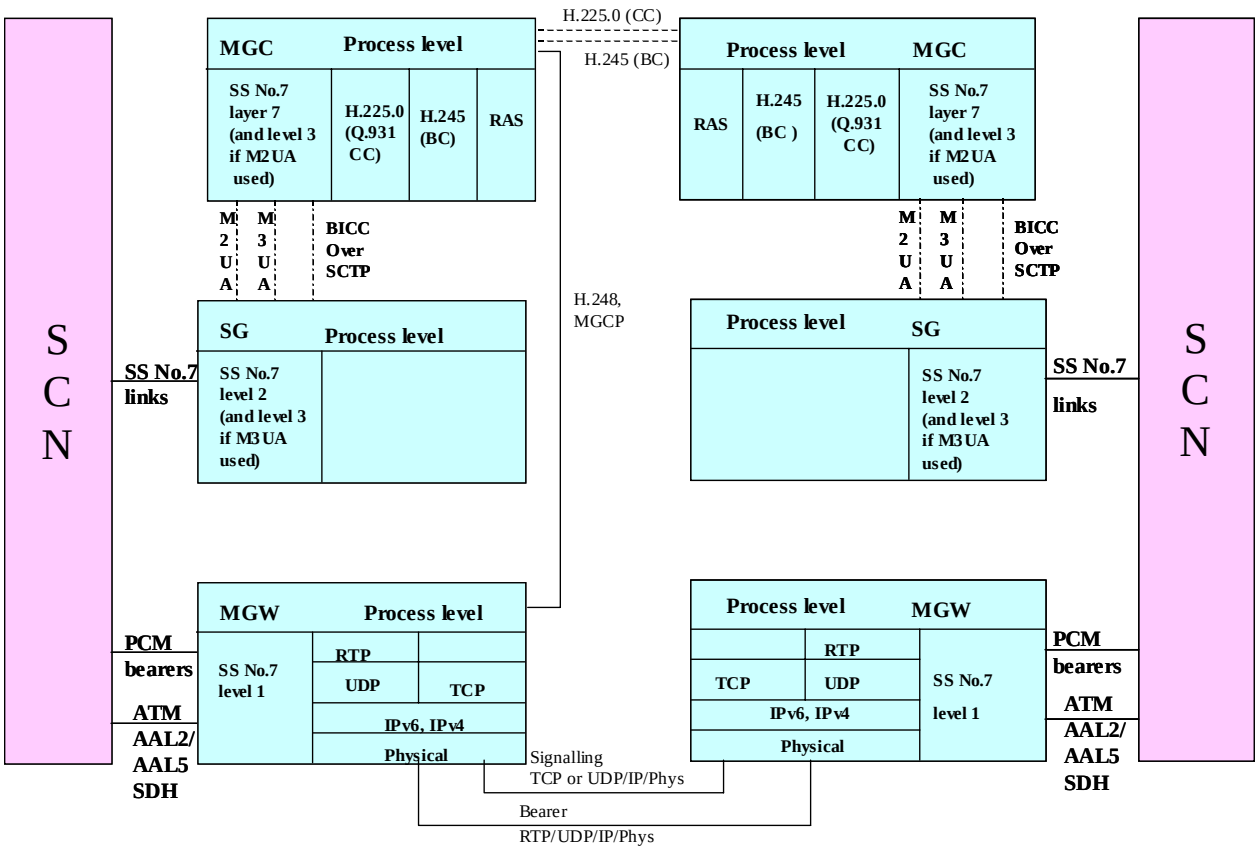


Figure 8.1.2: Functional elements of NGN nodes (here using H.323)

Communication occurs across the managed IP network in this example by using H.225.0 for the call control, and H.245 for bearer control. RAS is used for registration signalling to the H.323 Gatekeeper (which could be in this MGC or in an MGC across the network).

In version 2 of H.323, the H.245 signalling can be encapsulated within H.225.0 messages. Previously, separate signalling paths were required.

An NGN node's software provides:

- service provision;
- call management (i.e. a call server);
- subscriber management;
- call record generation;
- for the communications of terminals.

With the SIP protocol, the node implements the proxy functions.

8.1.2 Interworking between the SCN and the IP network

See also TR 101 308 [17] and ITU-T TD38 (see bibliography).

The SCN typically uses ISUP over MTP, with IN using INAP over TC over SCCP over MTP.

At the NGN node, there could be conversion of ISUP to BICC or SIP over SCTP over IP, or e.g. BICC over M3UA over SCTP over IP, or H.323 over TCP over IP. Or ISUP could be conveyed across the IP network over M3UA over SCTP. There are numerous possibilities.

NOTE: SIP-I can encapsulate ISUP to enable interworking. ISUP could encapsulate H.323 or SIP-I (if it were defined), using the Application transport mechanism (APM) scheme.

At the media gateway, there is conversion of PCM voice/data in each channel timeslot to RTP over UDP over IPv4/v6.

8.1.3 Using SS7 applications in or through a Managed IP network

8.1.3.1 Protocols

See M2UA, RFC 3331, M3UA, RFC 3332, SUA and SCTP.

The IETF SIGTRAN working group have defined a number of protocols to carry SS7 signalling over an IP network. These are called "User Adaptation Layer" protocols. One exists for MTP level 3 (M3UA, RFC 3332), one for MTP level 2 (M2UA, RFC 3331), one for SCCP (SUA, as yet an Internet draft - 14). Yet another protocol has been defined for MTP level 2 peer-to-peer signalling (M2PA, as yet an Internet draft - 7). SNMP Management Information Base drafts have also been defined for SCTP and M3UA protocols.

An AS is a an abstraction of an MGC function. An SG can be viewed in the SS7 network as an SEP (where the ASs have the same point code as the SG - however, this possibility is not allowed within ETSI), or as an STP (where the ASs can have different PCs to the SG) or SCCP relay point (SRP, where the ASs can have different SCCP addresses to the SG).

Figure 8.1.3.1 shows the M3UA arrangement from SCN to signalling gateway to MGC.

Further details can be found in annex D.

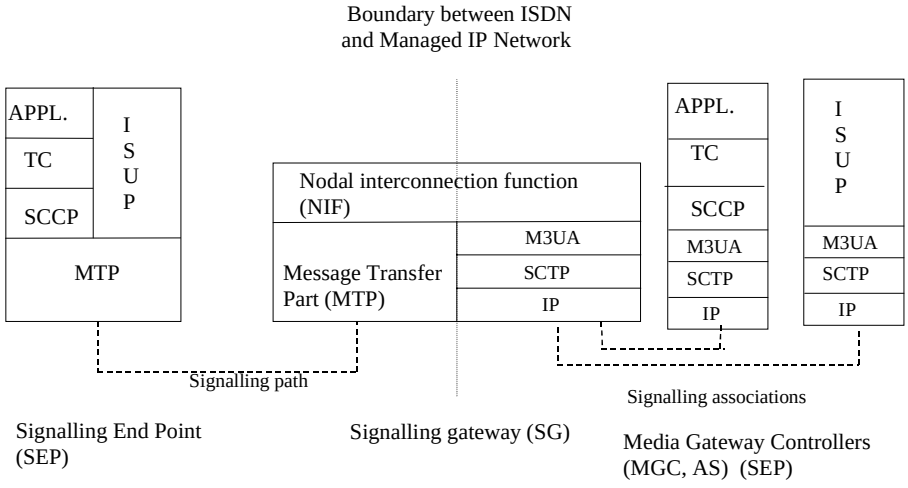


Figure 8.1.3.1: M3UA stack for carrying SS7 from ISDN to IP network

There is a significant amount of work to do before the SIGTRAN protocols should be used to carry live signalling traffic. First of all, the architecture(s) to be modelled should be defined. ETSI have now agreed a Work Item for this.

A guide may be useful for the selection of the appropriate User Adaptation Layer protocol, and how this should be integrated into existing networks.

Performance of the IP network could affect the SS7 network.

A possible area of study may be SUA to determine the effect of combining a managed IP network part with an SCN part on SCCP congestion/overload control mechanisms, and upon route and network availability.

A possible area of study may be in M3UA of how the SS7 flow, congestion and overload control mechanisms work between networks. The managed IP network has a potential to carry large amounts of message and call traffic, the time it takes to recognize a routeset failure or congestion is dependent upon the flow timer parameters used in the SCTP associations. In particular, the interaction of the ISUP and SCCP congestion control mechanisms has been studied for SS7 networks to enable a fair flow control policy to be established. How the parameters are to be set for the managed IP network, and how these affect the SS7 network flows, has to be determined.

For M2UA, MTP level 2 flow control is achieved by the Transmission buffer/retransmission buffer congestion onset thresholds being set to detect receive congestion quickly at the other end of a signalling link, and to inform local Users (and also remote ones if the signalling point this end is an STP) quickly enough for them to reduce message traffic in a timely fashion. The flow control in SCTP can be achieved by setting the receiver window size appropriately. However, M2UA admits that there might be oscillation when the MTP and M2UA methods have to interwork at the SG. A possible area of study may be how these mechanisms interact, and the effect on the SS7 network. It should be noted that the link capacity, delay characteristics and failure behaviour for links in SS7 networks have been determined by a large number of studies over a long period, that the managed IP network has the capability to inflict large loadings on an SS7 link, and as yet the interconnection of managed IP and legacy SS7 networks is in its infancy.

In addition, the time to detect link failure is well determined in SS7, and the rate of link failures, and taken together these factors are used to determine the network dimensions to give the required availability of the SS7 service. For SCTP the time to detect link failure depends upon the traffic patterns in the IP network and the retransmission timer values set for SCTP. Rules for setting these timer values need to be determined.

8.1.4 All IP path

There is a possibility for an all-IP path. For example, SIP-I could be used from origin PC with a VoIP phone attached to a destination PC with a VoIP phone (or even a speaker and microphone on the PC).

8.2 Joint management of the networks and QoS for the signalling transport layers

8.2.1 Management

See RFC 3410 [105], RFC 2578 to RFC 2580, M.3010 [31], Q. 751.1, Q.751.2 [54], TR 101 303 [107], IPHON MGMT2, TIPHON MGMT3 and ES 202 915-1 [108].

A possible area of study may be integration of the management of the SS7 User Adaptation Layers' managed objects into existing network management, e.g. into the MTP and SCCP management based upon OSI management (ITU-T Recommendations Q.751.x series, EN 301 007, Q.750 [52], X.700 [71], M.3010 [31], M.3100 [30].

The ITU-T MTP MIB is defined in ITU-T Recommendation Q.751.1 [53], the SCCP MIB is defined in ITU-T Recommendation Q.751.2 [54], both of these are endorsed in EN 301 007 [5].

8.2.2 QoS

See Jun VoIP, Y.1541 [110] and TR STQ-00037 (see bibliography).

For signalling transport within the IP network, a QoS comparable to that of SS7 signalling transport within the SCN is desirable.

ITU-T Recommendation Y.1541 [110] defines performance objectives for IP-based services, as yet it is unclear if a similar document exists concerned only with the QoS required for signalling transport within an IP network.

In order to be able to compare network performance estimates for SS7 signalling with that for IP-based services, an estimate for the parts contributed by the SS7 network in the equivalents of the parameters IPTD, IPDV, IPLR and IPER of table 1/Y.1541 [110] is needed.

Table 1/Y.1541 [110] gives the UNI to UNI performance objectives, but the example calculations given in the Appendices to Y.1541 [110] show the relevant network portions of these objectives, and it is these with which the MTP performance figures can be compared.

8.2.2.1 Availability and reliability

The probability of unavailability. is given by the probability of total inaccessibility of the sink from the source. It is assumed that a suitable IP network availability can be engineered. The availability equivalent to an MTP routeset might be provided by the use of an SCTP multi-homed association.

ITU-T Recommendation Q.706 [41] gives the probability for message loss in the MTP as 1 in 10^7, a 1 in 10^{10} probability for message duplication, and a 1 in 10^{10} probability for missequencing. If the SU error rate on a link is greater than 1 in 256 ($\sim 4 \times 10^{-3}$), the link fails. These figures should be compared to the values obtained for the particular layer 4 signalling used in the IP network. For example, TCP and SCTP retransmit messages if timeout occurs for acknowledgement, thus an overall message loss probability is related to, but is not the same as, a combined IPLR and IPER of ITU-T Recommendation Y.1541 [110]. Missequencing or message duplication might conceivably occur, for example, if SCTP uses its multi-homing capability on failure of an association. This is analogous to the probability of the MTP performing a time-dependent changeover and thereby mid-sequencing messages.

8.2.2.2 Performance

For call set up the acceptable signalling loop delay and its variation is governed by message response timers of the order of a few seconds, by the caller's expectations for post-dialling delay and by the charging implications if an answer message is delayed. Cut through of the speech path for voice calls needs to be done quickly to avoid speech clipping. Any signalling to retrieve information from external data bases during call set up or for call modification should not extend delays unduly over those experienced in the SCN. See ITU-T Recommendations Q.766, E.721 [2] and E.723. [3]

Estimates of such delays and delay variations need to be made for signalling transport associations, and some means of realizing the required QoS may need to be defined.

For M3UA, the bandwidth required for an SCTP signalling association could be defined, and this compared to that of a route in MTP3 (although in SCTP the number of links per linkset limitation does not apply).

The equivalent to Y.1541 [110] values of IPTD and IPDV need to be estimated for the SCN, to be able to define the QoS required of the IP network.

The QoS parameters appropriate to signalling transport need to be defined for a managed IP network. Those estimated for the existing SS7 network provide a valid starting point. A possible area of study may be to consider architectures, provisioning rules and traffic parameters appropriate for the signalling transport required for services to be provided by the IP network.

8.2.2.3 Security

See FIPS PUB 46-3 [101] and FIPS PUB 180-2 [102], also Code Book and Crypt Analysis.

IPsec (see RFC 2406 [98] and RFC 2401 [96]) or optionally TLS (see RFC 2246 [95]) are specified to be used by SIGTRAN protocols. These can enable confidentiality or authentication (one at least must be used - authentication can use an RSA-like handshake plus a signature), and in addition encryption of the signalling information (using a symmetrical algorithm, so using the same key for encryption and decryption - with the key being determined during the authentication phase). However, encryption *for use outside* the USA tends to be standard DES (albeit with CBC). It is possible this could be compromised in the near future, so a 128 bit key DES (3DES) or similar may be used instead. But it is not clear if the US will allow this outside the US. See FIPS PUB 46-3 [101] and FIPS PUB 180-2 [102].

The use of IPsec with multi-homed SCTP associations is at present inconvenient. If one end of a multi-homed association has *n* IP addresses, the other has *m* addresses, then 2*nm* security associations have to be set up, and these cover all applications using the SCTP association.

ETSI should provide guidance on the security scheme to use.

9 Addressing and naming issues

The systems for identifying called and calling parties use names and addresses.

Names

Names for email and web sites are familiar (email e.g. bob@etsi.org, web address www.etsi.org). ISDN numbers can also be regarded as names (e.g. for the free phone service).

Addresses

The SCN uses the E.164 scheme for routeing of calls, and some SCCP messages.

ENUM (see e.g. RFC 2916 in the bibliography) may be used to obtain an IP address from an E.164 one.

For M3UA (see [M3UA]), the Signalling Gateway (SG) and Application Servers (ASs) are identified within the SCN connected to the IP network by point codes (PCs). For routeing of messages within the IP network, a correspondence between an entity's IP address and its PC needs to be made within the M3UA routeing function. This also has to be defined in the management system.

For SUA (see [SUA]), messages can be routed on global title (GT) or on PC. GT Translation in the SCCP in the SCN in some cases translates E.164 numbers to DPC [+SSN] to route the message to the node and then distribute to the end subsystem. SUA performs a similar function, but here the result is ultimately an IP address. The function could be abbreviated to translate E.164 numbers directly to the SUA IP address. For IP telephony, DNS or ENUM may be used, but for SUA, since performance requirements preclude use of an outside data base, this probably cannot be done. The performance requirements are listed in ITU-T Recommendation Q.716 [51]. In any case, the management system needs to define the correspondence between GT and IP address.

RFC 3257 [80] discusses using SCTP with NATs.

10 Transition to IPv6 in Managed IP networks

There are a number of possibilities for managing the transition from IPv4 addressing to IPv6 within the IP network. These are covered in detail in the bibliography (see transition documents) and will not be repeated here.

It should be noted that SCTP (see [SCTP]) as defined for ETSI optionally allows for use of IPv6 addresses instead of, or as well as, IPv4 addresses. The SIGTRAN adaptation layers above SCTP also allow IPv6 addresses to be used. A signalling point can thus be identified by an SS7 identity (point code, global title etc.) which could have a representation within the IP network by both an IPv4 and an IPv6 address. As far as these layers are concerned, an SCTP association using IPv4 addressing could be re-established using IPv6, and this could appear seamless to layers using the SIGTRAN protocols.

11 Standardization in the IETF

The IETF produces RFCs (Request for Comments). These give the general framework for producing equipment, they are not (usually) detailed specifications. They are designed to allow competition between interested parties.

Verification occurs as a result of interoperability testing between implementations.

12 Identification of the standards areas concerned and the gaps

12.1 Signallings, interworkings and other items

Possible area of further investigation in the domain of Signallings and interworkings: a set of ETSI-defined services and supplementary services.

Possible areas of further investigation in the domain of signalling transport may be:

1) An architecture stating the choices possible for a SIGTRAN connected-IP network, and making recommendations. This may be beneficial to achieve similar QoS figures for NGNs. A Work Item has been agreed to examine the architecture of networks using the SIGTRAN protocols.

2) Interworking flows between the SIGTRAN network and the SS7 network

3) QoS and performance requirements for a SIGTRAN network.
To investigate whether the QoS parameters appropriate to signalling transport need to be defined for a managed IP network.
In addition, if this would be concluded, a mechanism may be investigated to provide this QoS within the IP network, for the lifetime of each signalling relation.

4) Architectures, provisioning rules and traffic parameters appropriate for the signalling transport recommended for services to be provided by the IP network.

5) QoS and performance requirements /recommendations for signalling using transport other than SIGTRAN in the IP network.

6) Availability requirements/recommendations of SIGTRAN and other IP network signalling.

7) Guidance on the security scheme to use with SIGTRAN IP network signalling, and how to achieve it.

NOTE: IPsec (see RFC 2406 [98] and RFC 2407 [99], also RFC 2401 [96], RFC 2404 [97] and RFC 2409 [100]) or optionally TLS (see RFC 2246 [95]) shall be used for SIGTRAN protocols. These can enable confidentiality or authentication (one at least must be used - authentication can use an RSA-like handshake + signature), and in addition encryption of the signalling information (using a symmetrical algorithm, so with the same key for encryption and decryption – the key is determined during the authentication phase. However, encryption *for use outside* the USA tends to be standard DES (albeit with CBC). It is possible this could be compromised in the near future, so a 128 bit key DES (3DES) or similar may be used instead. But will the US allow this outside the US? (See FIPS PUB 46-3 [101] and FIPS PUB 180-2 [102]).

12.2 IPv6 and IPv4 interconnection issues

ETSI needs to produce a deliverable to explain the issues and to provide a preference.

12.3 Management

OMAP (see ITU-T Recommendation Q.750 [52]) is used in SS7 networks for configuration, performance and fault management of MTP and SCCP. It is used also for monitoring and measurements of TC and ISUP. It allows network element management of MTP and SCCP from a network centre . These functions are also required for SG(P)s and AS(P)s (i.e. ~MGCs) where a managed IP network is carrying SS7 messages. RFC MIBs (or at least IETF draft MIBs) are being written, but they might need to be integrated into the MIBs of OMAP - this could result in a reduction in complexity and hence cost savings for managing the managed IP networks used to replace legacy networks.

ETSI may consider to produce a guide for integration of the management of the User Adaptation Layers' managed objects into existing networks' management, e.g. into the MTP and SCCP management based upon the ITU-T Recommendation Q.751.x series and EN 301 007 [5]. MIBs of SIGTRAN are for SNMP probably version 2 (RFCs 2578, 2579, 2580, 3410 and others, depending on whether it is the SCTP or M3UA draft MIB documents. And only M3UA and SCTP have draft MIBs).

12.4 Possible areas of further investigation in addition to the above

1) Whether to produce a deliverable which is the equivalent of ITU-T Recommendation Q.752 [55] for M2UA, M3UA, SUA and SCTP.

NOTE 1: SCTP and M3UA MIBs have a set of measurements for performance. But there is no equivalent to table 6 measurements of ITU-T Recommendation Q.752 [55], or to many other Q.752 items.

2) To study SUA to determine the effect on SCCP congestion/overload control mechanisms of combining a managed IP network part with an SCN part.

3) To study SUA to determine its effect upon route and network availability.

4) M3UA: how the SS7 flow, congestion and overload control mechanisms work between networks.
In particular, the interaction of the ISUP and SCCP congestion control mechanisms has been studied for SS7 networks to enable a fair flow control policy to be established. How the M3UA and SCTP parameters are to be set for the managed IP network, and how these affect the SS7 network flows, may need further investigation.

NOTE 2: The managed IP network has a potential to carry large amounts of message and call traffic, the time it takes to recognize a routeset failure or congestion is dependent upon the flow timer parameters used in the SCTP associations.

5) Level 2 flow control SCTP M2UA, and M2PA, MTP: how do these mechanisms interact, and what is the effect on the SS7 network.

6) Rules for setting timer values to detect link failure for SCTP.

NOTE: The time to detect link failure is well determined in SS7, and the rate of link failures. Taken together these factors are used in determining the network dimensions to give the required availability of the SS7 service. For SCTP the time to detect link failure depends upon the traffic patterns in the IP network and the retransmission timer values set for SCTP.

7) Loading of signalling links, effect upon signalling latency of IP network loading.

8) Mechanisms to ensure that signalling associations set up by SCTP for SIGTRAN protocols achieve the required QoS (e.g. if SCTP uses INTSERV or DIFFSERV or MPLS, how does this react?) .

9) Management system to define the correspondence between GT and IP address.

NOTE: For SUA (see [SUA]), messages can be routed on global title (GT) or on PC. GT Translation in the SCCP in the SCN translates E.164 numbers to DPC [+SSN] to route the message to the node and then the end subsystem. SUA performs a similar function, but here the result is ultimately an IP address. The function could be abbreviated to translate E.164 numbers directly to the SUA IP address. For IP telephony, DNS or ENUM (see RFC 2916 reference in Numbering and addressing section in the Bibliography, also RFC 2874 reference in IPv6 usage section) may be used, but for SUA, since performance requirements preclude use of an outside data base, this probably cannot be done. The performance requirements for SCCP are listed in ITU-T Recommendation Q.716 [51]), but this might need adaptation for SUA.

Annex A:
Security generalities

See TR 101 771 [18], "Crypt Analysis" and "Code Book" (bibliography).

Threats can be characterized as:

- Denial of service.
- Eavesdropping.
- Masquerade.
- Unauthorized access.
- Loss of information.
- Corruption of information.
- Repudiation.

Various mechanisms have been defined to protect against these threats, such as:

- Authentication:
  - with password;
  - with one-time password;
  - with secret key;
  - with digital signature;
- Access control;
- Virtual Private Network:
  - using access control, encryption and possibly Network Address Translation (NAT) for a Closed User Group (CUG) within a managed IP network.
- Secure configuration of Operating Systems (and Operations Systems);
- Secure configuration of networks:
  - access control to network elements, physical access control, entity authentication;
- Protection from Denial of Service (DOS) attacks on Hosts and media streams in IP networks:
  - filtering at network ingress by e.g. Firewalls;
  - filtering at network egress;
  - disable directed broadcast - but allow multicast to specific addresses;
  - media anti-spamming (H.323 v2) for RTP channels;
  - tools scanning for distributed drone software;

- Physical protection;
- Encryption for mobile subscribers and for IP networks:
  - symmetric algorithms, relying upon the same secret key for encrypting and decrypting (e.g. DES). These algorithms are typically much faster than antisymmetrical algorithms, but do rely upon the key remaining secret. In general the encryption algorithm and decryption algorithm use different but related functions. Some algorithms operate on a bit of the plaintext at a time, these are called stream ciphers. Other algorithms act on blocks of plaintext, these are called block ciphers.

NOTE: According to FIPS PUB 46-3 [101] section 12 "Single DES (i.e., DES) will be permitted for legacy systems only. New procurements to support legacy systems should, where feasible, use Triple DES products running in the single DES configuration." And in section 15 "With regard to the use of single DES, exhaustion of the DES (i.e., breaking a DES encrypted ciphertext by trying all possible keys) has become increasingly more feasible with technology advances. Following a recent hardware based DES key exhaustion attack, NIST can no longer support the use of single DES for many applications."

  - Antisymmetric algorithms, using a public key for encryption, and a private key for decryption (e.g. RSA) or vice versa for digital signatures.
    To sign data D, a hash function H known to sender and receiver alike is used by the sender upon D, producing H(D). The sender then uses private key P in his encryption algorithm to form P(H(D)) = S, and sends D+S. Only the sender can form S, since no-one else knows P. The receiver produces H(D), and uses public key K upon S in his decryption algorithm, to form K(P(H(D))), which should be the same as H(D). Thus, effectively, K is P^{-1}, although K cannot easily be inverted to produce P, because the operation P(H(D)) is effectively a one-way function. To avoid man in the middle attacks, the signature should employ a certificate from a trusted authority which states whose signature this is. So D should be augmented by this certificate before H acts on it.
  - Using an antisymmetric algorithm (with receiver's public key L) upon a private key A to be able to send key A to enable its use in a symmetric algorithm for data encryption and decryption during a session. The receiver decrypts L(A) with his private key Q, to form Q(L(A)), which is A. Only the receiver can decrypt L(A), because Q cannot be produced from inverting L, and Q is private to the receiver.
  - Using hardware or software. Signalling stream and media stream can use different encryption. Media stream encryption needs to consider lawful interception requirements.
  - Used during authentication.
- Intruder detection.
- Auditing and logging.

Annex B:
SCN details

B.1 Routeing in switched circuit networks

In a circuit switched network such as an ISDN, calls are routed from switch to switch, following the voice/data circuits used. In the circuit-associated case, the signalling and the transmission circuit follow the same path and each switch decides to which subsequent switch to route the call. The circuit's origin is at the exchange (and signalling end point) identified by the OPC, its termination is at the exchange identified by the DPC. The circuit is identified by the OPC, DPC and circuit identity (CIC) combination. The 4 least significant bits of the CIC value equal the SLS field value used by the MTP for load sharing.

The MTP uses the DPC for routeing messages, and at the message destination denoted by the DPC, the MTP distributes each message to the appropriate MTP User (e.g. ISUP) according to the value of the Service Indicator in the message's SIO field.

Some networks use "signalling transfer points" (STPs) in order to economize on the number of signalling links, and the signalling is then classified as "quasi-associated".

Networks may also use SCCP signalling relay points, which can perform SCCP routeing based on "Global Titles" (GTs). A GT could contain an E.164 number, it could, for instance, incorporate a calling subscriber's number when the freephone service is used, and when translated should provide the network address of the particular IN database to query for the called number. Or in GSM, the called subscribers identity may be used as a Global Title which when translated yields the network address of that subscriber's Home Location Register. The SCCP distributes messages at the SCCP end point according to the messages' SSN values in the SCCP called party address.

B.2 Signalling protocol stacks in a Time Division Multiplex SCN

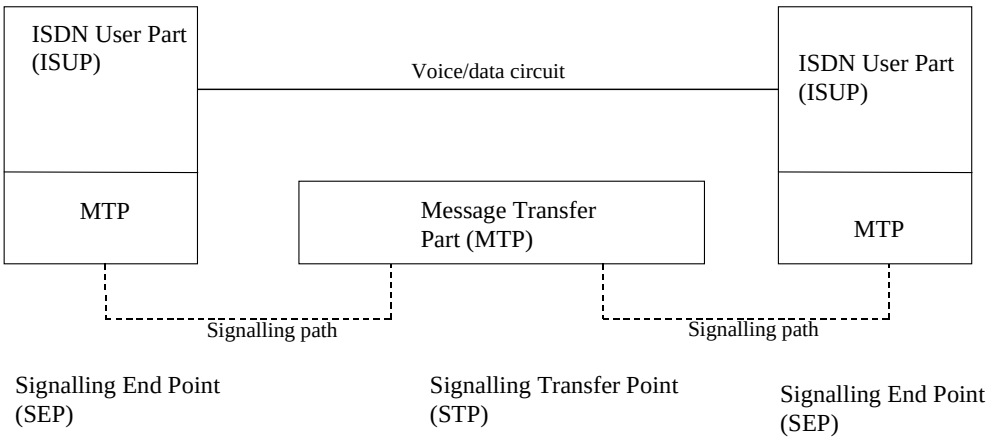


Figure B.1: Typical SS7 stacks for ISUP call control

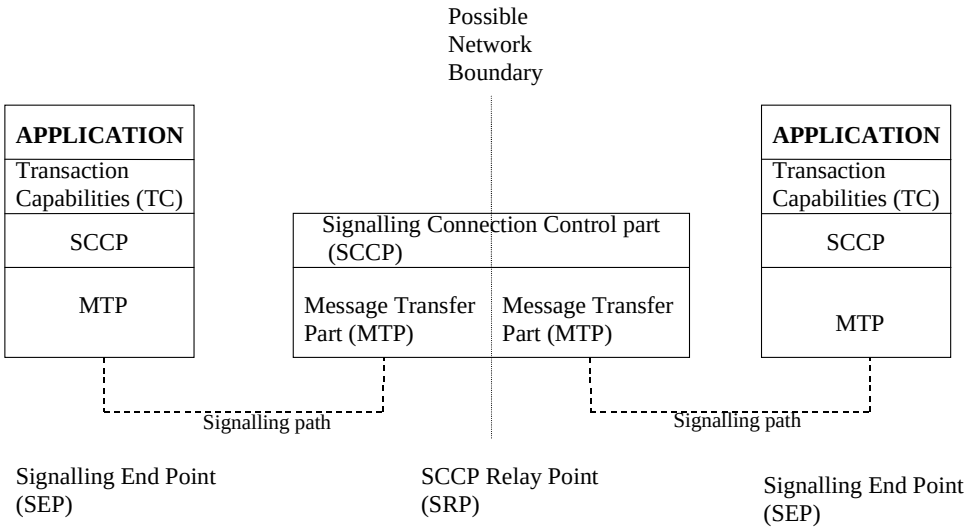


Figure B.2: Typical SS7 stacks for e.g. IN data base access

In the figure B.1, the signalling transport layer is the MTP. In figure B.2 it is the MTP + the SCCP.

B.3 ATM packet network instead of TDM

The ITU-T defined a variant of the MTP, MTP3b, to allow SS7 Users to signal over an ATM packet network. The ATM network emulates a circuit switched network by use of virtual switched circuits, identified by virtual channel and virtual path identifiers (VCIs and VPIs).

BICC (EN 301 848 [7], Q.1901 [32] and TRQ 2003 are standards developed in ITU-T and ETSI for signalling which is defined independently of the underlying transport layer. It is heavily based on ISUP. It relies upon a signalling transport service between it and the underlying transport layer (see ITU-T Recommendation Q.2150.0 [33]), and can run over narrow band or broad band MTP, ATM, or an IP network using SCTP over IP (v4 or v6).

Figure B.3 shows two possible protocol stacks for BICC used in an ATM network.(the figure indicates the transport adaptation layer service underneath BICC by a double line).

Figure B.4 shows a protocol stack used for SS7 Applications communicating over an ATM network.

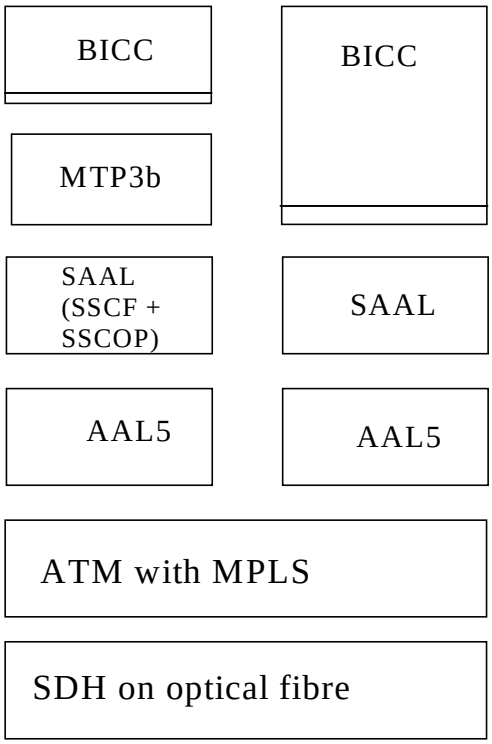


Figure B.3: Typical stacks for BICC over ATM

Here, the signalling transport layer includes the signalling transport service adaptation layer just underneath BICC (denoted by the double line in the BICC boxes), and everything underneath it for each protocol column.

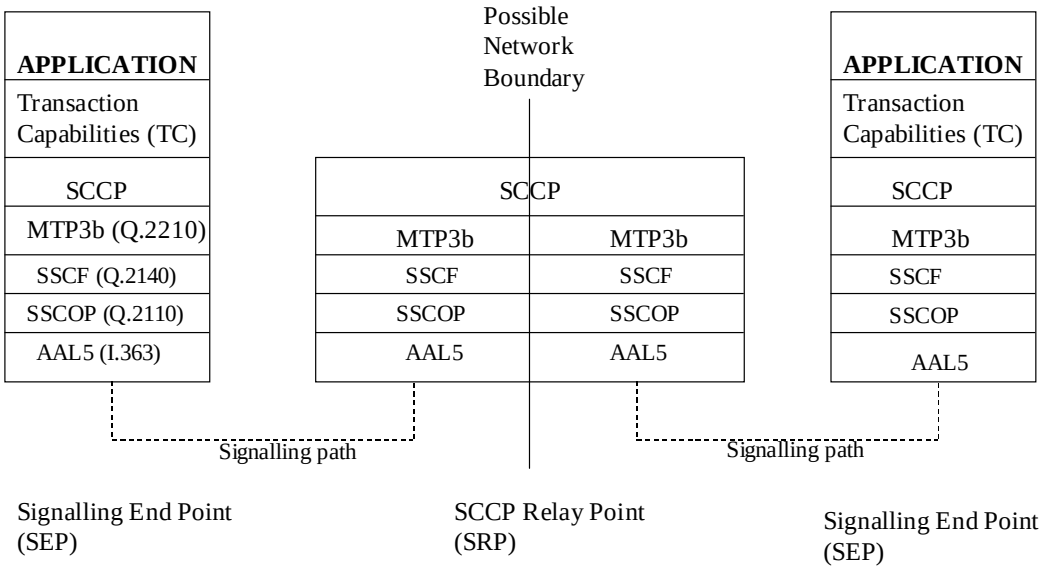


Figure B.4: Typical stacks for e.g. IN data base access over ATM

Here, the signalling transport layer includes the SCCP and everything below it. ITU-T Recommendation numbers are shown for each ATM layer and MPT3b.

B.4 Management and QoS of the signalling transport layer in SCN and ATM networks

B.4.1 Management

The following is extracted from ITU-T Recommendation Q.750 [52].

B.4.1.2 OMAP management categories

The purpose of management is to provide a service, and this can be classified as initial provisioning, maintaining existing service, and expansion or contraction of the service.

Management activities can be divided into categories which satisfy one or more of the above classifications.

OSI defines the categories of fault management, configuration management, performance management, accounting management and security management. Of these, the first three categories are applicable to OMAP.

B.4.1.2.1 Fault management for OMAP

OMAP fault management encompasses fault detection, location, isolation and the correction of abnormal operation of the SS No. 7 network. Correction of faults can in some instances require fault diagnosis. Faults can cause the network to fail to meet operational objectives (e.g. visible faults might reduce the network's traffic capacity, latent faults would reduce the network's reliability).

Fault management includes:

- handling of alarm conditions, e.g. the failure of a signalling linkset or the inaccessibility of a signalling point;
- the required interactions with resources of other TMN parts (e.g. transmission failures causing signalling link failures need to be correlated);
- The activation of measurements or tests. These include certain ITU-T Recommendation Q.752 [55] defined measurements, and the MTP route verification test.

B.4.1.2.2 Configuration management

Configuration management controls the resources of, and collects and provides data for, the signalling network and its components. This facilitates the preparation for, and initialization of, signalling services, and allows such services to be started, continued, and stopped.

Two main activities can be distinguished:

- setting the static configuration in the SS No. 7 network (e.g. installing and initializing SS No. 7 components); and
- altering the configuration of the network while it is running, and providing information about its changing state.

The particular facilities provided are defined by the operations applicable to, and the behaviour of, the managed objects defined in the ITU-T Recommendation Q.751-series of Recommendations.

B.4.1.2.3 Performance management

This enables the behaviour of network resources and the effectiveness of communication activities in the network to be evaluated.

Functions to gather statistics, maintain and read logs of the network and system state histories, and to determine network performance under normal and abnormal conditions are provided.

Certain system parameters may be altered in order to monitor and change the performance of the network.

Network performance can be optimized by monitoring and managing the network.

Performance management functions include:

1) collection of measurements to enable long and short term control:

   a) alarm monitoring;

   b) activation of certain Recommendation Q.752 [55] measurements;

   c) provision of network information from these measurements regarding resource usage, e.g. route utilization;

2) medium term control of resources, e.g.:

   d) modification of linkset capacity (e.g. increasing the number of active links);

   e) modification of route capacity (e.g. coordinated increase in constituent linkset sizes);

   f) timer adjustments;

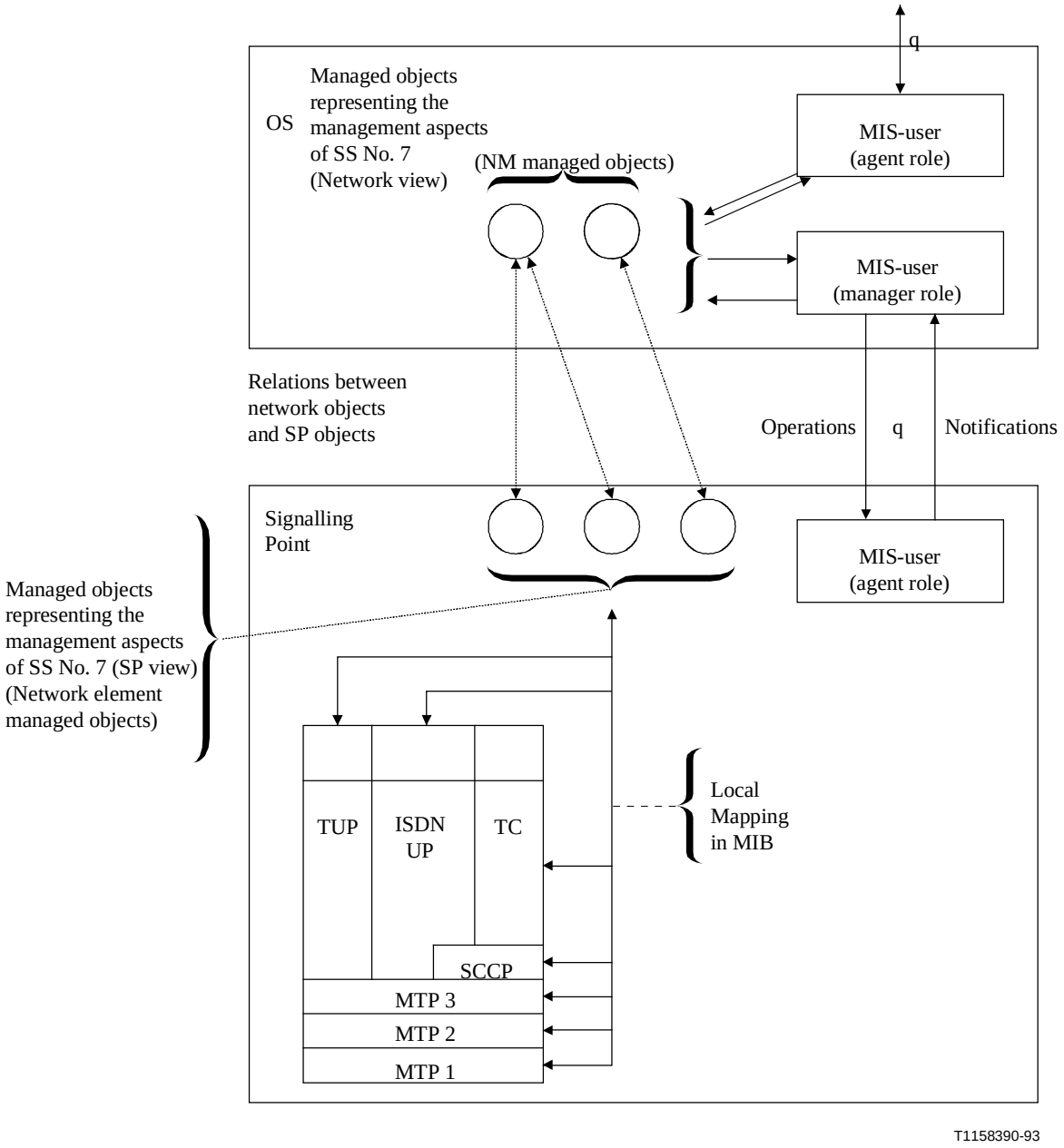
3) real time control of message and traffic flows in the network, e.g.:

   a) real time adjustment of routing tables (e.g. changing time of day routing);

   b) activation of additional signalling links or linkset.

ITU-T Recommendation X.731 [73] defines the OSI state management function. Each OMAP managed object's "OSI state" (i.e. the state perceived for its management) is defined as part of the object behaviour definition in the Q.751-Series of Recommendations. If the managed object has a "functional state" defined, then the mapping between functional state and OSI state is also part of the object definition. Informal descriptions of behaviour use text; SDL is used for a more formal description.

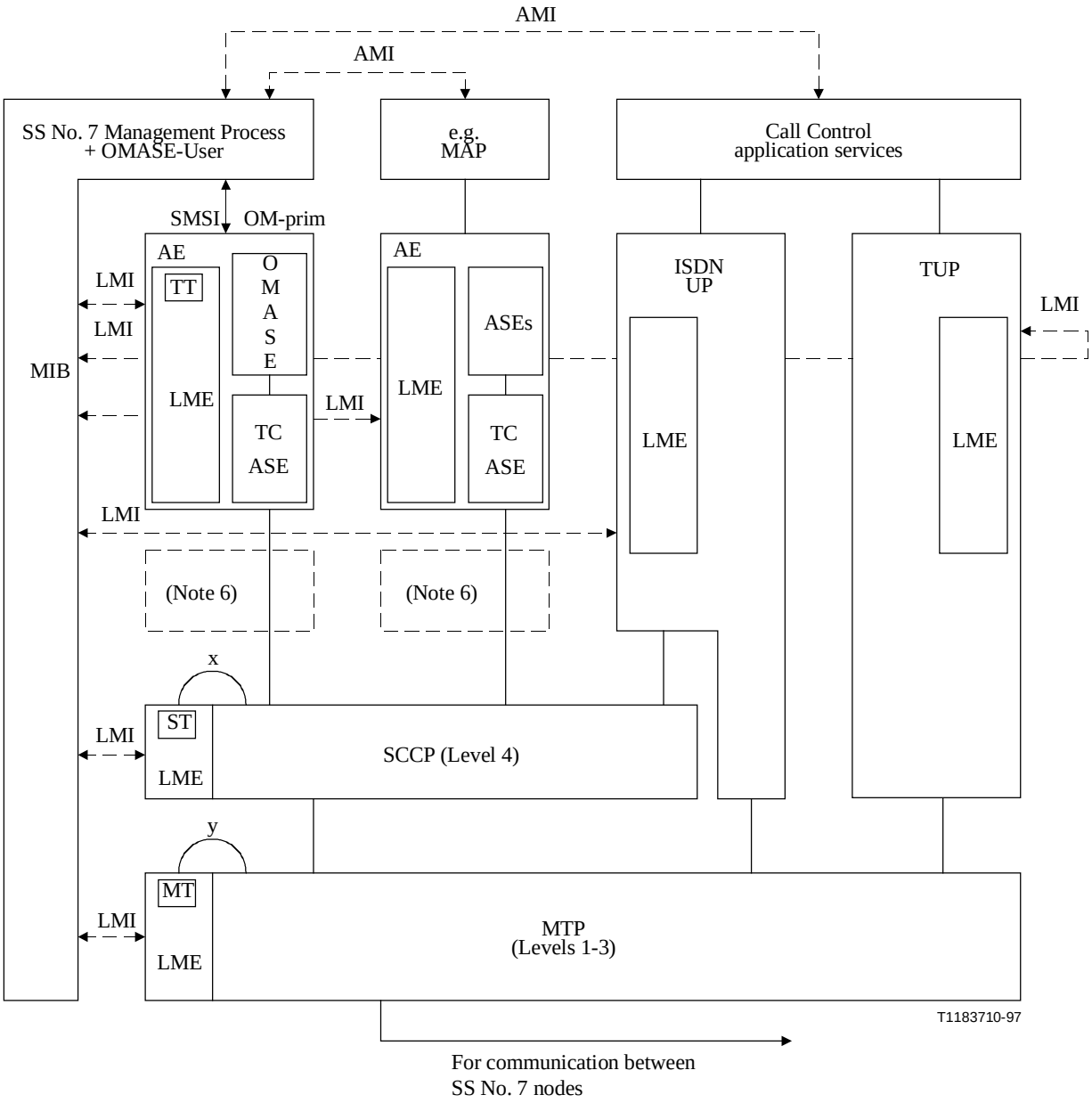
OSI systems management (see ITU-T Recommendation X.701 [72] for example) defines a model of management, and this model is employed in OMAP. The model is used for most of the OMAP managed objects. Figure B.4.1 (which is the same as figure 3/Q.750 [52]) shows this model.



MIS Management Information Service

Figure B.4.1: Classical OMAP managed objects model

The detailed picture of OMAP at a signalling point is shown in figure B.4.2 (which is the same as figure 5/Q.750 [52]).



NOTE 1: Dotted lines (but not boxes) denote direct management interfaces. Only the SMSI (see note 5) is realized with primitives.
NOTE 2: The LMI (Level Management Interface) is not a subject for standardization.
NOTE 3: The AMI (Application Management Interface) is not a subject for standardization.
NOTE 4: The items managed by OMAP can be regarded as conceptually resident in the MIB.
NOTE 5: The SMSI is the systems management service interface, the OM primitives are defined for use over it for managed object functions defined in ITU-T Recommendation Q.753 [56].
NOTE 6: OSI layers 4, 5 and 6 are null in SS No. 7. TC forms the bottom of OSI layer 7; SCCP the top of OSI layer 3 (but is in SS No. 7 level 4).
NOTE 7: Interface x uses sub-system number to test the SCCP using the SCCP Tester (ST); interface y uses SIO to test the MTP using the MTP Tester (MT). The TC Test Responder (TT) has its own SSN, conceptually it resides in the OMAP LME.
NOTE 8: The LME (Level Management Entity) is defined for management of and within each level of SS No. 7. This is conceptually where each managed item resides as far as the level is concerned.

Figure B.4.2: SS7 stack and management by OMAP at a signalling point

Here the transport layer management information base is defined in the Q.751.x series of ITU-T Recommendations. ITU-T Recommendations Q.753 [56] and Q.754 [57] define the OMAP functions for the MTP Routeing Verification Test (MRVT) and the SCCP RVT (SRVT) which are used in some networks to audit the network routeing tables for the MTP and SCCP respectively. ITU-T Recommendation Q.752 [55] defines the SS7 monitoring and measurements.

B.4.2 QoS and congestion

B.4.2.1 Congestion

MTP link congestion in an SCN is detected and handled as follows:
Receiver congestion causes the link to transmit a "busy" indication to the sending end, and a timer is started there, which, if it expires, cause the link to be taken out of service and changeover occurs.
The transmitting side of a link has a transmission buffer, containing messages waiting to be sent for the first time, and a retransmission buffer containing those messages sent but not yet acknowledged at level 2. Congestion onset and abatement thresholds are set (either for transmission buffer and retransmission buffer separately, or combined, or for one and not the other, depending upon implementation), which determine the congestion status of the link (and hence an implied status of the linkset and routeset(s) for which the link carries messages). If the transmitting side of a link detects receiver congestion at the other end, MTP level 3 is informed. The congestion onset and abatement thresholds are set to avoid oscillation between congested and uncongested states, and to allow MTP users (either local or remote) to be informed in sufficient time for them to reduce traffic.

In addition, there is at MTP level 2 a timer for the expected delay to acknowledge a message. If this timer expires, the link is taken out of service, and changeover occurs.

Note that, although congestion on a link or linkset or routeset might occur, this of itself does not cause rerouteing.

If congestion occurs on a routeset, the signalling point informs its local users (and remote users sending it messages if it is an STP), so that they can reduce message traffic (the MTP message traffic can be reduced by reducing the number of calls or transactions being supported by the MTP).

ITU-T Recommendation Q.752 [55] contains measurements for congestion events.

B.4.2.2 QoS

The Implementors' Guide (12/99) for Q.706 [41] (ITU-T Recommendation COM 11-R 205-E [38]) provides in figures 5/Q.706 [41] and 6/Q.706 [41] values for the mean and standard deviation of the total queueing delay for each channel of traffic on a signalling link against the signalling link loading, for a number of MSU total (i.e. level 2) sizes between 15 and 279 octets, for MSU error probabilities of 0 and 0,001, and for the signal unit error probability of 0,004 at which the signalling link will fail. The details of the calculations are shown in annex B.

According to ITU-T Recommendation E.733 [4], the M/G/1 model used in ITU-T RecommendaQ 706 is an acceptable approximation to give the queueing delay of a link providing certain assumptions are met. These are:

1) a Poisson call arrival process is a good approximation to the actual call arrival process; and

2) the time separation between messages in the same direction associated with the call are greater than 1 second for most calls. (This stops the known message correlation affecting significantly the queueing behaviour of the M/G/1 model); and

3) the Signalling Point processing does not distort significantly the message inter arrival times (no significant batching or smoothing of these times); and

4) no more than 10 % to 20 % of any one signalling link's load is sent to the link under investigation, and no one link contributes more than 10 % to 20 % of the load on this link.

With these assumptions, the queueing model of Q.706 IG [42] may be extended to provide the STP or SCCP relay point message transfer time. Using this, the message transit time and transit time variation across the SS7 network may be estimated. See ITU-T Recommendation Q.709 [45] for more information.

As an example, the STP delay and standard deviation through a typical STP for MSUs of length 57 octets (MTP level 2 length) is given in figure B.4.3. This calculation uses an M/G/1 model for calculating the delay to service the STP's incoming link, another M/G/1 model for the delay to service the outgoing link, and an approximation to a G/G/1 model for the delay to emission of the MSU on to the outgoing link from the transmission queue (see Q. 706 IG [42] and Kleinrock). The model's parameters have been adjusted to give the table 5/Q.706 message transfer times of 20 ms. for the mean delay, and 40 ms for the 95 percentile, at a "normal" signalling traffic load of 0,5 Erlang per link. The total delays to the MSU in its progress through the SS7 network may be estimated with such nodal delays in a similar fashion as for an IP network in ITU-T Recommendation Y.1541 [110].

The delay through an SCCP relay point may be calculated in an analogous way to the delay through an STP, provided that the details of additional delays for performing global title translation are fed into the model (GTT delay depends for example on the depth of GTT translation i.e. the point at which the next DPC to which the message should be sent is determined. If an external data base is used or number portability is a consideration, these need to be factored-in).

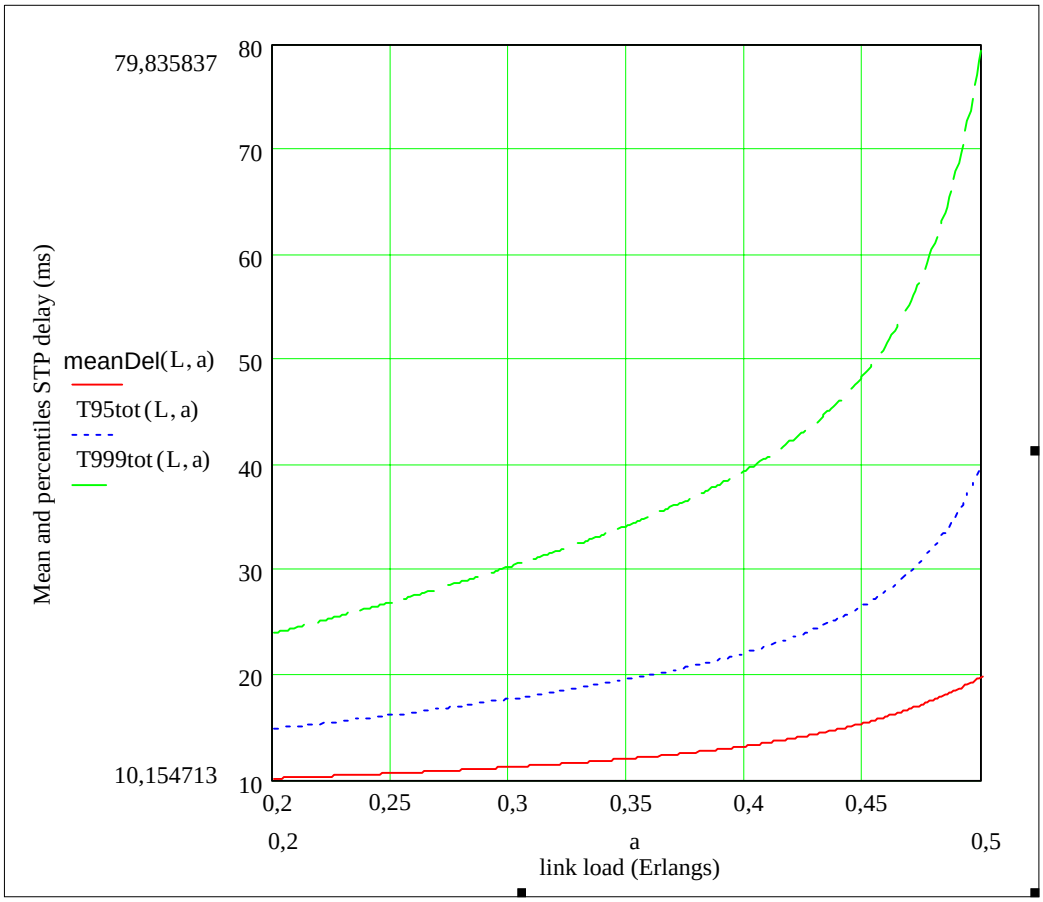


Figure B.4.3: typical mean, 95 and 99.9 percentiles STP delay for 57 octet MSUs

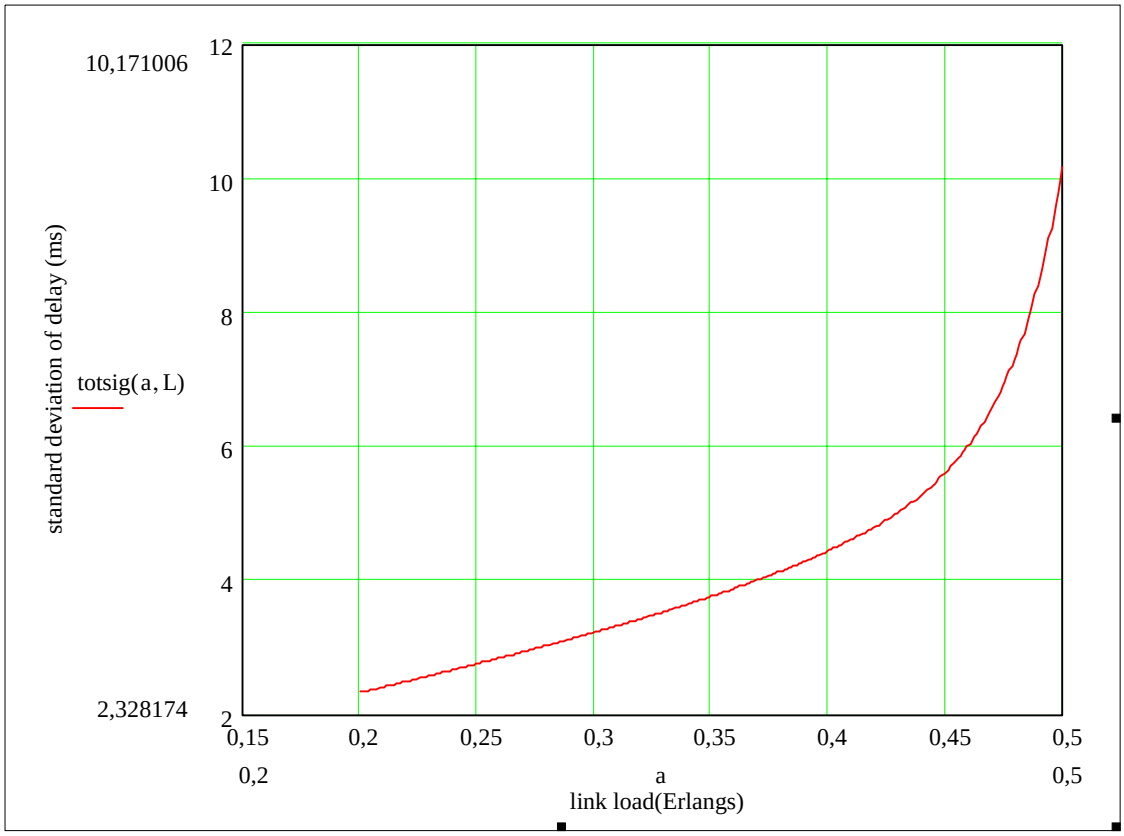


Figure B.4.4: Typical standard deviation for STP delay for 57 octet MSUs

The MSU delay, and delay variation, across a network containing an origin signalling endpoint, a number of STPs and a destination signalling endpoint can then be estimated.

This performance contributes to the delay to setup of a call of < ~500 ms, given that the cross office delay for an IAM is ~150 ms, (see ITU-T Recommendation Q.766 [62]).

Such calculations could produce figures corresponding to those of Y.1541 [110], and help to choose the QoS class needed for signalling transport within the IP network, as well as providing the bounds of the QoS required.

Annex C:
IP network details

C.1 Design

There are only a few managed IP networks at present. Most are not interconnected with each other, since there is no single agreement on standards between networks.

The network topology is determined by the physical cables, fibres or radio links between nodes.

- At the physical level (layer 1) the Synchronous Digital Hierarchy (SDH) is used to subdivide the capacity on the cable fibres and to provide basic fault monitoring. At nodes cross connects may be used to interconnect different units of capacity on different cables.
- At the link level (layer 2) a packet system time - shares capacity on the topology created by SDH. This is either ATM using short fixed length cells, or the frame relay system using longer, variable length, frames. The ATM links connect ATM routers that switch ATM cells in accordance with a link identifier called a virtual path - virtual channel combination (VPI/VCI).
- At the network level (layer 3), traffic between end users is sent in IP packets that are routed by IP routers according to the IP address of the destination.

IP packets can be carried on ATM over SDH or they can be carried directly on SDH, i.e. layer 2 can be null.

SDH is also not essential, and routers that put IP packets directly into optical modulators are being developed.

C.2 IPv6 details

C.2.1 Neighbour discovery

Nodes within the IPv6 network make use of a set of procedures called Neighbor Discovery (RFC 2461 [87]), which allow routeing tables within host and router nodes to be updated.

Neighbor Discovery classifies addresses further into:

1) all-nodes multicast address - the link-local scope address to reach all nodes (FF02::1, see below for an explanation of the structure of the address).
2) all-routers multicast address - the link-local scope address to reach all routers (FF02::2).
3) solicited-node multicast address - a link-local scope multicast address that is computed as a function of the solicited target's address. The function is chosen so that IP addresses which differ only in the high-order bits, e.g., due to multiple high-order prefixes associated with different providers, will map to the same solicited-node address hence reducing the number of multicast addresses a node must join.
4) link-local address - a unicast address having link-only scope that can be used to reach neighbours. All interfaces on routers must have a link-local address. Also, it is required that interfaces on hosts have a link-local address.

Neighbor Discovery enables the following:

- Hosts to locate routers that reside on an attached link (router discovery).
- Hosts to discover the set of address prefixes that define which destinations are on-link for an attached link (Prefix Discovery). Nodes use prefixes to distinguish destinations that reside on-link from those reachable only through a router.

- A node to learn such link parameters as the link MTU or such Internet parameters as the hop limit value to place in outgoing packets (parameter discovery).
- Nodes to configure automatically an address for an interface (address autoconfiguration).
- Nodes to determine the link-layer address of an on-link destination (e.g. a neighbour) given only the destination's IP address (address resolution).
- Next-hop determination, which is the algorithm for mapping an IP destination address into the IP address of the neighbour to which traffic for that destination should be sent. The next-hop can be to a router or to the destination itself.
- Nodes to determine that a neighbour is no longer reachable (Neighbor Unreachability Detection). For neighbours used as routers, alternate default routers can be tried. For both routers and hosts, address resolution can be performed again.
- A node to determine that an address it wishes to use is not already in use by another node (duplicate address detection).
- A router to inform a host of a better first-hop node to reach a particular destination, if such exists (redirect).

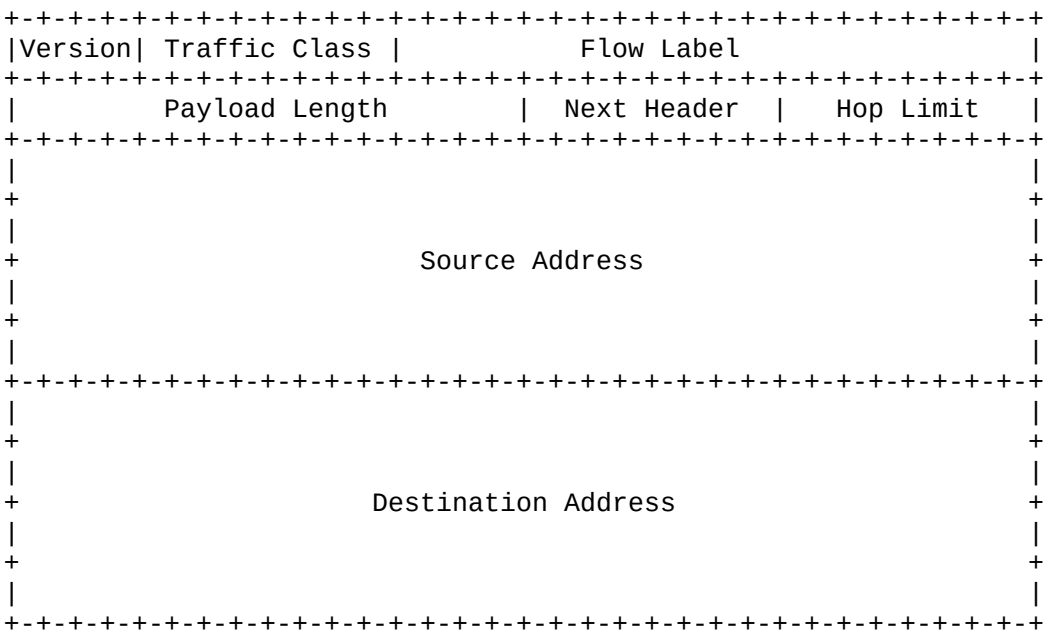
C.2.2 Routeing of packets

Routeing information is held in Destination cache, Prefix list and Neighbour cache entries and used at a node until the cached information is suspected to be in error. At a host, each time that an upper layer protocol hands a message packet to the IP layer, the IP layer examines its Destination cache to see if an entry exists for that destination. If not, the next hop is determined by comparing the packet's address against the Prefix list to match the longest prefix there. If the destination is on-link, the next hop is the packet's destination. If not, the router to use is selected from the Default router list for this destination. The next hop information is then written into the cache. Having obtained the IP address of the next hop, if it is of type unicast, the Neighbour cache is examined for the link-layer information of the neighbour (e.g. its physical link identity). Address resolution is required if there is no neighbour information for this IP address. The message is sent once the link is determined.

The IP layer uses information from some of its higher layers (e.g. TCP) that its addresses are still reachable. IP sends a Neighbor Solicitation message if it suspects that a neighbour is unreachable, and a Neighbor Advertisement message is expected in reply. Nodal parameters are defined as to the frequency of this test, in the absence of higher layer assurance.

C.2.2.1 IPv6 headers and extension headers

The format of the IPv6 header is:

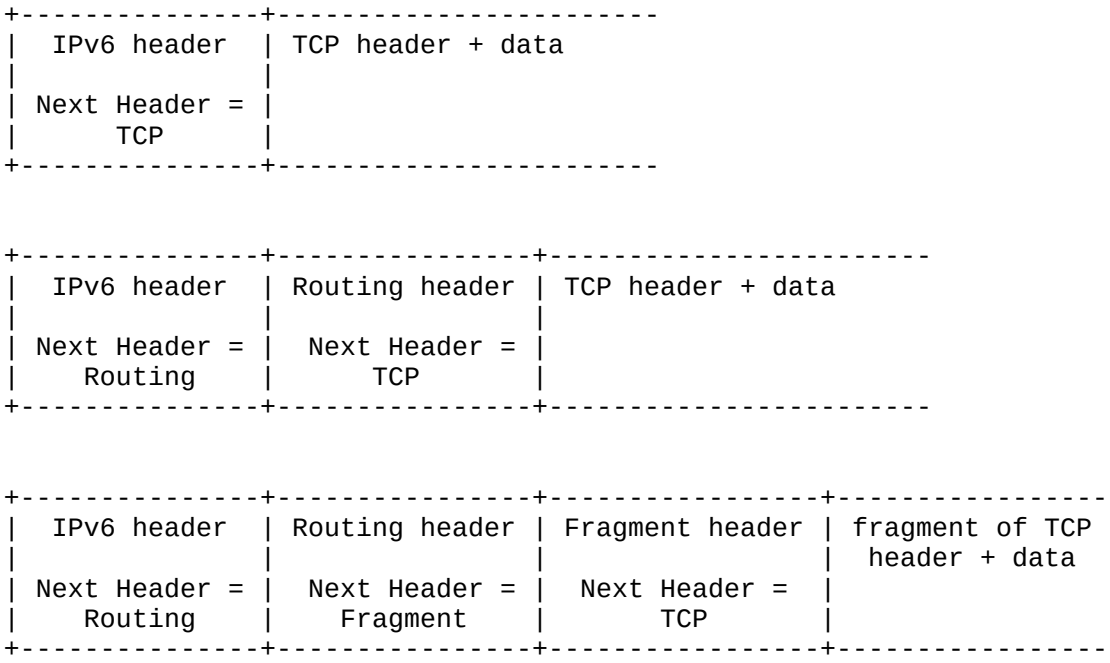


Version:	4-bit Internet Protocol version number = 6
Traffic Class	8-bit traffic class field. Marked as experimental in the RFC. Could be used for e.g. DIFFSERV (RFC 2474 [83])
Flow Label	20-bit flow label. Marked as experimental in the RFC. Could be used for e.g. special QoS (e.g. real time)
Payload Length	16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets.

NOTE: Any extension headers present are considered part of the payload, i.e. included in the length count.

Next Header	8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field
Hop Limit	8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero
Source Address	128-bit address of the originator of the packet
Destination Address	128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

The extension headers are used as shown:



Apart from the Hop-by-Hop Options header, extension headers are not examined or processed by any node along a packet's delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header.

There, normal demultiplexing on the Next Header field of the IPv6 header invokes the module to process the first extension header, or the upper-layer header if no extension header is present. The contents and semantics of each extension header determine whether or not to proceed to the next header. Therefore, extension headers must be processed strictly in the order they appear in the packet.

The Hop-by-Hop Options header carries information that must be examined and processed by every node along a packet's delivery path, including the source and destination nodes. When present, it must follow immediately the IPv6 header. Its presence is indicated by the value zero in the Next Header field of the IPv6 header.

If the upper-layer header is another IPv6 header (in the case of IPv6 being tunnelled over or encapsulated in IPv6), it may be followed by its own extension headers.
The following extension headers exist:

1) Hop-by-Hop Options.

2) Routing. Used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. Identified by a Next Header value of 43 in the immediately preceding header.

3) Fragment. Used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination.

NOTE: Fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.) Identified by a Next Header value of 44 in the immediately preceding header.

4) Destination Options. Used to carry optional information that need be examined only by a packet's destination node(s). Identified by a Next Header value of 60 in the immediately preceding header.

5) Authentication. See RFC 2406 [98].

6) Encapsulating Security Payload. See RFC 2406 [98].

C.3 SCTP details

See RFC 2960 [77], RFC 3257 [80], RFC 3309 [78] and TS 102 144 [76].

C.3.1 Architectural View of SCTP

SCTP is viewed as a layer between the SCTP user application and a connectionless packet network service such as IP.

The basic service offered by SCTP is the reliable transfer of user messages between peer SCTP users. It performs this service within the context of an association between two SCTP endpoints.

SCTP is connection-oriented in nature. SCTP provides the means for each SCTP endpoint to provide the other endpoint (during association startup) with a list of transport addresses (i.e. multiple IP addresses in combination with an SCTP port) through which that endpoint can be reached and from which it will originate SCTP packets. The association spans transfers over all of the possible source/destination combinations which may be generated from each endpoint's lists.

C.3.2 Functional view of SCTP

The SCTP transport service can be decomposed into a number of functions. These are association startup and teardown, sequenced delivery within streams, User data fragmentation where necessary, acknowledgements and avoidance of congestion, chunk bundling, packet validation and path management.

C.3.3 Association startup and takedown

An association is initiated by a request from the SCTP user.

A cookie mechanism is employed during the initialization to provide protection against security attacks. The cookie mechanism uses a four-way handshake, the last two legs of which are allowed to carry user data for fast setup.

SCTP provides for graceful shutdown of an active association on request from the SCTP user. SCTP also allows the association to be aborted, either on request from the user (ABORT primitive) or as a result of an error condition detected within the SCTP layer.

When either endpoint performs a shutdown, the association on each peer stops accepting new data from its user and only delivers data in the queue at the time of the graceful close.

C.3.4 Sequenced delivery within streams

The term "stream" is used in SCTP to refer to a "pipe" which carries sequences of user messages that are to be delivered to the upper-layer protocol in order with respect to other messages within the same stream.

The SCTP user can specify at association startup time the number of streams to be supported by the association. This number is negotiated with the remote end. User messages (SEND, RECEIVE primitives) are associated with stream numbers. Internally, SCTP assigns a stream sequence number to each message passed to it by the SCTP user. On the receiving side, SCTP ensures that messages are delivered to the SCTP user in sequence within a given stream. However, while one stream may be blocked waiting for the next in-sequence user message, delivery from other streams may proceed.

SCTP provides a mechanism for bypassing the sequenced delivery service. User messages sent using this mechanism are delivered to the SCTP user as soon as they are received.

C.3.5 User data fragmentation

When needed, SCTP fragments user messages to ensure that the SCTP packet passed to the lower layer conforms to the path MTU. On receipt, fragments are reassembled into complete messages before being passed to the SCTP user.

C.3.6 Acknowledgement and congestion avoidance

SCTP assigns a Transmission Sequence Number (TSN) to each user data fragment or unfragmented message. The TSN is independent of any stream sequence number assigned at the stream level. The receiving end acknowledges all TSNs received, even if there are gaps in the sequence. In this way, reliable delivery is kept functionally separate from sequenced stream delivery.

The acknowledgement and congestion avoidance function is responsible for packet retransmission when timely acknowledgement has not been received. Packet retransmission is conditioned by congestion avoidance procedures similar to those used for TCP.

C.3.7 Chunk bundling

The SCTP packet as delivered to the lower layer consists of a common header followed by one or more chunks.

Each chunk may contain either user data or SCTP control information. The SCTP user has the option to request bundling of more than one user messages into a single SCTP packet. The chunk bundling function of SCTP is responsible for assembly of the complete SCTP packet and its disassembly at the receiving end.

During times of congestion an SCTP implementation may still perform bundling even if the user has requested that SCTP not bundle. The user's disabling of bundling only affects SCTP implementations that may delay a small period of time before transmission (to attempt to encourage bundling). When the user layer disables bundling, this small delay is prohibited but not bundling that is performed during congestion or retransmission.

C.3.8 Packet validation

A mandatory Verification Tag field and a 32 bit checksum field are included. The Verification Tag value is chosen by each end of the association during association startup. Packets received without the expected Verification Tag value are discarded, as a protection against blind masquerade attacks and against stale SCTP packets from a previous association. The checksum should be set by the sender of each SCTP packet to provide additional protection against data corruption in the network. The receiver of an SCTP packet with an invalid checksum silently discards the packet.

C.3.9 Path management

The sending SCTP user is able to manipulate the set of transport addresses used as destinations for SCTP packets. The SCTP path management function chooses the destination transport address for each outgoing SCTP packet based on the SCTP user's instructions and the currently perceived reachability status of the eligible destination set. The path management function monitors reachability through heartbeats when other packet traffic is inadequate to provide this information and advises the SCTP user when reachability of any far-end transport address changes. The path management function is also responsible for reporting the eligible set of local transport addresses to the far end during association startup, and for reporting the transport addresses returned from the far end to the SCTP user.

At association start-up, a primary path is defined for each SCTP end-point, and is used for normal sending of SCTP packets.

On the receiving end, the path management is responsible for verifying the existence of a valid SCTP association to which the inbound SCTP packet belongs before passing it for further processing.

C.4 TCP details

Taken from RFC 793 [106].

C.4.1 Communication using TCP

A stream of data sent on a TCP connection is delivered reliably and in order at the destination.

Transmission is made reliable via the use of sequence numbers and acknowledgments. Conceptually, each octet of data is assigned a sequence number. The sequence number of the first octet of data in a segment is transmitted with that segment and is called the segment sequence number. Segments also carry an acknowledgment number which is the sequence number of the next expected data octet of transmissions in the reverse direction. When TCP transmits a segment containing data, it puts a copy on a retransmission queue and starts a timer; when the acknowledgment for that data is received, the segment is deleted from the queue. If the acknowledgment is not received before the timer runs out, the segment is retransmitted.

An acknowledgment by TCP does not guarantee that the data has been delivered to the end user, but only that the receiving TCP has taken the responsibility to do so.

To govern the flow of data between TCPs, a flow control mechanism is employed. The receiving TCP reports a "window" to the sending TCP. This window specifies the number of octets, starting with the acknowledgment number, that the receiving TCP is currently prepared to receive.

C.4.2 Connection establishment and clearing

To identify the separate data streams that TCP may handle, TCP provides a port identifier. Since port identifiers are selected independently by each TCP instance they might not be unique. To provide for unique addresses within each TCP instance, an internet address identifying the TCP instance is concatenated with a port identifier to create a socket which is unique throughout all networks connected together.

A connection is fully specified by the pair of sockets at the ends. A local socket may participate in many connections to different foreign sockets. A connection can be used to carry data in both directions, that is, it is "full duplex".

TCP instances are free to associate ports with processes however they choose. However, several basic concepts are necessary in any implementation. There must be well-known sockets which the TCP associates only with the "appropriate" processes by some means. Processes may "own" ports, and processes can initiate connections only on the ports they own.

A connection is specified in the OPEN call by the local port and foreign socket arguments. In return, the TCP supplies a (short) local connection name by which the user refers to the connection in subsequent calls. The OPEN call also specifies whether the connection establishment is to be actively pursued, or to be passively waited for.

There are several things that must be remembered about a connection. To store this information assume there is a data structure called a Transmission Control Block (TCB).

A passive OPEN request means that the process wants to accept incoming connection requests rather than attempting to initiate a connection. Often the process requesting a passive OPEN will accept a connection request from any caller. In this case a foreign socket of all zeros is used to denote an unspecified socket. Unspecified foreign sockets are allowed only on passive OPENs.

A service process that wished to provide services for unknown other processes would issue a passive OPEN request with an unspecified foreign socket. Then a connection could be made with any process that requested a connection to this local socket. It would help if this local socket were known to be associated with this service.

Well-known sockets are a convenient mechanism for a priori associating a socket address with a standard service. For instance, the "Telnet-Server" process is permanently assigned to a particular socket, and other sockets are reserved for File Transfer, Remote Job Entry, etc. A socket address might be reserved for access to a "Look-Up" service which would return the specific socket at which a newly created service would be provided. The concept of a well-known socket is part of the TCP specification, but the assignment of sockets to services is outside the TCP specification.

Processes can issue passive OPENs and wait for matching active OPENs from other processes and be informed by TCP when connections have been established. Two processes which issue active OPENs to each other at the same time will be correctly connected.

There are two principal cases for matching the sockets in the local passive OPEN and a foreign active OPEN. In the first case, the local passive OPEN has fully specified the foreign socket. In this case, the match must be exact. In the second case, the local passive OPEN has left the foreign socket unspecified. In this case, any foreign socket is acceptable as long as the local sockets match. Other possibilities include partially restricted matches.

If there are several pending passive OPENs (recorded in TCBs) with the same local socket, a foreign active OPEN will be matched to a TCB with the specific foreign socket in the foreign active OPEN, if such a TCB exists, before selecting a TCB with an unspecified foreign socket.

The procedures to establish connections utilize the synchronize (SYN) control flag and involves an exchange of three messages. This exchange has been termed a three-way hand shake.

A connection is initiated by the rendezvous of an arriving segment containing a SYN and a waiting TCB entry each created by a user OPEN command. The matching of local and foreign sockets determines when a connection has been initiated. The connection becomes "established" when sequence numbers have been synchronized in both directions.

The clearing of a connection also involves the exchange of segments, in this case carrying the FIN control flag.

C.4.3 Data communication

The data that flows on a connection may be thought of as a stream of octets. The sending user indicates in each SEND call whether the data in that call (and any preceding calls) should be immediately pushed through to the receiving user by the setting of the PUSH flag.

A sending TCP is allowed to collect data from the sending user and to send that data in segments at its own convenience, until the push function is signalled, then it must send all unsent data. When a receiving TCP sees the PUSH flag, it must not wait for more data from the sending TCP before passing the data to the receiving process.

There is no particular relationship between push functions and segment boundaries. The data in any particular segment may be the result of a single SEND call, in whole or part, or of multiple SEND calls.

The purpose of the push function and the PUSH flag is to push data through from the sending user to the receiving user. It does not provide a record service.

There is a coupling between the push function and the use of buffers of data that cross the TCP/user interface. Each time a PUSH flag is associated with data placed into the receiving user's buffer, the buffer is returned to the user for processing even if the buffer is not filled. If data arrives that fills the user's buffer before a PUSH is seen, the data is passed to the user in buffer size units.

TCP also provides a means to communicate to the receiver of data that at some point further along in the data stream than the receiver is currently reading there is urgent data. TCP does not attempt to define what the user specifically does upon being notified of pending urgent data, but the general notion is that the receiving process will take action to process the urgent data quickly.

C.4.4 Precedence and security

TCP makes use of the internet protocol type of service field and security option to provide precedence and security on a per connection basis to TCP users. Not all TCP modules will necessarily function in a multilevel secure environment; some may be limited to unclassified use only, and others may operate at only one security level and compartment. Consequently, some TCP implementations and services to users may be limited to a subset of the multilevel secure case.

TCP modules which operate in a multilevel secure environment must properly mark outgoing segments with the security, compartment, and precedence. Such TCP modules must also provide to their users or higher level protocols such as Telnet an interface to allow them to specify the desired security level, compartment, and precedence of connections.

C.5 Routeing in IP networks

C.5.1 Routeing in the public Internet

In the public Internet, there is normally a two stage process for general routeing (the special arrangements for SIP and H.323 are described elsewhere). Most communications are established in a client to server mode, e.g. access to an email server or a web site, where the called host has a fixed IP address:

- The first stage determines the IP address of the called host. The calling host of the client uses the public domain name system (DNS) to resolve the Internet name for the host at the distant end into a public IP address.
- Packets are sent to the called host's IP address and each router routes the packets according to routeing tables. Because the IP addresses use aggregation and reflect the connection topology of the Internet, the size of the routeing tables is kept to manageable proportions.

This arrangement works satisfactorily where clients (e.g. users' PCs) have IP addresses that are assigned dynamically by their ISP, because the communications sessions are always established from the client to the host and the only incoming communications to the client come from a host that the client has first accessed.

C.5.2 Managed IP networks

Managed IP networks at present are not usually interconnected with each other for telephony or other services at the IP level, although they may have interconnection to the SCNs and to the Internet. Their main use is to provide VPNs and interconnection between LANs at different sites within an organization. There may be some connections between customers of the same managed IP network.

Managed networks normally use compatible products from a single vendor. Currently, these products are based on either SIP or H.323 with proprietary additions.

C.6 The Internet

C.6.1 Firewalls and NATS

C.6.1.1 Firewalls

A firewall separates administration zones and enforces network security. This is achieved by allowing packets to flow from one side of the firewall to the other, or by preventing them, depending upon IP address, port number and protocol.

Firewalls are usually divided into two groups:

- packet filtering firewalls that are usually implemented in routers or other network components; and
- application gateways that are implemented on computers.

The main difference between the two is that the first type of firewall is part of the IP infrastructure and can control the traffic at network level. The second type works at the application level, and thus has much finer control, but is restricted to single applications. A firewall system consists of both types of firewall working in conjunction to control all traffic entering and leaving the network.

For VoIP, application firewalls are necessary, since VoIP applications make heavy use of dynamically allocated port addresses and so it is impossible to control traffic with just a filtering firewall.

For a firewall to operate effectively, it must sit in series with the network connection between the protected network and the unprotected network. A firewall hence sits in the signalling and media path of a VoIP session that crosses the boundary between a protected (e.g. private) network and an unprotected (e.g. public) network. This can create problems by allowing TCP sessions carrying call signalling, whilst blocking UDP packets carrying the actual media. This type of behaviour can allow calls to be set up, but the media to be lost.

Some hybrid firewalls combine the intelligence of an application gateway with the performance of a packet filter. For example, firewalls may be specifically designed to interpret the TCP signalling protocol of a VoIP session and selectively to open and close UDP media ports on demand. The interface between application gateway and packet filter is internal in these systems.

It is inherently more difficult to protect against misuse of UDP packets than misuse of TCP packets. TCP opens and closes sockets using a handshake procedure, UDP does not. Firewall systems often interact with TCP handshaking in order to limit packet handling demands on endpoints. For example, a maximum number of simultaneous connections may be imposed, or the active open setup rate may be limited.

The absence of a similar open and close handshake for UDP connections implies that any UDP address port that is opened inbound to an endpoint at the firewall - even for a short time - presents an opportunity for an external agent to overwhelm the endpoint (a denial of service attack). Where some inbound UDP traffic is permitted, it is restricted to indirect connectivity via a robust or expendable proxy server located within the private network.

C.6.1.2 NATS

See also RFC 3257 [80] and its references.

IP Network Address Translation (NAT) is an address mapping technique for mapping packets between two networks. It works by mapping the IP headers of packets on one side into IP headers compatible with the other side, as packets cross from one administration zone to the other. At present this is largely restricted to protocols that use request/response exchanges, in order that the NAT can establish how the packets should be mapped. These rules can then be held in a mapping table within the NAT device.

Because NATs change the values of IP addresses in packets they interfere with the operation of applications that are aware of IP addresses. For example, SIP signalling messages may contain end IP addresses in the call identities, and these addresses need to be altered as the SIP messages cross a NAT. This requires an Application Layer Gateway NAT (NAT ALG) to make the necessary changes.

Another consequence of using NAT is that it must operate in series with the flow of packets from one zone to the other. As with firewalls, a NAT can be placed in the path of packets between two end-points. Unlike firewalls, NAT can pass a variety of protocols, provided that it can establish intelligible address mapping relationships. Consequently a NAT function may enable TCP sessions transparently, and possibly SCTP.

NAT can also support UDP. However this is generally easier to support in one direction through the NAT than the other, hence the NAT usually behaves asymmetrically with UDP.

In a typical NAT configuration, one side is connected to a network using private IP addresses, the other to a network using public addresses. If a packet which is destined for a device on the public network side arrives from a device connected to the private addressing side, the source address is a private address and the destination address is a public one. The NAT intercepts the packet, translates the source address to a valid public address and then forwards the packet to the public side of the NAT. In this case the device connected to the public network successfully receives the packet. However the NAT is unable to match correctly a packet received on its public network side with an address on its private address side - unless it were expecting the packet to arrive, which is the case with TCP.

VoIP - enabled NAT products are emerging. These products serve to track call control protocols and to open UDP port mappings accordingly. This allows an outbound call signalled over TCP to receive an inbound UDP audio stream, but the NAT still behaves asymmetrically.

However, the asymmetric operation of NAT helps to protect private networks, both by hiding private IP addresses and by enabling local dynamic IP addressing (e.g. using local DHCP) so that an end user possesses a particular address only during a call.

NAT acts as an efficient first line of defence against packet storm attacks - it is the IP address of the NAT device that is presented as the endpoint. If no valid inbound mapping is present, then the packets are simply discarded by the NAT.

Annex D:
Using SS7 applications in or through a Managed IP network

D.1 General

The IETF SIGTRAN working group have defined a number of protocols to carry SS7 signalling over an IP network. These are called "User Adaptation Layer" protocols. One exists for MTP level 3 (M3UA, RFC 3332 - see bibliography), one for MTP level 2 (M2UA, RFC 3331), one for SCCP (SUA, as yet an Internet draft - 14). Yet another protocol has been defined for MTP level 2 peer-to-peer signalling (M2PA, as yet an Internet draft - 7). Management Information Bases have also been defined for these various protocols.

The architectures and stacks for these protocols are shown in figures D.1 to D.3.

D.2 Architecture for SIGTRAN protocols

Figure D.1 shows the SUA stack.

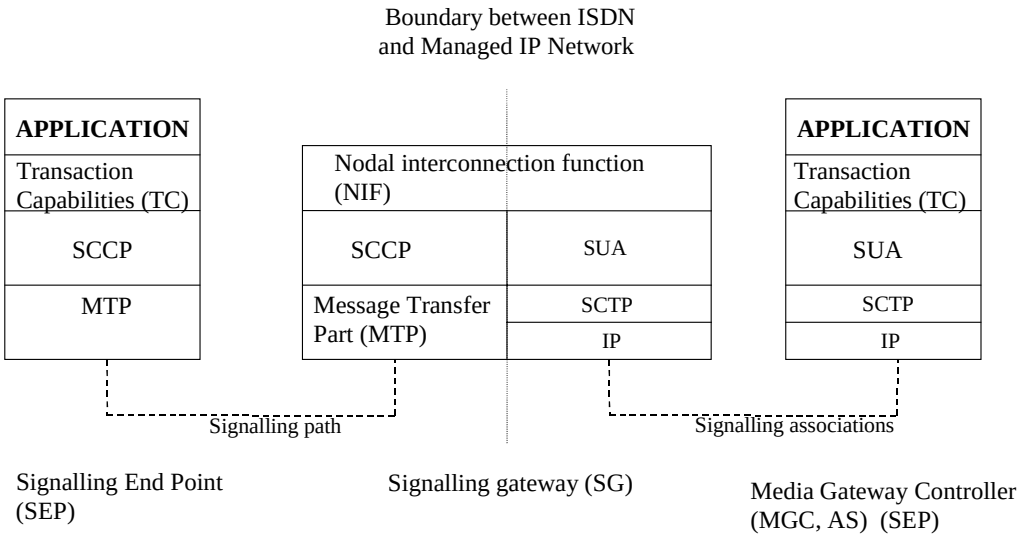


Figure D.1: SUA stack for carrying SS7 from ISDN to IP network

The SCTP associations between SG and ASPs are multi-homed, to increase the "routeset" availability. The SCTP itself will switch over (seamlessly as far as its users are concerned) to an alternative transport address if the current active one fails. Failure of an association is detected by a threshold number of path retransmissions being exceeded.

SCTP allows a number of streams to be defined for an association, this allows messages of a particular priority to be given their own stream (e.g. ASP state management messages can be sent on a different stream to traffic messages, so that they are not held up (by "head of line" blocking) by traffic). However, congestion handling is across all streams of an association, and is achieved by the sender adjusting its (per destination) control window according to the number of timeouts it experiences waiting for message acknowledgements from that destination.

Performance of the IP network could affect the SS7 network. In any case, the SG MUST react to congestion or overload indications from the SS7 network (and so it should accept e.g. the SSC message indicating subsystem/SCCP congestion and the TFC message indicating nodal congestion/overload, and react to them).

Studies should be done (which should include network simulations) to determine the effect of combining a managed IP network part with an SCN part on congestion/overload control mechanisms, and upon route and network availability.

Figure D.2 shows the M3UA stack.

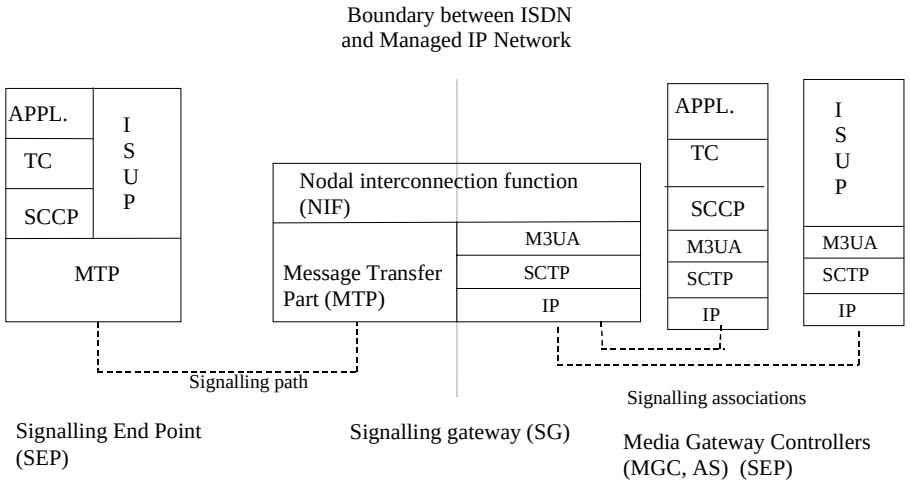


Figure D.2: M3UA stack for carrying SS7 from ISDN to IP network

Note that for ETSI the Routing Key granularity is no finer than DPC, and the SG and ASs must have distinct point codes. Hence each separate AS has its own point code, and so if a single physical MGC is to contain both ISUP and SCCP, it must have at least two point codes.

Here, studies need to be done (including network simulations) of how the flow, congestion and overload control mechanisms work between networks. The managed IP network has a potential to carry large amounts of message and call traffic, the time it takes to recognize a routeset failure or congestion is dependent upon the flow timer parameters used in the SCTP associations. In particular, the interaction of the ISUP and SCCP congestion control mechanisms has been studied for SS7 networks to enable a fair flow control policy to be established. How the SCTP parameters are to be set for the managed IP network, and how these affect the SS7 network flows, has to be determined.

In addition, the effect upon route and network availability of using a managed IP network in conjunction with an SCN needs to be determined.

Figure D.3 shows the M2UA stack.

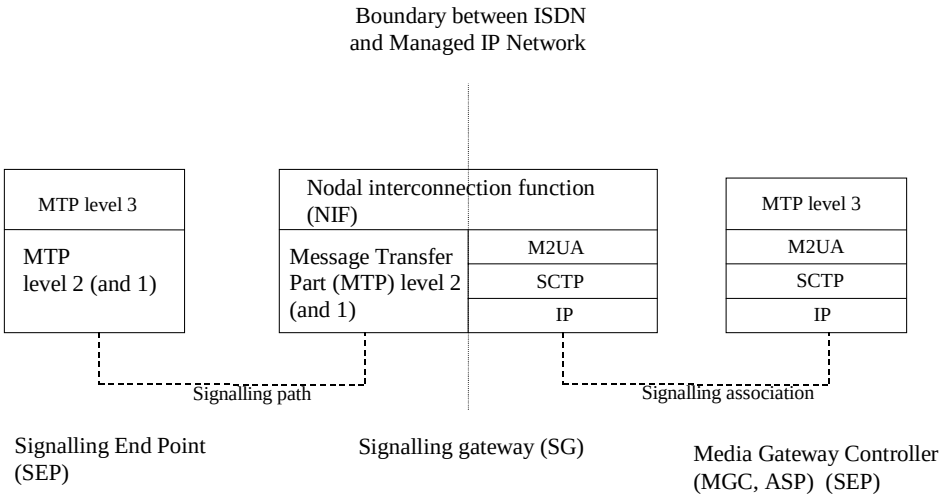


Figure D.3: M2UA stack for "backhauling" SS7 signalling links from SG to MGC in IP network

Here, MTP level 2 flow control is achieved by the Transmission buffer/retransmission buffer congestion onset thresholds being set to detect receive congestion quickly at the other end of a signalling link, and to inform local Users (and also remote ones if the signalling point this end is an STP) quickly enough for them to reduce message traffic in a timely fashion. The flow control in SCTP can be achieved by setting the receiver window size appropriately. However, M2UA admits that there might be oscillation when the MTP and M2UA methods have to interwork at the SG. Consequently, it is necessary to study (including by simulations) how these mechanisms interact, and the effect on the SS7 network. It should be noted that the link capacity, delay characteristics and failure behaviour for links in SS7 networks have been determined by a large number of studies over a long period, that the managed IP network has the capability to inflict large loadings on an SS7 link, and as yet the interconnection of managed IP and legacy SS7 networks is in its infancy.

In addition, the time to detect link failure is well determined in SS7, and the rate of link failures, and taken together these factors are used to determine the network dimensions to give the required availability of the SS7 service. For SCTP the time to detect link failure depends upon the traffic patterns in the IP network and the retransmission timer values set for SCTP. Rules for setting these timer values need to be determined.

D.3 Models for SIGTRAN

The start of these User Adaptation Layers was to define a model for each, where the layer above the particular SS7 level/layer was "remoted" into the managed IP network away from the SS7 level/layer at the Signalling Gateway (SG).

Thus, initially, for example, MTP Users which are above level 3 of the MTP in SS7, were "remoted" into the managed IP network at Application Servers (ASs, with granularity given by DPC + SIO), with instances AS Processes (ASPs). An AS is an abstraction of the function performed for the SS7 User at a Media Gateway Controller. Each ASP is addressed in the IP network with an IP address, and the SG has to derive this from the DPC and SIO, plus load sharing information (e.g. SLS code) in the MTP label of received messages, in order to forward them. This model was later extended to allow the nodes (Hosts) containing the ASs to be addressed with point codes different from that of the SG. Hence the managed IP network was integrated into a unified SS7 network, with the SG developed into an STP. In order for SS7 network management to operate efficiently, the granularity within the ETSI M3UA model is taken as no finer than a DPC. This means that, for example, if an AS (known to the SS7 part of the network by its point code) as a whole fails, the SG can broadcast TFP messages within the SS7 network. (If the granularity were finer, i.e. DPC + SI, then the only SS7 network management message that could be used would be a User Part Unavailable (UPU) message, which is just sent in response to a message destined to the unavailable user, and is not broadcast). Furthermore, on recovery of the AS, the SG can broadcast TFA messages, whereas it is left to MTP Users to detect the availability of an MTP User (i.e. there is no MTP UP available message corresponding to the UPU message).

Use of a separate point code for the AS from that of the SG also allows more efficient use of flow and congestion control.

A similar model to that for M3UA was developed for the SCCP User Adaptation Layer (SUA), where the SG could have its SCCP Users (granularity of DPC + SSN) remoted, but addressed within SS7 by the same Point Code or Global Title as the SG, or each AS could have its own DPC+SSN or GT address. In order to make load sharing across ASPs for an AS work at an SG without breaking the layering principles of SS7, it is further preferred in ETSI for each ASP to have its own unique GT or (AS point code +) SSN, in addition to those of the ASs which it serves.

See the figures D.4 to D.7 for the possible models for M3UA and SUA.

D.3.1 M3UA models

D.3.1.1 MTP/M3UA users homed on SG

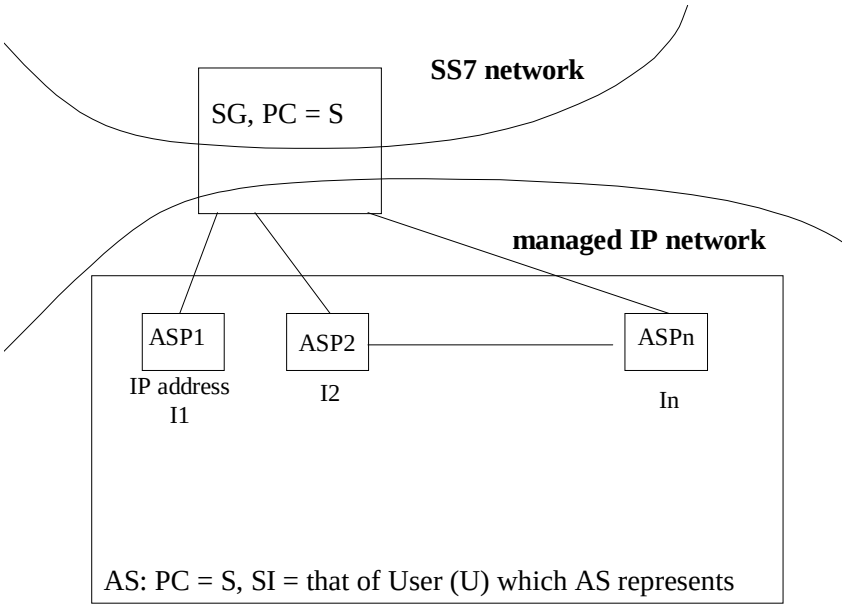


Figure D.4: Homed users

Here, the AS containing the M3UA/MTP users is remoted from the SG within the managed IP network.

An AS (and its ASPs) has the same point code as the SG. The SIO of the MTP User distinguishes the AS from other ASs homed on the SG. The ASPs contain a process instance of the AS (an ASP can serve more than one AS if necessary), and can act either in loadsharing mode or primary/backup mode (IETF allows a broadcast mode, but ETSI does not).

The SG can also be implemented as a set of SG processes, to improve availability if required.

An SG establishes an SCTP association to each ASP, the association itself can be multi-homed, thus giving a variety of paths to increase route availability.

Note that this model is not supported by ETSI, since the routeing key granularity is there limited to be no finer then DPC - each AS must have its own DPC.

D.3.1.1.1 MTP management

The SG acts as an MTP endpoint (SEP), and is responsible for MTP management for its MTP/M3UA Users.

There is thus no MTP management at the AS/ASPs.

The ASPs know of availability/congestion status of destinations in the SS7 network because of "local broadcast" by the MTP/M3UA in the SG when the status changes. These broadcasts use transformed primitives of MTP-PAUSE, MTP-RESUME and MTP-STATUS.

There are no audits for route availability status from AS to SG concerning SS7 destinations, and none from SG to AS either (the latter are not required anyway because the ASP and AS status (Up, Down, Active, Inactive) are known from the interchange of ASPSM and ASPTM messages).

D.3.1.1.2 Message routeing

Within the SS7 network, the routeing of a message up to the SG is by DPC. The AS required is selected by the SG from the message's SIO value, and the ASP by a suitable load-sharing parameter (e.g. SLS in the message's MTP label). As the SG is an MTP endpoint, M3UA routeing from it to ASP should be on IP address only.

All M3UA messages between the SG and the AS(Ps) are carriers of primitives between the MTP and its Users, call these "transformed MTP primitives", as opposed to MTP messages transformed into M3UA messages.

D.3.1.2 MTP/M3UA Users at AS/ASPs with own point codes

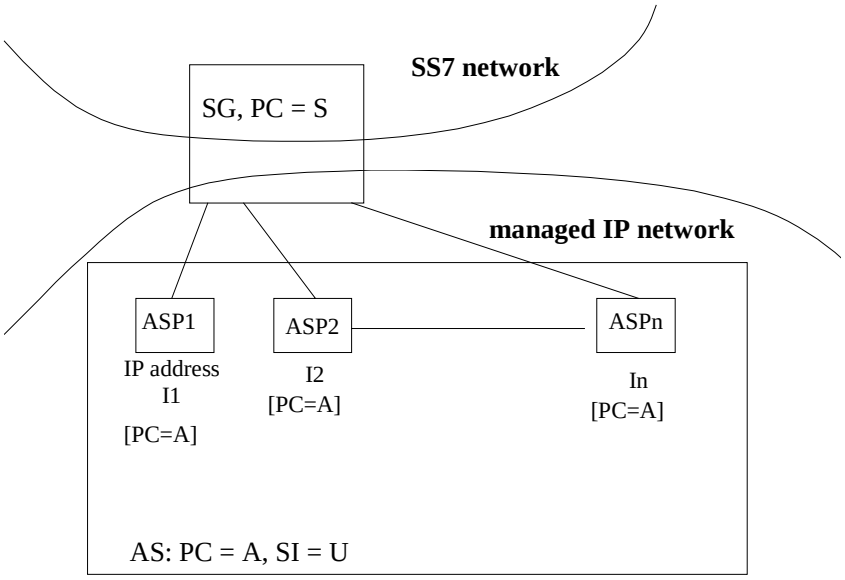


Figure D.5: Users own PCs

Here, the SG acts as an STP as far as the SS7 network is concerned, with its own point code "S".

The AS has a point code separate from the SG's, "A". Each ASP *"a"* has the same point code "A" as the AS it serves, being distinguished from other ASPs in the AS by its current load-sharing parameter (e.g. OPC/DPC/SLS values it currently supports).

The SG could perform multi-point code working at MTP level (and then, strictly, the AS and ASP point code "belongs" to the SG, in the SS7 sense. But in the M3UA sense, the only point code belonging to the SG(P) is S).

For ETSI, the SG and each AS have their own point code. Thus, for instance, an ISUP AS accessed through an SG has a point code "I" say, with the SG having point code "S", and an AS for SCCP, say, has a different point code "J".

Correlation between the states of each ASP of an AS is required at an SG in order for the complete state of an AS to be recognized and signalled to the SS7 network. How this is done is not specified in the RFC, or TS.

D.3.1.2.1 MTP network management

If the SG does multi-point code working, it could in addition act as a proxy for MTP network management for the nodes containing the ASPs.

If the SG does not do multi-point code working, each node containing one or more ASPs must also support MTP network management.

If an ASP becomes congested, it can send a SCON message (equivalent to an MTP TFC message referring to itself) to the SG. Or, if in addition the IP network is congested, it could signify its own congestion by closing up its SCTP receive window. For ETSI, the ASP must signal congestion if it occurs. When it becomes congested depends on its implementation, and which method it chooses depends on the network circumstances. There might be other methods of signifying congestion, which could be chosen instead, but in any case the method must be according to the ETSI specifications for the network (SCON and close SCTP receiver window are according to the M3UA and SCTP TSs respectively).

D.3.1.2.2 Message routeing

If the SG acts as a proxy for MTP network management at the AS/ASP nodes, M3UA messages between SG and ASPs are transformed MTP primitives. M3UA messages should then be routed on IP address.

If the SG does not act as a proxy for MTP management at AS/ASP nodes, M3UA messages between SG and ASPs are transformed MTP messages.

D.3.2 SUA Models

D.3.2.1 SCCP/SUA Users homed on SG

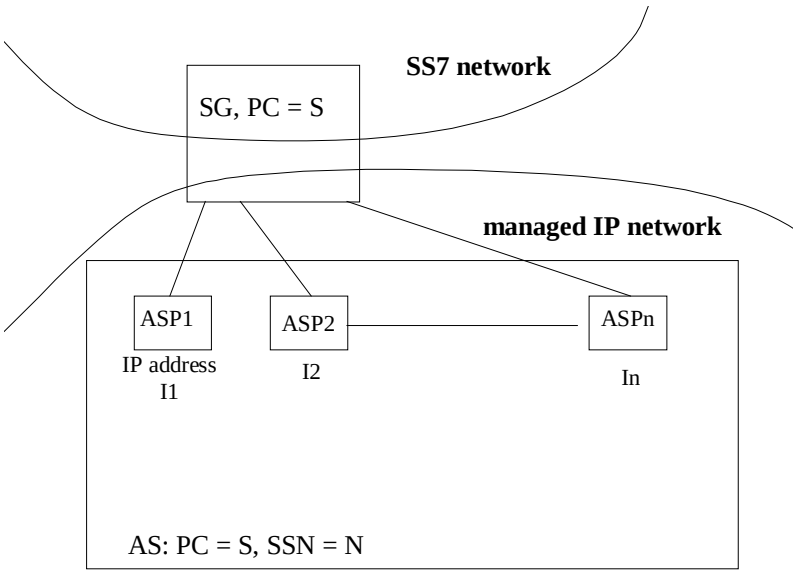


Figure D.6: Homed Users

Here, the AS containing the SUA/SCCP users is remoted from the SG within the managed IP network.

The AS (and its ASPs) has the same point code as the SG.

D.3.2.1.1 SCCP management

The SG acts as an SCCP endpoint, and is responsible for SCCP management for its SCCP/SUA Users.

There is thus no SCCP management at the AS/ASPs.

The ASPs know of availability/congestion status of destinations and subsystems in the SS7 network because of "local broadcast" by the SCCP/SUA in the SG when the status changes. These broadcasts use transformed primitives of N-STATE and N-PCSTATE.

There are no audits for subsystem availability or route availability status from ASP to SG concerning SS7 destinations (except possibly when an ASP recovers) and none from SG to AS either (the latter are not required anyway because the ASP and AS status (Up, Down, Active, Inactive) are known from the interchange of ASPSM and ASPTM messages).

D.3.2.1.2 Message routeing

Within the SS7 network, the routeing up to the SG could be on GT or SSN. As the SG is an SCCP endpoint, SUA routeing from it to AS(P) should be on IP address only.

All SUA messages between the SG and the AS(Ps) are carriers of primitives between the SCCP and its Users, call these "transformed SCCP primitives", as opposed to SCCP messages transformed into SUA messages.

Loadsharing across ASPs could be done by each ASP having its own SSN (and initial message routeing from SS7 network to SG done on GT, subsequent CLS messages could be routed on GT or SSN), or the RFC's TID or DRN scheme could be used. Or, if all ASPs have the same SSN (as the AS), then load sharing could be done, for example, by OPC/DPC/Sequence control combination.

D.3.2.2 SCCP/SUA Users at AS/ASPs with own addresses

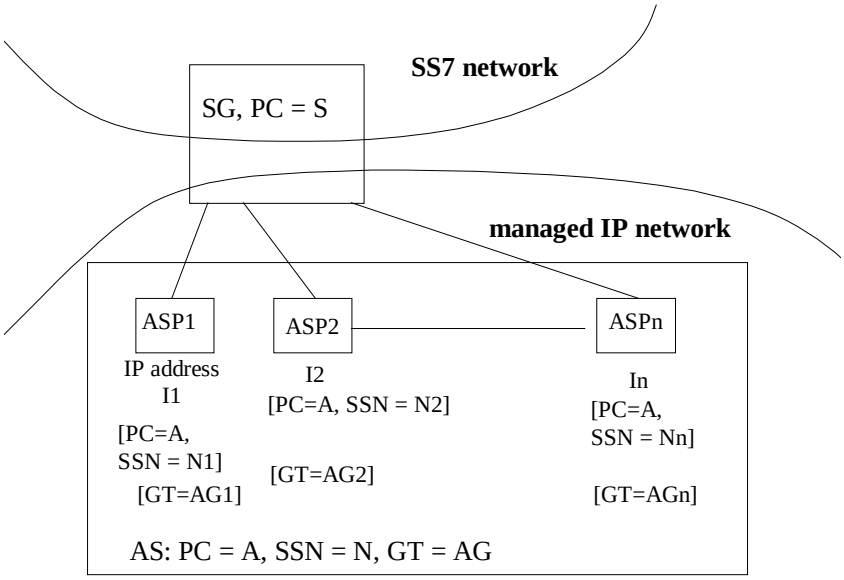


Figure D.7: Users own addresses

Here, the SG acts as a relay point.

1) There could be a GT for the AS as a whole, with a separate GT for each ASP.

2) Or there could be a point code separate from the SG's for the AS (possibly with the AS having its own GT), with each ASP having the same point code as the AS, but its own SSN.

3) Or each ASP could have the same SSN as the AS, but be distinguished by, for example, the OPC/DPC/Sequence control combination it supports.

4) Or 1 above could hold, and one of 2 or 3.

The SG could perform multi-point code working at MTP level (and then, strictly, the AS and ASP point code "belongs" to the SG, in the SS7 sense. But in the SUA sense, the only point code belonging to the SG(P) is S).

D.3.2.2.1 SCCP management

If the SG does multi-point code working, it could in addition act as a proxy for SCCP management for the nodes containing the ASPs.

If the SG does not do multi-point code working, each node containing one or more ASPs must also support SCCP management, and sufficient MTP network management to support SCCP management. In this case, if the ASPs share the same point code with the AS, then each ASP should be distinguished by a different SSN if inter-ASP communication is to be avoided for SCCP management for a non-replicated subsystem.

D.3.2.2.2 Message routeing

If the SG does **not** do multi-point code working, an initial message of a sequence, where sequences are load shared across ASPs, are best routed from the SS7 network on GT (especially if the TID/DRN mechanism is not to be used for subsequent messages).

Messages can be routed on GT or SSN from the SS7 network if the SG does multi-point code working.

If the SG acts as a proxy for SCCP management at the AS/ASP nodes, SUA messages between SG and ASPs are transformed SCCP primitives. SUA messages should then be routed on IP address. The enhanced SCON message corresponding to SSC is not then required. However, it would be advisable for each AS and ASP to have some form of congestion control for use when it itself becomes congested. This could be to close its SCTP receiver window.

If the SG does not act as a proxy for SCCP management at AS/ASP nodes, SUA messages between SG and ASPs are transformed SCCP messages. SUA messages can then be routed on GT or SSN in the SCCP fashion (with the AMF of SUA deriving an IP address).

ETSI does not allow the TID mechanism to be used in SUA, since it breaks the layering principle at the SG (SUA should not examine the TC part of any message it is carrying, except possibly in order to do (unspecified) message screening). ETSI also does not allow the DRN mechanism to be used for connection-oriented SUA, since there are better methods available (e.g. the dynamic method as specified for the SCCP of coupling of connection sections).

Load sharing can be done for messages routed on GT, or for messages routed by [DPC+] SSN by using, for example, the OPC/DPC/Sequence control value as a load sharing key.

Annex E (informative): Bibliography

ETSI TS 102 228 (V4.4.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Technology Mapping; Implementation of TIPHON architecture using BICC".

DTR/STQ-00037 V0.0.4 (2003-03): "Speech Processing, Transmission and Quality Aspects (STQ); The quality of speech when carried over packet technology including IP".

ETSI ETR 003: "Network Aspects (NA); General aspects of Quality of Service (QoS) and Network Performance (NP)".

ITU-T Recommendation H.323: "Packet-based multimedia communications systems".

ITU-T Temporary Document TD 38 to WP 3/11: "Draft Q.1912.SIP", November 2002.

Juniper Networks White Paper (2001): "Supporting Differentiated Service Classes in Large IP Networks", C.Semeria, J.W.Stewart III.

Juniper Networks White Paper (2002): "IP Dependability: Network Link and Node Protection", C.Semeria.

Juniper Networks White Paper (2000): "Traffic Engineering for the New Public Network", C.Semeria.

Juniper Networks White Paper (2001): "Voice over IP Solutions", S.Cristensen.

IETF RFC 3331: "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer".

IETF RFC 3332: "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)".

IETF RFC 2578: "Structure of Management Information Version 2 (SMIv2)".

IETF RFC 2579 "Textual Conventions for SMIv2".

IETF RFC 2580: "Conformance Statements for SMIv2".

IETF RFC 1902: "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)".

IETF RFC 1903: "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)".

IETF RFC 1904: "Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)".

IETF RFC 1905: "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)".

IETF RFC 1906: "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2) ".

IETF RFC 2272: "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) ".

IETF RFC 2574: "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)".

IETF RFC 2273: "SNMPv3 Applications".

IETF RFC 2572: "SNMPv3 Applications".

Further reading is:

IPv6 useage:

IETF RFC 1886: "DNS Extensions to support IP version 6", by S. Thomson and C. Huitema, December 1995.

IETF RFC 1888 (experimental): "OSI NSAPs and IPv6", by J. Bound, B. Carpenter, D. Harrington, J. Houldsworth and A. Lloyd, August 1996.

IETF RFC 1981: "Path MTU Discovery for IP version 6", by J. McCann, S. Deering and J. Mogul, August 1996.

IETF RFC 2374 (Obsoletes 2073): "An IPv6 Aggregatable Global Unicast Address Format", by R. Hinden, M. O'Dell and S. Deering, July 1998.

IETF RFC 2462 (Obsoletes 1971): "IPv6 Stateless Address Autoconfiguration ", by S. Thomson and T. Narten, December 1998.

IETF RFC 2464 (Obsoletes 1972): "Transmission of IPv6 Packets over Ethernet Networks", by M. Crawford, December 1998.

IETF RFC 2472 (Obsoletes 2023): "IP Version 6 over PPP", by D. Haskin and E. Allen, December 1998.

IETF RFC 2874: "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", by M. Crawford and C. Huitema, July 2000.

IETF RFC 2894: "Router Renumbering for IPv6" by M. Crawford, August 2000.

IETF RFC 3314 (informational): "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", by M. Wasserman, Ed., September 2002.

IETF RFC 2553 (Informational), Obsoletes 2133: "Basic Socket Interface Extensions for IPv6", by R. Gilligan, S. Thomson, J. Bound and W. Stevens, March 1999.

MIBs for SCTP and M3UA:

draft-ietf-sigtran-sctp-mib-09 (using SMIv2, RFC 2578, 2579 and 2580), draft-ietf-sigtran-m3ua-mib-04 (using SMIv2, RFC 1902, 1903, 1904; SNMPv3, RFC 1906, 2272, 2574; SNMPv2PO, RFC 1905; SNMPv3APP, RFC 2273, SNMPv3VACM, RFC 2572). But see RFC 3410.

MPLS:

IETF RFC 2702 (Informational): "Requirements for Traffic Engineering Over MPLS", by D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell and J. McManus, September 1999.

Numbering and addressing (including ENUM):

IETF RFC 2276 (Informational): "Architectural Principles of Uniform Resource Name Resolution", by K. Sollins, January 1998.

IETF RFC 2916: "E.164 number and DNS", by P. Faltstrom, September 2000.

IETF RFC 3401 (informational), Obsoletes 2915, 2168: "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS", by M. Mealling, October 2002.

IETF RFC 3402 (Obsoletes 2915, 2168): "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm", by M. Mealling, October 2002.

IETF RFC 3403 (Obsoletes 2915, 2168): "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", by M. Mealling, October 2002.

IETF RFC 3404 (Obsoletes 2915, 2168): "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application", by M. Mealling, October 2002.

IETF RFC 3405 (Best Current Practice): "Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures", by M. Mealling, October 2002.

draft-ietf-enum-rfc2916bis-03.txt (Obsoletes: 2916 (if approved)): "The E.164 to URI DDDS Application (ENUM)", by P. Faltstrom and M. Mealling, January 22, 2003.

draft-ietf-enum-usage-scenarios-00.txt (Informational): " ENUM Usage Scenarios", by S. Lind, June 6, 2002.

draft-ietf-sipping-e164-02: "Using ENUM for SIP Applications", by J. Peterson, H. Liu, J. Yu and B. Campbell, October 26, 2002.

QoS and Routeing:

IETF RFC 2386 (Informational): "A Framework for QoS-based Routing in the Internet", by E.Crawley, R.Nair, B.Rajagopalan, H.Sandwick, August 1998.

IETF RFC 2676 (Experimental): "QoS Routing Mechanisms and OSPF Extensions", by G.Apostolopoulos, D.Williams, S.Kamat, R.Guerin, A.Orda, T.Przygienda, August 1999.

Security, encryption, authentication:

IETF RFC 2104 (Informational): "HMAC: Keyed-Hashing for Message Authentication", by H. Krawczyk, M. Bellare, R. Canetti, February 1997.

"The Code Book", by S.Singh, published by Fourth Estate, 1999.

"Cryptanalysis of Number Theoretic Ciphers", by S.S.Wagstaff Jr., Chapman & Hall/CRC, 2003.

SIP and SDP:

IETF RFC 2976: "The SIP INFO Method", by S. Donovan, October 2000.

IETF RFC 3262: "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)", by J. Rosenberg and H. Schulzrinne, June 2002.

IETF RFC 3263 (Obsoletes 2543): "Session Initiation Protocol (SIP): Locating SIP Servers", by J. Rosenberg and H. Schulzrinne, June 2002.

IETF RFC 3264 (Obsoletes 2543): "An Offer/Answer Model with the Session Description Protocol (SDP)", by J. Rosenberg and H. Schulzrinne, June 2002.

IETF RFC 3265 (Updates: 2543): "Session Initiation Protocol (SIP) - Specific Event Notification", by A. B. Roach, June 2002.

IETF RFC 3311: "The Session Initiation Protocol (SIP) UPDATE Method", by J. Rosenberg, September 2002.

RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers", by H. Schulzrinne, August 2002.

IETF RFC 2327: "SDP: Session Description Protocol", by M. Handley and V. Jacobson, April 1998

IETF RFC 3266: "Support for IPv6 in Session Description Protocol (SDP)", by S. Olson, G. Camarillo and A. B. Roach, June 2002

Draft-ietf-sip-dhcpv6-01.txt: "DHCPv6 Options for SIP Servers", by H. Schulzrinne and B. Volz, November 4, 2002.

Draft-ietf-sip-sctp-03.txt: " The Stream Control Transmission Protocol as a Transport for the Session Initiation Protocol", by J. Rosenberg, H. Schulzrinne and G. Camarillo, June 28, 2002.

Draft-ietf-sipping-3gpp-r5-requirements-00.txt: "3rd-Generation Partnership Project (3GPP) Release 5 requirements on the Session Initiation Protocol (SIP)", by M. Garcia-Martin, October 11, 2002.

Draft-ietf-sipping-aaa-req-01.txt: "Authentication, Authorization and Accounting Requirements for the Session Initiation Protocol", by J. Loughney and G. Camarillo, November 4, 2002.

Draft-ietf-sipping-basic-call-flows-01.txt: "Session Initiation Protocol Basic Call Flow Examples", by A. Johnston, S. Donovan, R. Sparks, C. Cunningham, K. Summers, October 2002.

Draft-ietf-sipping-pstn-call-flows-01.txt: "Session Initiation Protocol PSTN Call Flows", by A. Johnston, S. Donovan,R. Sparks, C. Cunningham and K. Summers, November 2002.

Draft-ietf-sipping-service-examples-03.txt: "Session Initiation Protocol Service Examples", by Alan Johnston, Robert Sparks, Chris Cunningham, Steve Donovan and Kevin Summers, November 2002.

SIP-T:

IETF RFC 3372 (BCP): "Session Initiation Protocol for Telephones (SIP-T): Context and Architectures", by A.Vemuri and J. Peterson, September 2002.

Mapping SIP to ISUP:

IETF RFC 3398: "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping", by G. Camarillo, A. B. Roach, J. Peterson and L. Ong, December 2002.

draft-ietf-iptel-trunk-group-00.txt: "Representing trunk groups in sip/tel Uniform Resource Identifiers (URIs)", by Vijay K. Gurbani, Cullen Jennings and Jon Peterson, October 2002.

draft-ietf-sipping-overlap-03.txt: "Mapping of ISUP Overlap Signalling to the Session Initiation Protocol", by Gonzalo Camarillo, Adam Roach, Jon Peterson and Lyndon Ong, Augusto 2002.

SIP, NAT and Firewalls:

Draft-ietf-sipping-nat-scenarios-00.txt: "NAT and Firewall Scenarios and Solutions for SIP", by J. Rosenberg, R. Mahy and S. Sen, June 24, 2002.

TCP ECN:

IETF RFC 3168 (Updates 2474, 2401, 793, Obsoletes 2481): "The Addition of Explicit Congestion Notification (ECN) to IP", by K. Ramakrishnan, S. Floyd, D. Black, September 2001.

Transport over TCP:

IETF RFC 2126: "ISO Transport Service on top of TCP (ITOT)", by Y. Pouffary and A. Young, March 1997.

Transition from IPv4 to IPv6:

IETF RFC 1933: "Transition Mechanisms for IPv6 Hosts and Routers", by R. Gilligan and E. Nordmark, April 1996.

IETF RFC 2529: "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", by B. Carpenter and C. Jung, March 1999.

IETF RFC 2765: "Stateless IP/ICMP Translation Algorithm (SIIT)", by E. Nordmark, February 2000.

draft-ietf-ngtrans-6to4-multicast-01.txt: "Support for Multicast over 6to4 Networks", by Dave Thaler, 29 June 2002.

draft-ietf-ngtrans-dstm-08.txt: "Dual Stack Transition Mechanism (DSTM)", by Jim Bound, Laurent Toutain, Francis Dupont, Hossam Afifi, Alain Durand, Expires December 2002.

draft-ietf-ngtrans-dstm-overview-00.txt: "Dual Stack Transition Mechanism (DSTM) Overview", by Jim Bound, Expires December 2002.

draft-ietf-ngtrans-interaction-01.txt: "Interaction of transition mechanisms", by A. Baudot, G. Egeland, C. Hahn, P. Kyheroinen, A. Zehl, Expires December, 2002.

NOTE: This is not in accordance with section 10 of RFC 2026. Derivative works may not be published.

draft-ietf-ngtrans-ipv6-smtp-requirement-06.txt: "SMTP operational experience in mixed IPv4/IPv6 environements", Motonori Nakamura and Jun-ichiro itojun Hagino, June 28, 2002.

draft-ietf-ngtrans-isatap-12.txt: " Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", by F. Templin, T. Gleeson, M. Talwar and D. Thaler, January 24, 2003.

draft-ietf-ngtrans-isatap-scenario-01.txt: "ISATAP Transition Scenario for Enterprise/Managed Networks", by F. Templin, T. Gleeson and M. Lehman, 1 November 2002.

draft-ietf-ngtrans-mech-v2-01.txt, Obsoletes 2893: "Basic Transition Mechanisms for IPv6 Hosts and Routers", by E. Nordmark and R. E. Gilligan, November 4, 2002.

draft-ietf-ngtrans-mtp-03.txt: "An IPv6/IPv4 Multicast Translator based on IGMP/MLD Proxying (mtp)", by K. Tsuchiya, H. Higuchi, S. Sawada and S. Nozaki, October 15, 2002.

draft-ietf-ngtrans-shipworm-08.txt: "Teredo: Tunneling IPv6 over UDP through NATs", by C. Huitema, September 17, 2002.

draft-ietf-ngtrans-unmanscope-02.txt: "Unmanaged Networks Transition Scope", by C. Huitema, R. Austein and R. van der Pol, November 1, 2002.

draft-ietf-v6ops-3gpp-analysis-01.txt: "Analysis on IPv6 Transition in 3GPP Networks", by J. Wiljakka (Editor), January 2003.

draft-ietf-v6ops-3gpp-cases-02.txt: "Transition Scenarios for 3GPP Networks", by J. Soininen (Editor), January 2003.

draft-ietf-v6ops-ipv4survey-00.txt: "Survey of IPv4 Addresses in Currently Deployed IETF Standards", by Philip J. Nesser II, January 13, 2003.

draft-ietf-v6ops-unman-scenarios-00.txt: "Unmanaged Networks IPv6 Transition Scenarios", by C. Huitema, R. Austein, R. van der Pol, January 10, 2003.

NGNI references:

NGNI, SmartMan Consortium, IST-1999-20591: "Management for Next Generation Networks", Version 3.0, Editor: Dr. Willie Donnelly, 11/02/02, at www.ngni.org.

NGNI, VoIP Technologies and Service: "VoIP: Architecture, Services and NGN", September 02.

NOTE: This contains inaccuracies, particularly with respect to SIGTRAN, BICC, etc.

NGNI, SMONET, Document D03 from WP03: "Specification of Integrated Network Platform Architecture", 12/2001.

NGNI (Access Networks Working Group): "Evolution of access technologies (draft)", 05/2003.

History

Document history		
V1.1.1	October 2003	Publication