
**Information technology — Generic digital
audio-visual systems —**

**Part 8:
Management architecture and protocols**

*Technologies de l'information — Systèmes audiovisuels numériques
génériques —*

Partie 8: Architecture et protocoles de gestion

Reference number
ISO/IEC 16500-8:1999(E)



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 1999

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents	Page
Foreword	v
Introduction	vi
1 Scope.....	1
2 Normative References.....	1
3 Definitions.....	3
4 Acronyms and abbreviations	4
5 Conventions	7
6 DAVIC System Management Architecture.....	7
6.1 Scope of DAVIC System Management Architecture.....	7
6.2 Partitioning.....	7
6.2.1 Functional OSF Partitioning	7
6.2.2 TMN Logical Layer Partitioning	8
6.2.3 DAVIC Management Scenarios	11
6.3 Interworking Scenarios Between CMIP and SNMP Based Management.....	16
6.3.1 Integration through the Human-Machine Interface	17
6.3.2 Dual protocol Stacks.....	18
6.3.3 CMIP-to-SNMP Proxy	18
7 Access Network Management Information Model.....	20
7.1 Scope of Access Network Management.....	20
7.2 Network Delivery Systems Architecture and Interfaces	21
7.3 Access Network Management Architecture	21
7.4 Access Network Management Functions	23
7.4.1 Configuration Management Functions.....	24
7.4.2 Fault Management Functions.....	24
7.4.3 Performance Management Functions.....	24
7.5 Access Network Management Protocol Stack	25
7.6 Management Information Model Overview	25
7.6.1 Managed Object Classes	25
7.6.2 Object Class Relationships.....	27
7.6.3 Application of the Model to DAVIC Information Flows	32
7.6.4 Managed Object Class Overview.....	39
7.7 Management Information Details - GDMO & ASN.1 Specification	48
7.7.1 Object Classes.....	48
7.7.2 Packages.....	52
7.7.3 Attributes	52
7.7.4 Name Bindings	56
7.7.5 ASN.1 Productions	60
8 Service Related Control Management Information Model	62
8.1 Introduction.....	62
8.2 Information Model Motivation.....	62
8.2.1 Configuration Management	63
8.2.2 Video on Demand Service-Related Control.....	66

8.2.3	Broadcast Service Management in the Delivery System Domain	67
8.2.4	Service Management View	71
8.3	Information Model Overview.....	71
8.3.1	broadbandDrop	72
8.3.2	broadcastProgram.....	72
8.3.3	broadcastProgramFeature.....	73
8.3.4	controlSystem.....	74
8.3.5	cpe	74
8.3.6	cpeAuthorization.....	75
8.3.7	domain.....	75
8.3.8	serviceConnectionPoint	75
8.3.9	serviceProvider.....	75
8.4	GDMO Information Model	75
8.4.1	Managed Object Classes	76
8.4.2	Conditional Packages.....	80
8.4.3	Attributes.....	83
8.4.4	Name Bindings.....	91
8.4.5	Actions	95
8.4.6	ASN.1 Module	95
Annex A	(informative) Management protocol independent modeling techniques.....	100
A.1	Introduction	100
A.2	Overview of independent description notations	101
A.3	Examples of notations in use	120
A.4	Summary	126
Bibliography		128

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 16500 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 16500-8 was prepared by DAVIC (Digital Audio-Visual Council) and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

ISO/IEC 16500 consists of the following parts, under the general title *Information technology — Generic digital audio-visual systems*:

- *Part 1: System reference models and scenarios*
- *Part 2: System dynamics, scenarios and protocol requirements*
- *Part 3: Contours: Technology domain*
- *Part 4: Lower-layer protocols and physical interfaces*
- *Part 5: High and mid-layer protocols*
- *Part 6: Information representation*
- *Part 7: Basic security tools*
- *Part 8: Management architecture and protocols*
- *Part 9: Usage information protocols*

Annex A of this part of ISO/IEC 16500 is for information only.

Introduction

ISO/IEC 16500 defines the minimum tools and dynamic behavior required by digital audio-visual systems for end-to-end interoperability across countries, applications and services. To achieve this interoperability, it defines the technologies and information flows to be used within and between the major components of generic digital audio-visual systems. Interoperability between these components and between individual sub-systems is assured through specification of tools and specification of dynamic systems behavior at defined reference points. A reference point can comprise one or more logical (non-physical) information-transfer interfaces, and one or more physical signal-transfer interfaces. A logical interface is defined by a set of information flows and associated protocol stacks. A physical interface is an external interface and is fully defined by its physical and electrical characteristics. Accessible reference points are used to determine and demonstrate compliance of a digital audio-visual subsystem with this international standard.

A summary of each part follows.

ISO/IEC 16500-1 (DAVIC 1.3.1a Part 2) defines the normative digital audio-visual systems technical framework. It provides a vocabulary and a Systems Reference Model, which identifies specific functional blocks and information flows, interfaces and reference points.

ISO/IEC 16500-2 (DAVIC 1.3.1a Part 12) defines system dynamic behavior and physical scenarios. It details the locations of the control functional entities along with the normative protocols needed to support the systems behavior. It is structured as a set of protocol walk-throughs, or “*Application Notes*”, that rehearse both the steady state and dynamic operation of the system at relevant reference points using specified protocols. Detailed dynamics are given for the following scenarios: video on demand, switched video broadcast, interactive broadcast, and internet access.

ISO/IEC 16500-3 (DAVIC 1.3.1a Part 14) provides the normative definition of DAVIC Technology Contours. These are strict sets of Applications, Functionalities and Technologies which allow compliance and conformance criteria to be easily specified and assessed. This part of ISO/IEC 16500 contains the full details of two contours. These are the Enhanced Digital Broadcast (EDB) and Interactive Digital Broadcast (IDB). ISO/IEC 16500-3 specifies required technologies and is a mandatory compliance document for contour implementations.

ISO/IEC 16500-4 (DAVIC 1.3.1a Part 8) defines the toolbox of technologies used for lower layer protocols and physical interfaces. The tools specified are those required to digitize signals and information in the Core Network and in the Access Network. Each tool is applicable at one or more of the reference points specified within the Delivery System. In addition a detailed specification is provided of the physical interfaces between the Network Interface Unit and the Set Top Unit and of the physical interfaces used to connect Set Top Boxes to various peripheral devices (digital video recorder, PC, printer). The physical Delivery System mechanisms included are copper pairs, coaxial cable, fiber, HFC, MMDS, LMDS, satellite and terrestrial broadcasting.

ISO/IEC 16500-5 (DAVIC 1.3.1a Part 7) defines the technologies used for high and mid-layer protocols for ISO/IEC 16500 digital audio-visual systems. In particular, this part defines the specific protocol stacks and requirements on protocols at specific interfaces for the content, control and management information flows.

ISO/IEC 16500-6 (DAVIC 1.3.1a Part 9) defines what the user will eventually see and hear and with what quality. It specifies the way in which monomedia and multimedia information types are coded and exchanged. This includes the definition of a virtual machine and a set of APIs to support interoperable exchange of program code. Interoperability of applications is achieved, without specifying the internal design of a set top unit, by a normative Reference Decoder Model which defines specific memory and behavior constraints for content decoding. Separate profiles are defined for different sets of multimedia components.

ISO/IEC 16500-7 (DAVIC 1.3.1a Part 10) defines the interfaces and the security tools required for an ISO/IEC 16500 system implementing security profiles. These tools include security protocols which operate across one or both of the defined conditional access interfaces CA0 and CA1. The interface CA0 is to all security and conditional access functions, including the high speed descrambling functions. The interface CA1 is to a tamper resistant device used for low speed cryptographic processing. This cryptographic processing function is implemented in a smart card.

ISO/IEC 16500-8 (DAVIC 1.3.1a Part 6) specifies the information model used for managing ISO/IEC 16500 systems. In particular, this part defines the managed object classes and their associated characteristics for managing the access network and service-related data in the Delivery System. Where these definitions are taken from existing standards, full reference to the required standards is provided. Otherwise a full description is integrated in the text of this part. Usage-related information model is defined in ISO/IEC 16500-9.

ISO/IEC 16500-9 (DAVIC 1.3.1a Part 11) specifies the interface requirements and defines the formats for the collection of usage data used for billing, and other business-related operations such as customer profile maintenance. It also specifies the protocols for the transfer of Usage Information into and out of the ISO/IEC 16500 digital audio-visual system. In summary, flows of audio, video and audio-visual works are monitored at defined usage data collection elements (e.g. servers, elements of the Delivery System, set-top boxes). Information concerning these flows is then collected, processed and passed to external systems such as billing or a rights administration society via a standardised usage data transfer interface.

Additional Information

ISO/IEC TR 16501 is an accompanying Technical Report. Further architectural and conformance information is provided in other non-normative parts of DAVIC 1.3.1a (1999). A summary of these documents is included here for information.

ISO/IEC TR 16501 (DAVIC 1.3.1a Part 1) provides a detailed listing of the functionalities required by users and providers of digital audio-visual applications and systems. It introduces the concept of a contour and defines the IDB (Interactive Digital Broadcast) and EDB (Enhanced Digital Broadcast) functionality requirements which are used to define the normative contour technology toolsets provided in ISO/IEC 16500-3.

DAVIC 1.3.1a Parts 3, 4 and 5 are DAVIC technical reports. They provide additional architectural and other information for the server, the delivery-system, and the Service Consumer systems respectively. Part 3 defines how to load an application, once created, onto a server and gives information and guidance on the protocols transmitted from the set-top user to the server, and those used to control the set-up and execution of a selected application. Part 4 provides an overview of Delivery Systems and describes instances of specific DAVIC networked service architectures. These include physical and wireless networks. Non-networked delivery (e.g. local storage physical media like discs, tapes and CD-ROMs) are not specified. Part 5 provides a Service Consumer systems architecture and a description of the DAVIC Set Top reference points defined elsewhere in the normative parts of the specification.

DAVIC 1.3.1a Part 13 is a DAVIC technical report, which provides guidelines on how to validate the systems, technology tools and protocols through conformance and / or interoperability testing.

Document ID: 123456789

Information technology — Generic digital audio-visual systems — Part 8: Management architecture and protocols

1 Scope

This part of ISO/IEC 16500 describes the management architecture and protocol for managing the DAVIC System. The DAVIC system management architecture is the TMN-based (Telecommunication Management Network) architecture defined in ITU-T Recommendation M.3010. This management architecture allows for automatic administration, configuration, monitoring, billing, and maintenance of the Service Provider System, the Delivery System, and the Consumer System over the DAVIC S5 flows. In accordance with DAVIC 1.3.1a Part 4 and ISO/IEC 16500-5, the content of these flows is based on either the CMIP protocol or the SNMP protocol, depending on the complexity of the underlying subsystem or the preference of the network provider. SNMP MIBs (Management Information Base) for managing the STU and the Server have been defined in ISO/IEC 16500-5. Usage related information models have also been defined in ISO/IEC 16500-9 using both CMISE and SNMP. For managing the ATM, SDH/SONET components of the Core Network of the DAVIC Delivery System, CMISE models defined in ITU-T and ATM Forum are recommended in ISO/IEC 16500-5 subclause 10.5.3. Taking into account that the current DAVIC specification for the Access Network is ATM-based¹, this Part of ISO/IEC 16500 defines CMISE information models for managing the DAVIC Access Network and service-related data in the Delivery System. In the future, if DAVIC specifications allow alternative access technologies (such as IP-based), additional system management information models (such as SNMP MIB) may be needed. The management of the coexistence of different access network technologies, using different protocols, could be achieved through interworking tools (i.e., interworking between CMIP and SNMP) as described in subclause 6.4. Tutorial information on a protocol-independent modeling technique is also provided in an informative annex.

This part of ISO/IEC 16500 is organized as follows:

Management Architecture	Clause 6 describes the TMN-based management architecture for DAVIC system management.
Access Network Information Model	Clause 7 defines a CMISE information model for the management of the Access Network.
Service Related Control Information Model	Clause 8 defines a CMISE information model for the management of service-related data in the Delivery System.
Informative Annex A: Protocol Independent Modeling Techniques	This informative annex provides tutorial information of management protocol independent modeling technique.

This part of ISO/IEC 16500 refers to system architecture and interface information that are described in ISO/IEC 16500 parts –1, –5 and –9 and in DAVIC 1.3.1a Part 4: *Delivery system architecture and interface*.

2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 16500. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 16500 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau (TSB) maintains a list of currently valid ITU-T Recommendations.

¹ ATM-based Access Network includes Non-ATM HFC (i.e., Non-ATM at A1 and ATM at A4).

2.1 ISO/IEC and ITU-T normative references

- ITU-T Recommendation G.774, *SDH Management Model for the Network Element View*, 1992 and Corrigendum, 1996.
- ITU-T Recommendation G.774, Corrigendum, 1996.
- ITU-T Recommendation G.774-01, *SDH Performance Monitoring for the Network Element View*, 1994 and Corrigendum, 1996.
- ITU-T Recommendation G.774-06, *SDH Unidirectional Performance Monitoring for the Network Element View*, 1996.
- ITU-T Recommendation I.751, *Asynchronous Transfer Mode (ATM); Management of the network element view*.
- ITU-T Recommendation M.3100, *Generic Network Information Model*, 1995.
- ITU-T Recommendation Q.811 (1993), *Lower layer protocol profiles for the Q3 interface*.
- ITU-T Recommendation Q.812 (1993), *Upper layer protocol profiles for the Q3 interface*.
- ITU-T Recommendation Q.821, *Stage 2 and 3 Functional Descriptions for the Q3 Interface - Alarm Surveillance*, 1992.
- ITU-T Recommendation Q.822, *Stage 2 and 3 Functional Descriptions for the Q3 Interface - Performance Monitoring*, 1994.
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1995, *Information technology - Abstract Syntax Notation 1 (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.690 (1994), *Information technology - ASN.1 Encoding Rules: Specification of BER, CER, DER..*
- CCITT Recommendation X.700 (1992), *Management framework for Open Systems Interconnection (OSI) for CCITT applications*.
- CCITT Recommendation X.701 (1992), *Information technology – Open Systems Interconnection – Systems management overview*.
- CCITT Recommendation X.711 (1991), *Common management information protocol specification for CCITT applications*.
- ITU-T Recommendation X.721 | ISO/IEC 10165-2:1992, *Information technology - Open Systems Interconnection - Structure of management information: Definition of management information*.
- ITU-T Recommendation X.722 | ISO/IEC 10165-4:1992, *Information technology - Open Systems Interconnection - Structure of management information: Guidelines for the definition of managed objects*.
- ITU-T Recommendation X.745, *Test management function* (1993).

2.2 Additional normative references

The following are additional normative references to the extent specified in Table 7-1.

- ANSI T1.240, *Telecommunications - Operations, Administration, Maintenance and Provisioning (OAM&P) - Generic Network Information Model for Interfaces between Operations Systems and Network Elements*, 1997
- ANSI T1.247, *Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) Communications - Performance Management Functional Area Services and Information Model for Interfaces Between Operations Systems and Network Elements*, 1997
- ATMF af-nm-0027.000, *CMIP Specification for the M4 Interface*, September, 1995 {#6} available at <ftp://ftp.atmforum.com/pub/approved-specs/af-nm-0027.000.pdf>

- ATMF af-nm-0071.000, *Network Management: AAL Management for the M4 “NE View” Interface*, January, 1997 {#6} available at <ftp://ftp.atmforum.com/pub/approved-specs/af-nm-0071.000.pdf>
- ATMF af-nm-0072.000, *Circuit Emulation Service Interworking Requirements, Logical and CMIP MIB*, January, 1997 {#6} available at <ftp://ftp.atmforum.com/pub/approved-specs/af-nm-0072.000.pdf>
- Bellcore GR-1114-CORE, *Generic Operations Interface Requirements : ATM Information Model*, Issue 3, 1996

3 Definitions

This clause defines new terms, and the intended meaning of certain common terms, used in this part of ISO/IEC 16500. Annex A of ISO/IEC 16500-1 defines additional terms and, in some cases, alternative interpretations that are appropriate in other contexts. For convenience, the normative definitions below are included in the annex.

- 3.1. Actor:** A person or system component who interacts with the system as a whole and who provides stimulus which invoke actions.
- 3.2. Class:** Describes a group of Objects with similar properties and behavior.
- 3.3. Class Diagram:** Shows the existence of classes and their relationships in the logical view of the system.
- 3.4. Class and Object Modeling:** Used to define business objects and application architecture. Shows how classes interoperate dynamically to offer use cases and application behavior.
- 3.5. Component Diagram:** Shows the dependencies between software components.
- 3.6. Computational Model:** Gives a description of a system in a graphical form highlighting Objects and their interfaces, as such it is similar to the OMT and UML notion of a class Diagram. An Object Distributed processing (ODP) concept.
- 3.7. Deployment Modeling:** Allows you to model how your application is mapped to a distributed deployment network.
- 3.8. Domain Analysis:** An iterative process that focuses on what is in the system but not on how it is implemented. Domain Analysis builds a language/system independent description of the domain.
- 3.9. Event Trace Diagram:** Interaction Diagram or Message Trace Diagram.
- 3.10. Functional Model (OMT):** Shows how objects in the system interact.
- 3.11. Interaction Diagram:** Similar in principle to collaboration diagrams. Show the interaction between objects over time.
- 3.12. Message Trace Diagram:** Interaction Diagram or Event Trace Diagram.
- 3.13. Method:** A systematic way to achieve a particular goal.
- 3.14. Methodology:** A coherent, integrated set of methods from which a coherent sub-set can be selected for particular applications. A methodology should contain at least four components:
1. a conceptual model of constructs essential to the problem,
 2. a set of procedures suggesting the direction and order to proceed,
 3. a series of guidelines identifying things to be avoided, and
 4. a collection of evaluative criteria for assessing the quality of the product.
- 3.15. Methodology framework:** a way, or structure, that supports a number of methods and languages to be used together when developing a system.
- 3.16. Network Element (NE):** A component of a telecommunications network, whose function is to provide communications services to users. These functions include information transport, adaptation, switching and control.
- 3.17. Object:** A representation of a system component that has both state and behavior.
- 3.18. Object Collaboration Diagram:** Provides a snapshot of a systems state and is used to emphasize relationships.

3.19. Object Model: Shows the static relationships between classes. An object model is described using a class diagram. The Object Model defines the behavior required by the various classes to ensure that the use cases and business rules are supported correctly.

3.20. Operations Support System (OS): A system whose main function it is to run applications that manage network elements, networks and services.

3.21. Package: A nested name space in a model, which contains classes.

3.22. Scenario Diagram: Shows how the Objects in a system interact over time.

3.23. State Transition Diagram: Shows the state of a given context, the events that cause a transition from one state to another and the actions that result.

3.24. Telecommunications Management Network (TMN): A network consisting of Operations Support Systems (OS) and data networking facilities whose purpose it is to provide management capabilities for telecommunications networks, network elements, resources and services.

3.25. Technique: A way that a method is realized, or implemented.

3.26. Tool: A software item, which automates or supports the use of a particular method or language. In system/software engineering, a step-by-step, formalized, manual or automated, process for solving an engineering problem.

3.27. Use Case Diagram: Shows the system's main Use Cases and the Actors that interact with them.

3.28. Use Case Modeling: A requirement analysis technique. Use Cases capture the functional requirements of a system.

4 Acronyms and abbreviations

This clause defines the acronyms and abbreviations used in this part of ISO/IEC 16500. Annex B of ISO/IEC 16500-1 defines acronyms and abbreviations used within ISO/IEC 16500.

AAL	ATM Adaptation Layer
ACTS	Advanced Communications Telematics Services
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation 1
ATM	Asynchronous Transfer Mode
AU4	Administrative Unit - 4
AU44C	Administrative Unit - 44C
AUG	Administrative Unit Group
BCU	Broadcast Control Unit
CAGR	Customers' Anticipate Growth Rate
CAP	Carrierless Amplitude and Phase Modulation
CASE	Computer Aided Software Engineering
CATV	Cable TV
CCP	Channel Change Protocol
CFP	Call for Proposals
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CTP	Connection Termination Point
DAB	Digital Audio Broadcasting
DAVIC	Digital Audio Visual Council
DBS	Digital Broadcast Satellite
DBR	Deterministic Bit Rate
DII	DAVIC Interface Initialization
DIIP	DAVIC Interface Initialization Protocol

DS3	Digital Signal - Level 3
DSM-CC	Digital Storage Media - Command & Control
DTTB	Digital Terrestrial Television Broadcasting
DVB	Digital Video Broadcasting
EDI	Electronic Data Interchange
EMC	Electromagnetic Compatibility
EMMA	European Multimedia experiments in ATM environment
EMS	Element Manager System
FCC	Federal Communications Committee
FITL	Fiber Into The Loop
FR	Frame Relay
FSN	Full Service Network
FTP	File Transfer Protocol
FTTB	Fiber To The Building
FTTC	Fiber To The Curb
FTTH	Fiber To The Home
GDMO	Guidelines for the Definition of Managed Object
HFC	Hybrid Fiber Coax
HMI	Human Machine Interface
HFTTB	Hybrid Fiber To The Building
HTML	Hyper Text Mark up Language
IDL	Interface Definition Language
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internal Engineering Task Force
IN	Intelligent Network
INVOD	Intelligent Near Video On Demand
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	ITU - Telecommunications Standardization Sector
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LEWS	Local Exploitation Work station
LMDS	Local Multipoint Distribution Service
MIB	Management Information Base
MF	Management Function
MHEG	Multimedia and Hypermedia Information coding Experts Group
MMC	Multimedia Conferencing
MMS	Multimedia Conference Services
MO	Managed Object
MOC	Managed Object Class
MOD	Movies On Demand
MPEG	Motion Pictures Experts Group
MS	Multiplex Section
MVDS	Multimedia Video on Demand System
NC	Network Computer
NMF	Network Management Forum
NMS	Network Management System
NOD	News On Demand
NT	Network Termination
NVOD	Near Video On Demand
PDH	Plesiochronous Digital Hierarchy
PLCP	Physical Layer Conversion Protocol
RF	Radio Frequency
RS	Regenerator Section
QAM	Quadrature Amplitude Modulation
OAN	Optical Access Network
OFDM	Orthogonal Frequency Division Multiplexing
OLT	Optical Line Termination
OMG	Object Modeling Group

OMT	Object Modeling Technique
ONU	Optical Network Unit
ONP	Open Network Provision
OO	Object Oriented
OOAD	Object Oriented Analysis and Design
QPSK	Quaternary Phase Shift Keying
OSI	Open System Interconnection
PC	Personal Computer
PCR	Peak Cell Rate
PIN	Personal Identification Number
PNO	Public Network Operator
PON	Passive Optical Network
POTS	Plain Old Telephony System
PPI	Pay Per Information unit
PPP	Pay Per Page
P-PSN	Public Packet Switched Network
PPT	Pay Per Time
PPV	Pay Per View
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Connection
QoS	Quality of Service
RDN	Relative Distinguished Name
RSVP	Resource ReServations Protocol
SBR	Statistical Bit Rate
SCR	Sustainable Cell Rate
SDB	Switched Digital Broadcast
SDH	Synchronous Digital Hierarchy
SDV	Switched Digital Video
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPI	Synchronous Physical Interface
SPVC	Semi-Permanent Virtual Connection
STB	Set Top Box
STU	Set-Top Unit
SVC	Switching Virtual Connection
TC	Transmission Convergence
TCP/IP	Transmission Control Protocol/Internet Protocol
TMN	Telecommunication Management Network
TTP	Trail Termination Point
VC	Virtual Channel
VC4	Virtual Container 4
VC44C	Virtual Container 44C
vcCTP	Virtual Channel Connection Termination Point
VCi	Virtual Channel Identifier
UDP	Usage Data Protocol
VDSL	Very high bit rate Digital Subscriber Loop
UML	Unified Modeling Language
VP	Virtual Path
VPI	Virtual Path Identifier
URL	Uniform Resource Locator
UNI	User-Network Interface
VDT	Video Dial Tone
VOD	Video On Demand
VPN	Virtual Private Network
WWW	World Wide Web

5 Conventions

The style of this part of ISO/IEC 16500 follows the general guidelines of *Guide for ITU-T and ISO/IEC JTC 1 cooperation. Appendix II: Rules for presentation of ITU-T | ISO/IEC common text, (March 1993).*

6 DAVIC System Management Architecture

6.1 Scope of DAVIC System Management Architecture

This document describes the management architecture of a DAVIC system. The DAVIC system management architecture allows for automated administration, monitoring, billing, and maintenance of the Service Provider System, the Delivery System, and the Consumer System over DAVIC S5 flows. These flows may occur within a single DAVIC system or between DAVIC systems. They may also be carried transparently through a DAVIC system in order to reach another DAVIC system. In accordance with DAVIC 1.3.1a Part 4, the content of these flows is based on either the CMIP protocol or the SNMP protocol, depending on the subsystem. Industry trends may encourage the addition of Web-based management or object broker-based management (e.g., CORBA) in future DAVIC specifications.

To deal with the complexity of managing a DAVIC network and its services, the management functionality is considered to be partitioned into logical layers, as defined in the TMN Logical Layered Architecture (LLA) of ITU-T M.3010. A logical layer reflects a particular level of abstraction of the network or service and addresses aspects of management that are associated with that level of abstraction. The following five logical layers are defined:

- Business Management Layer;
- Service Management Layer;
- Network Management Layer;
- Element Management Layer; and
- Network Element Layer.

Management aspects of network elements, networks, and services are supported by applications called operations support functions (OSF). An OSF is a unit of management functionality, which meets a focused set of management goals. An OSF client is typically implemented within one of the four management layers, while its server is implemented in one or more layers below it. To satisfy the TMN architecture, each layer of an OSF must provide sufficient functionality to serve its own purpose and to meet the needs of the layers above it which address the same overall management goals. It is therefore apparent that the Network Element Layer, which is typically implemented in an embedded system, has the broadest scope since it has the potential to serve all four management layers.

It should be noted that logical management layers and OSFs are conceptual in nature, and that the implementation of a management system may combine layers or functions.

6.2 Partitioning

6.2.1 Functional OSF Partitioning

An example of OSF partitioning based upon business, service, network, and element management applications is depicted in Figure 6-1. As shown, some implementations may include business OSFs that are concerned with a total enterprise (i.e., all services and networks) and carry out an overall business goal. Service OSFs are concerned with services offered by one or more networks and will normally perform a customer-interfacing role. Network OSFs are concerned with the management of networks, and Element OSFs with the management of individual elements.

Network OSFs cover the realization of network-based TMN application functions by interacting with Element OSFs. Element and Network OSFs collaborate to manage activities across the network and support “Network” demands of service OSFs. Thus, Element OSFs and Network OSFs share the infrastructure aspects of a telecommunications network, whereas Service and Business OSFs are founded on the financial and service-related practices of an enterprise, which pertain to or depend on the network.

The layering of OSFs based in the reference model shown in Figure 6-1, although widely accepted, should not be regarded as the only possible implementation of DAVIC management systems. Additional or alternative layers may be used to specialise the functionality.

6.2.2 TMN Logical Layer Partitioning

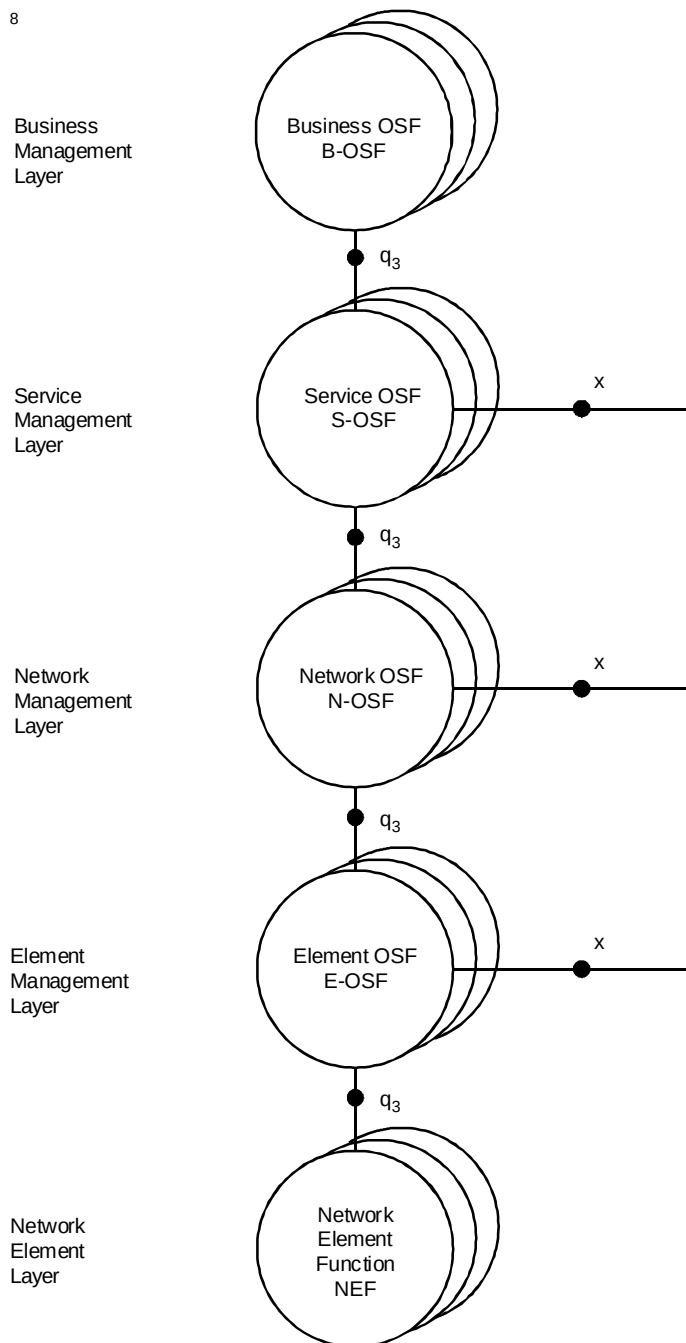
The reference model of an operations system (OS) functional architecture with four management layers is illustrated in Figure 6-2 and described in the following subclauses.

6.2.2.1 Element Management Layer

The element management layer manages each network element on an individual or group basis and supports an abstraction of the functions provided by the network element layer.

The element management layer has the following three principal roles:

- The control and coordination of a subset of network elements on an individual NEF basis. In this role, the element OSFs support interaction between the network management layer and the network element layer by processing the management information being exchanged between network OSFs and individual NEFs. Element OSFs should provide full access to NE functionality.
- The element management layer may also control and coordinate a subset of network elements on collective basis. In this role, element OSFs may also provide a single entity view of a group of NEFs. In addition, the element OSFs may manage the relationships (e.g. connectivity) between NEFs.
- Maintaining statistical, log and other data about elements within its scope of control.



NOTES

- 1 Additional or alternative layers are permitted.
- 2 Other interactions may also occur between non-adjacent layers.

Figure 6-1 — Reference Model of OSF Architecture

OSFs in the element management layer interact with OSFs in the same or other layers within the same DAVIC management network through a q_3 reference point and in other DAVIC management networks through an x reference point.

The Element Management Layer information model for a DAVIC Access Network is defined in Clause 7. Future DAVIC specifications may define additional Element Management models for the Core Network, the Service Provider System, and the Consumer System.

6.2.2.2 Network management layer

The network management layer has the responsibility for the management of a network as supported by the Element Management layer.

At this layer, functions addressing the management of a wide geographical area are located. Complete visibility of the whole network is typical and, as an objective, a technology independent view will be provided to the service management layer.

The network management layer has the following four principal roles:

- 1) The control and coordination of the network view of all network elements within its scope or domain, augmenting the Element Management Layer by its knowledge of physical and logical connectivities.
- 2) The provision, cessation or modification of network capabilities for the support of service to customers.
- 3) The maintenance of network capabilities.
- 4) Maintaining statistical, log and other data about the network and interact with the service manager layer on performance, usage, availability, etc.

Thus, the network management layer provides the functionality to manage a network by coordinating activity across the network and supports the “network” demands made by the Service Management Layer. It knows what resources are available in the network, how these are interrelated and geographically allocated and how the resources can be controlled. It has an overview of the network. Furthermore, this layer is responsible for the technical performance of the actual network and will control the available network capabilities and capacity to give the appropriate accessibility and quality of service.

The Element Management and Network Management Layers are traditionally subdivided into the following functionalities, as described in DAVIC 1.3.1a Part 4:

- Network Client Directory Management (not currently addressed).
- Configuration Management (addressed in Clause 7 for the Access Network).
- Fault Management (addressed in Clause 7 for the Access Network).
- Performance Management (not currently addressed).
- Security Management (not currently addressed).
- Usage Data Collection (addressed in ISO/IEC 16500-9).

OSFs in the network management layer interact with OSFs in the same or other layers within the same TMN through a q3 reference point and in other TMNs through an x reference point.

6.2.2.3 Service management layer

Service management is concerned with, and responsible for, the contractual aspects of services that are being provided to customers or available to potential new customers. Some of the main functions of this layer are service order handling, complaint handling and invoicing.

The service management layer has the following four principal roles:

- 1) customer facing and interfacing with other administrations/ROAs;
- 2) interacting with service providers;
- 3) maintaining the statistical data (e.g. QOS);
- 4) interacting between services.

Customer facing provides the basic point of contact with customers for all service transactions including provision/cessation of service, accounts, QOS, fault reporting, etc.

OSFs in the service management layer interact with OSFs in the same or other layers within the same TMN through a q3 reference point and in other TMNs through an x reference point.

The Service Management layer is responsible for all negotiations and resulting in contractual agreements between a (potential) customer and the service(s) offered to this customer. It is traditionally subdivided into the following functionalities, as described in DAVIC 1.3.1a Part 4:

- ESP Directory Management (not addressed).
- User Directory Management (addressed by Clause 8).
- STU Directory Management (addressed by Clause 8).
- Usage Parameter Collection (addressed by ISO/IEC 16500-9).

The Service Management Layer management information model for DAVIC systems is defined by Clause 8. It addresses a service provider's management needs of SDV and VOD services. It is supplemented by the STU MIB in ISO/IEC 16500-5, Annex A, and the Server MIB in ISO/IEC 16500-5, Annex B. Future DAVIC specifications may define the management of additional service applications.

6.2.2.4 Business management layer

The business management layer has responsibility for the total enterprise. The business management layer comprises proprietary functionality. To prevent access to its functionality, business OSFs do not normally support x reference points. Business OSFs access the information and functionality in the other management layers. The business management layer is included in the TMN architecture to facilitate the specification of capability that it requires of the other management layers.

This layer normally carries out goal setting tasks rather than goal achievement but can become the focal point for action in cases where executive action is called for. This layer is part of the overall management of the enterprise and many interactions are necessary with other management systems.

While the main functions of service and network management layers are the optimal utilization of existing telecommunications resources, those of the business management layer are for the optimal investment and use of new resources.

OSFs in the business management layer interact with OSFs in the same or other layers within the same TMN through a q3 reference point.

The business management layer has the following four principal roles:

- 1) Supporting the decision-making process for the optimal investment and use of new telecommunications resources;
- 2) Supporting the management of AO&M related budget;
- 3) Supporting the supply and demand of AO&M related manpower;
- 4) Maintaining aggregate data about the total enterprise.

The existing DAVIC management information models do not address the Business Management Layer.

Figure 6.2 below shows a possible assignment of management functionality consistent with the above principles.

6.2.3 DAVIC Management Scenarios

This sub-section provides example management scenarios. These scenarios are aligned with the scenarios in DAVIC 1.3.1a Part 4, Clause 11 but provide more detail concerning the management network architecture and interfaces. It should be noted that these are only example scenarios and the division of functionality and layering of EMS (Element Management System), NMS (Network Management System) and SMS (Service Management System) may vary.

6.2.3.1 Scenario 1

This is a scenario in which the end-to-end multimedia system is partitioned into two management domains based on provider boundaries. One management domain contains the Service Provider who owns the server. The second management domain contains the Delivery System provider who owns the Core Network, Access Network and the STB. These two management domains are managed by separate Management Systems to provide reliability in their portion of the end-to-end system. There is peer-to-peer communication between the two SMSs.

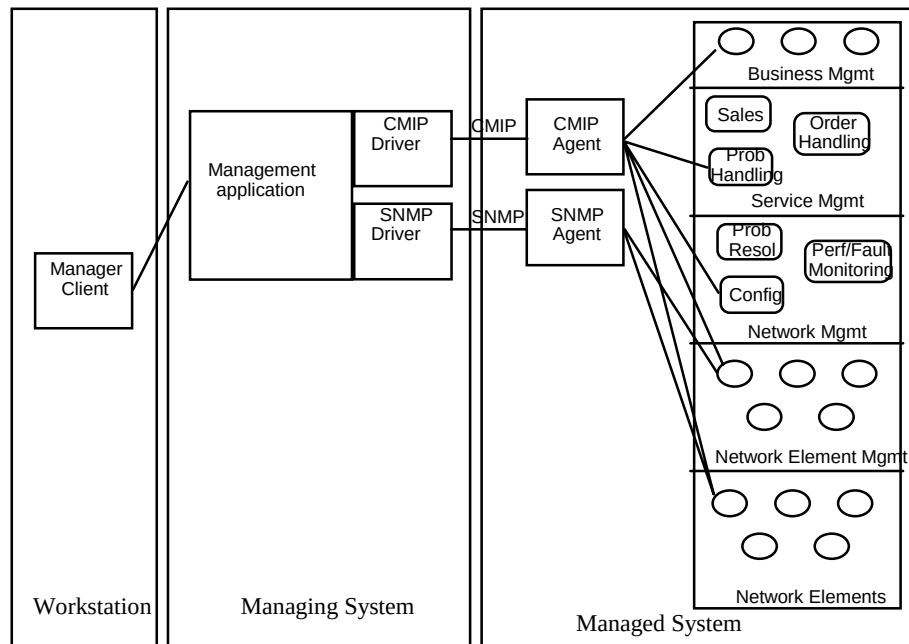


Figure 6-2 — OSF Partitioning Example

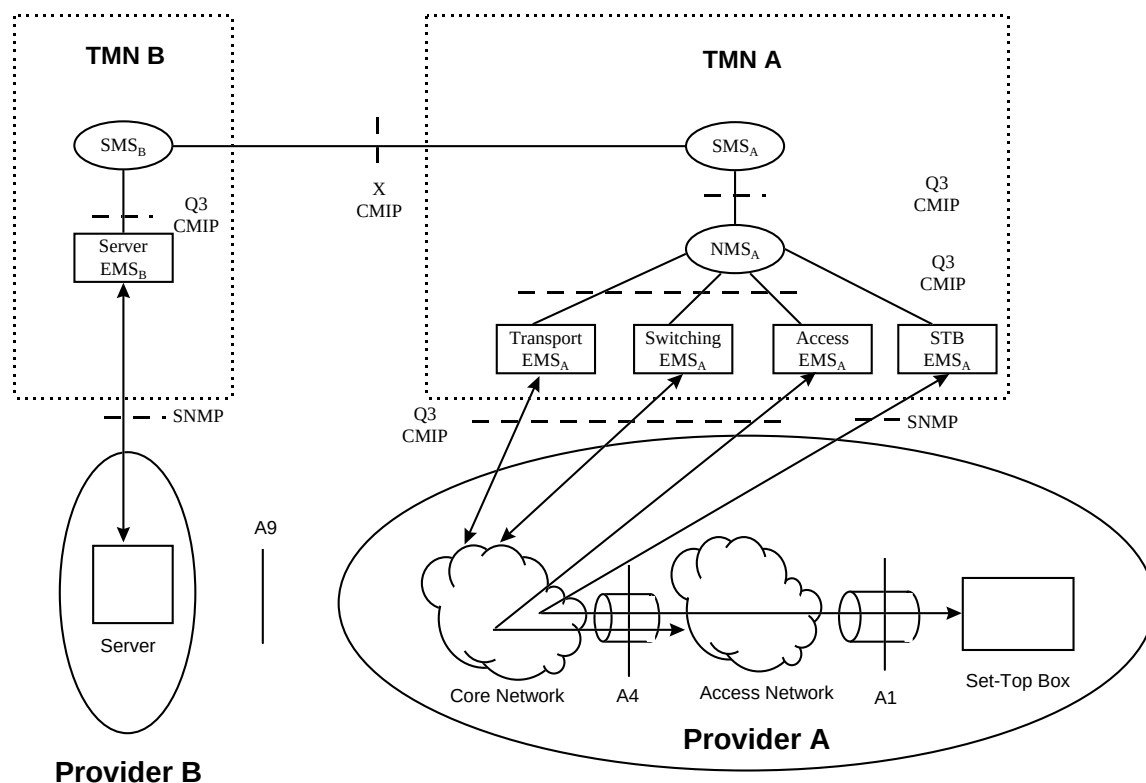


Figure 6-3 — Management Scenario 1

6.2.3.2 Scenario 2

This is a scenario in which the end-to-end multimedia system is partitioned into two management domains based on provider boundaries. One management domain contains the Service Provider who owns the server and the STB. The second management domain contains the network provider who owns the Core Network, and the Access Network. The two domains are managed by separate Network Management Systems. There is peer to peer communication between the two SMSs.

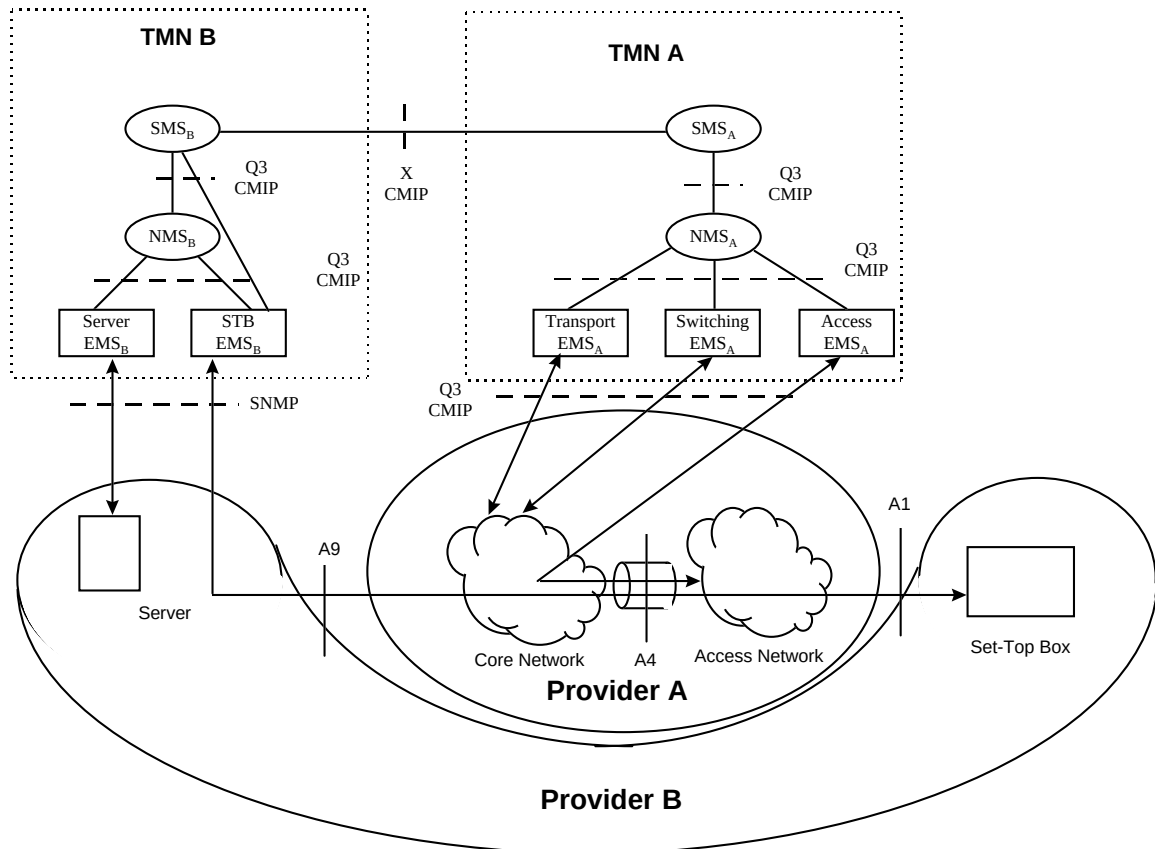


Figure 6-4 — Management Scenario 2

6.2.3.3 Scenario 3

This scenario is one in which the STB is owned by an End Consumer. The end-to-end multimedia system without the STB can now be partitioned into management domains based on the ownership of the several components of the system. The figure identifies one of the possible scenarios.

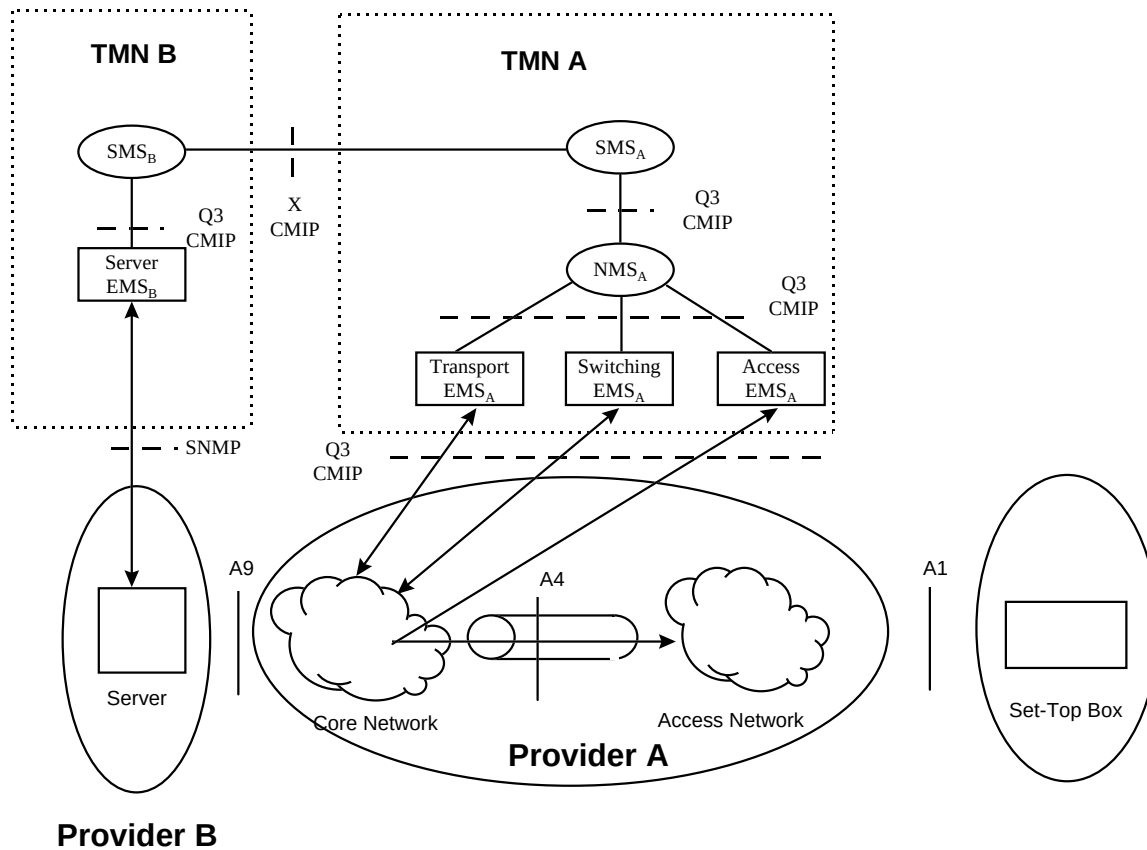


Figure 6-5 — Management Scenario 3

6.2.3.4 Scenario 4

This scenario shows a single enterprise scenario in which one provider owns the entire network. In this case, conceptually only one SMS is required to manage the network to provide reliable service. However to decrease complexity, the network can be partitioned into subnetworks to provide distributed management.

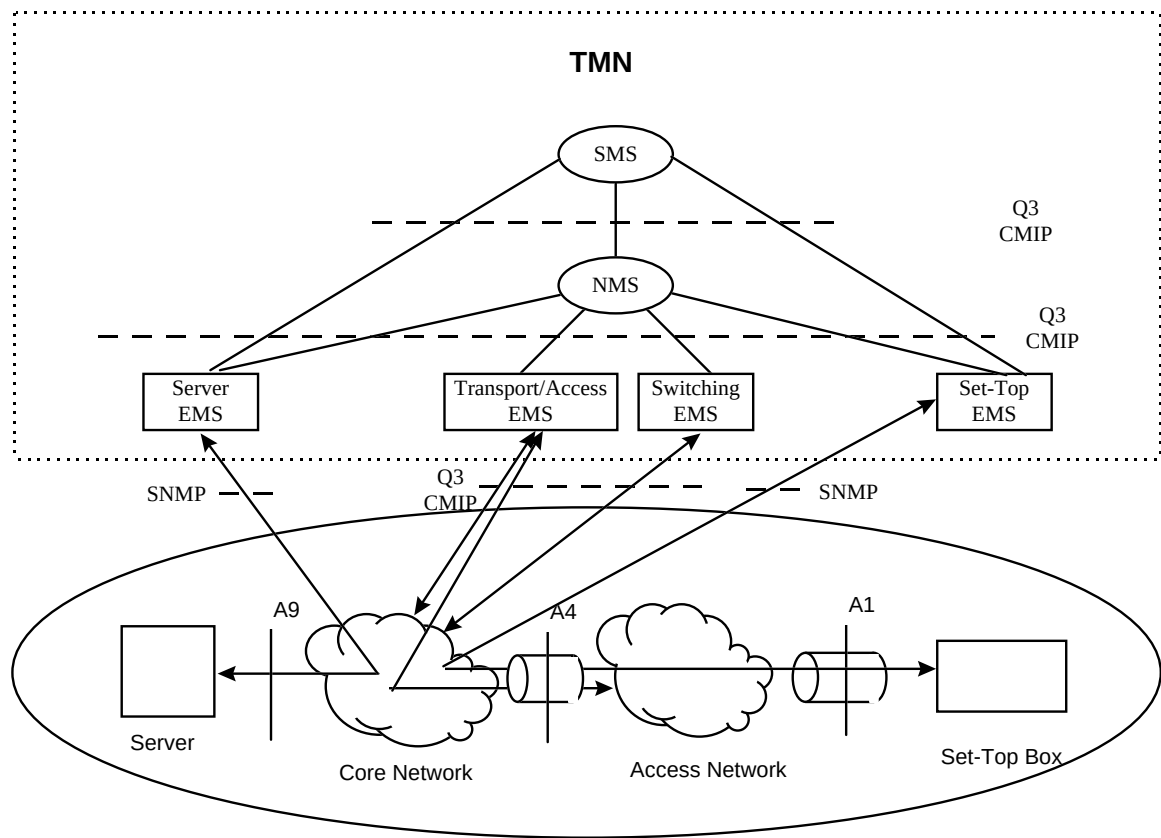


Figure 6-6 — Management Scenario 4

6.2.3.5 Scenario 5

In this scenario the Access Network provider also owns the STB. The end-to-end multimedia system can now be partitioned into management domains based on the ownership of the several components of the system as below.

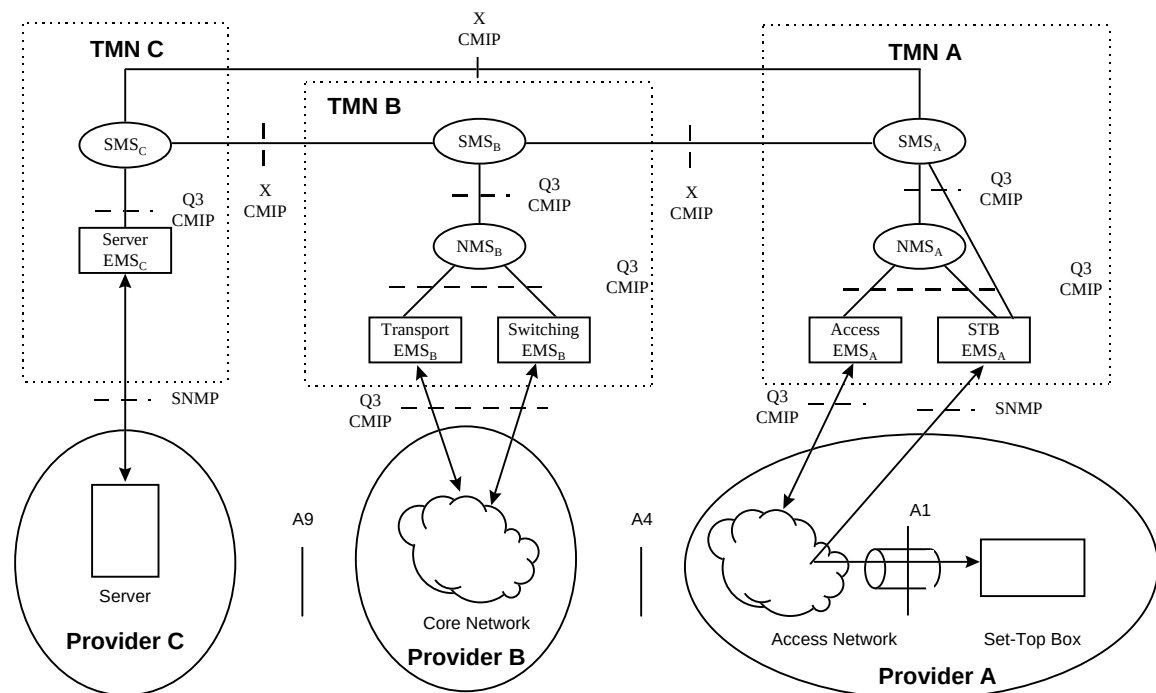


Figure 6-7 — Management Scenario 5

6.2.3.6 Scenario 6

In this scenario all resources belong to the network provider, however the network provider is selling capacity to service providers. Interactions, therefore, occur at the service level but all flowing within the DAVIC network are controlled by the network provider.

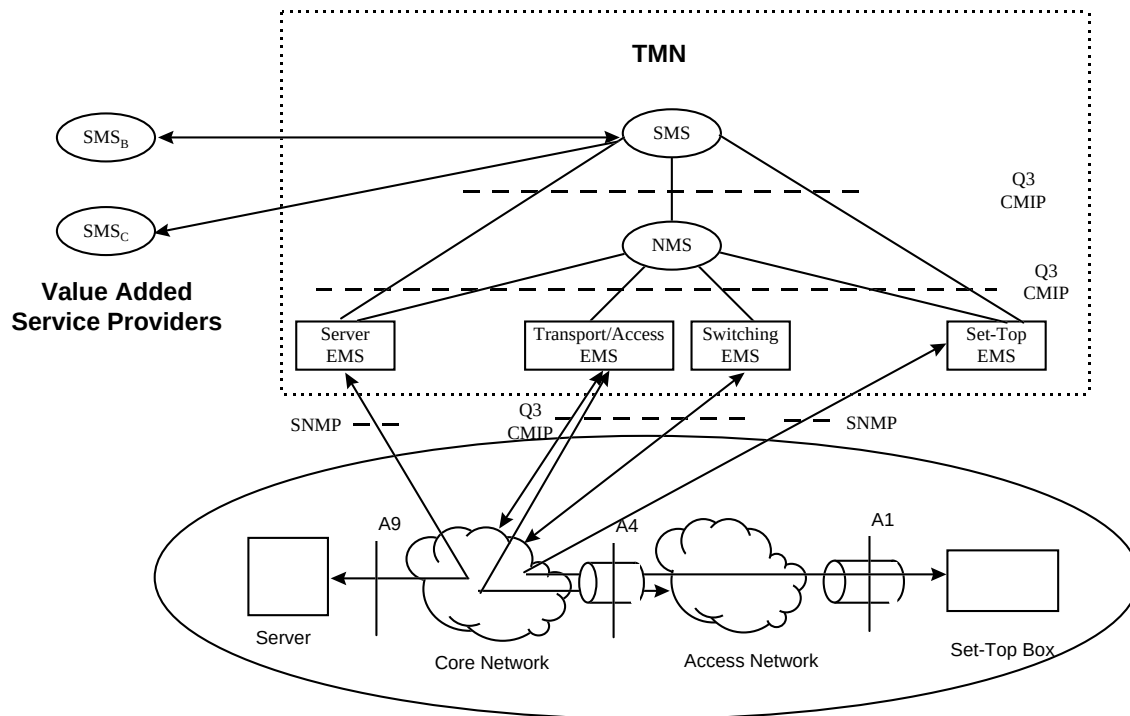


Figure 6-8 — Management Scenario 6

6.3 Interworking Scenarios Between CMIP and SNMP Based Management

This sub-section describes interworking options between CMIP and SNMP based management systems. Three possible scenarios are described. In addition it is noted that semantic integration within the managing system may be possible via an ORB (e.g. CORBA) but this semantic integration is not mandated by DAVIC and the ORB interface is not a DAVIC interface.

The three options are:

1. Integration through the Human-Machine Interface (HMI). The idea is to centralize on a single X-Window terminal the HMIs of several already implemented network managers.
2. Dual protocol stacks. The manager possesses two protocol stacks: a CMIP stack for communicating with CMIP agents, a SNMP stack for communicating with SNMP agents. A common API, such as X/Open XMP can be used over those two stacks.
3. CMIP-to-SNMP proxy. This proxy acts in a manager role regarding the SNMP agents, and in a agent role regarding the manager.
 - The CMIP MIB viewed by the manager is the translation of the SNMP MIB of the SNMP agents.
 - The proxy also does CMIP service emulation over SNMP i.e. it converts traps and/or polling operations into CMIP notifications and also translates scope and filter requests to individual SNMP operations and returns the correct CMIP results to the upstream manager.

As an option to facilitate the programming of management applications in a management system, “semantic” integration may be provided. The goal is to provide the management applications the same procedure calls to perform a given task on a given network resource type regardless of the fact that a particular network resource is accessed via CMIP or SNMP and whether or not it uses a standardized or a proprietary MIB.

This “semantic” integration could be accomplished by internal implementation of an IDL interface with which the internal applications interact. Beneath the IDL interface operations on managed objects are then invoked over dual protocol stack to the appropriate agent.

6.3.1 Integration through the Human-Machine Interface

In this scenario, every agent that is to be integrated is already managed by a management system, specific to a protocol, and offering a complete Human-Machine Interface, based for instance on X-Window. Bringing all the management capability to a central location is then realized allowing access to all these windows through a single X-Terminal. In the simple cut-through scenario this will result in the user having to adapt to a different look and feel for each window. Tighter integration is possible if the individual management systems, independent of protocol, implement the same look and feel and a consistent set of tools.

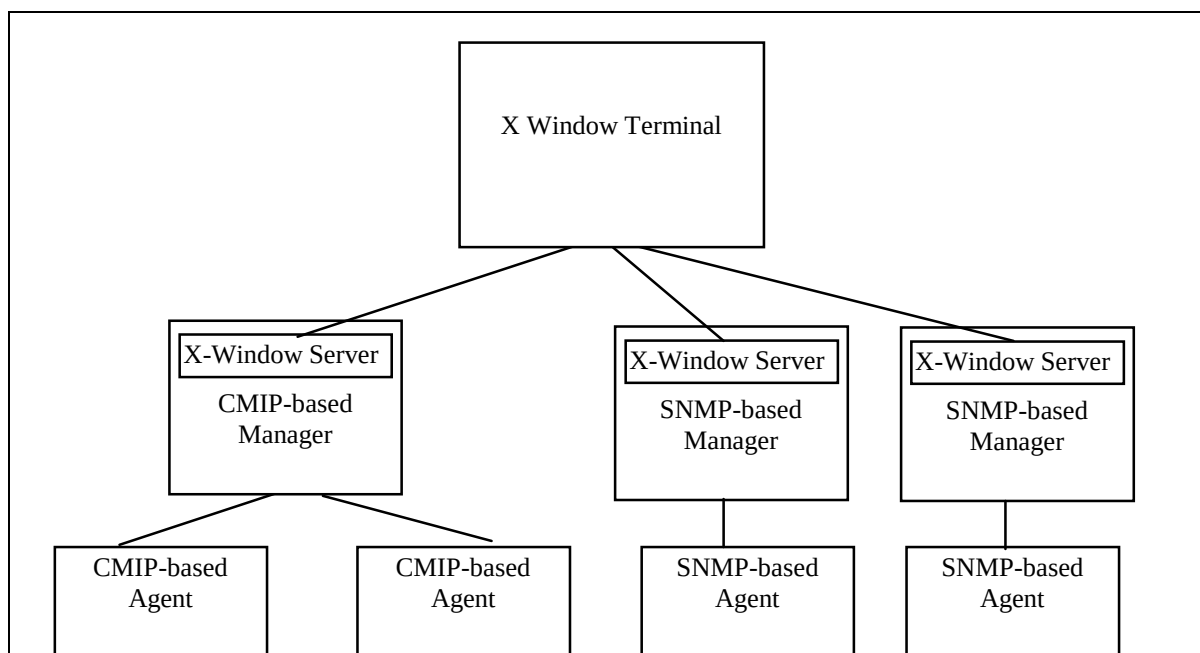


Figure 6-9 — Integration through the Human-Machine Interface

6.3.1.1 Advantages

This architecture offers:

- Ease of implementation
- Ability to integrate both standard and proprietary protocols
- Reuse of existing managers. This is particularly interesting in the case when a managing system, including an HMI and acting as a « black box », is provided by the managed equipment vendor.

6.3.1.2 Disadvantages

The end user remains aware of the multiple management systems. The end user may have to adapt to the « look and feel » of each system. He has to do all the job of integration and coordination between the different manager. For every task he has to do, he has to know and use the tool provided for this task by each manager.

6.3.2 Dual protocol Stacks

In this approach, the manager possesses two protocol stacks : a CMIP stack for communicating with CMIP agents, a SNMP stack for communicating with SNMP agents. Those stacks are accessed and used via different Application Programming Interfaces (APIs). In a refinement of this approach, an API common to both stacks can be defined. An example of such an API is the X/Open Management Protocol API (XMP).

XMP tries, as far as it is possible, to provide the same « C » programming language function calls and data structures for these requests that are common to both protocols (for example, simple Get and Set requests). Of course, those requests that are specific to one protocol correspond to a specific function of the API (for example SNMP GetNext, CMIP filter and scope requests, etc.)

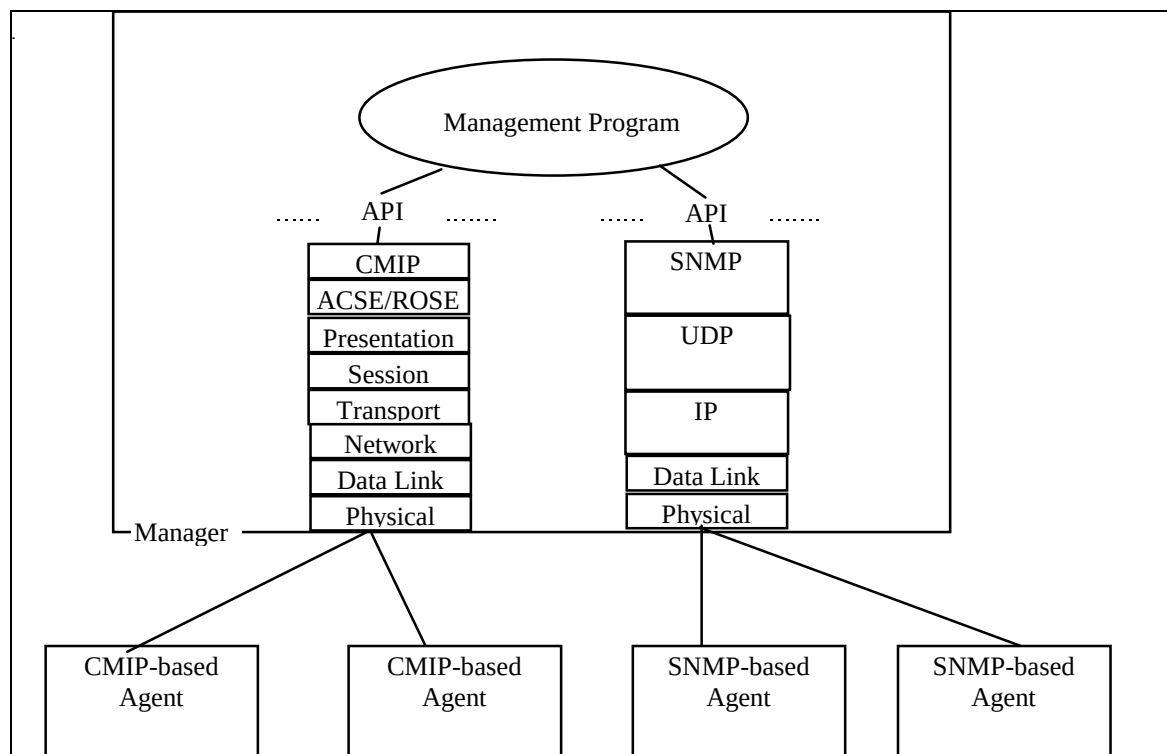


Figure 6-10 — Dual Protocol Stacks Example

6.3.2.1 Advantages

This architecture effectively permits the co-existence of CMIP and SNMP agents.

6.3.2.2 Disadvantages

This scenario doesn't provide real protocol transparency. The management program developer should be aware of which protocol will be used to access the network resources he wants to manipulate. For instance, he will be able to issue GetNext requests only for those resources that will be reached via SNMP.

Should the developer want to emulate a CMIP service like a scope and filter get (i.e. to access a set of resources to verify some properties) over a SNMP table, he would have to download the whole table (using SNMP GetNext). This would cause heavy traffic between the manager and the SNMP agent.

6.3.3 CMIP-to-SNMP Proxy

In this scenario, a CMIP-to-SNMP proxy is used to access a SNMP-based agent. One such proxy is specified by the NMF.

This proxy acts in a manager role with respect to the SNMP agents, and in a CMIP agent role with respect to the manager. The CMIP MIB viewed by the manager is the translation of the SNMP MIB of the SNMP agent. A translation procedure which can be performed almost fully automatic is defined by the NMF. Groups and

RowEntry objects of a SNMP MIB are converted to GDMO objects, SNMP scalar objects are converted to GDMO attributes, SNMP traps are converted to CMIP notifications, etc. All these GDMO objects are registered under a specific registration node, owned by the NMF.

This proxy also does service emulation. For instance:

- If the proxy receives a scope and filter CMIP request from the manager, it will automatically generate the corresponding Get and GetNext requests to the SNMP agent, process the results, filter them and send back to the manager only the required information.
- The proxy will do scheduled polling to emulate CMIP state transition notifications and will convert SNMP poll results into CMIP notifications.
- The proxy will be able to filter the SNMP traps, according to a CMIP Event Forwarding Discriminator set by the manager.

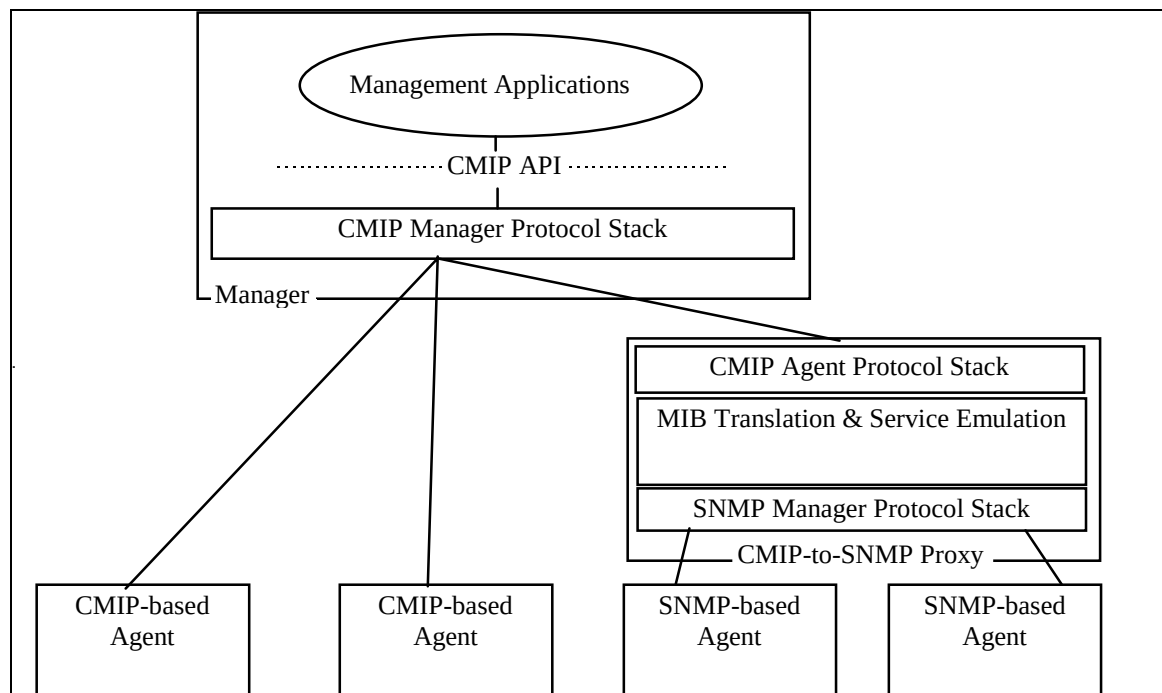


Figure 6-11 — CMIP-to-SNMP Proxy Example

6.3.3.1 Advantages

This architecture provides real protocol transparency. The management application programmer has only to deal with a CMIP API. He can use every service available on a CMIP interface.

The proxy can be located “near” the SNMP agents. The emulation of CMIP services over SNMP will consume high bandwidth only on the short distance between the proxy and the SNMP agents.

6.3.3.2 Disadvantages

This architecture doesn't provide “semantic” transparency, defined as follows : suppose two different network equipments that have the same network functionality (e.g. both of them are ATM cross-connects), but are provided by different vendors and have different agents. One has a CMIP MIB (say *M1*) and the other a SNMP MIB (say *M2*). With the CMIP-to-SNMP Proxy approach, and in particular with the automated MIB translation approach, SNMP MIB *M2* will be translated to a CMIP MIB (say *M3*). However *M1* and *M3* will be different (different object registrations at least, probably not the same conceptual attributes, etc.). This means that to do the same thing on these two equipments (for instance, to create an ATM cross-connection), the management application developer will have to issue two different CMIP requests.

7 Access Network Management Information Model

7.1 Scope of Access Network Management

This section describes the management of Access Network at the A8 interface in the DAVIC reference model. It provides a high level description of the functions required to manage an access network in the Delivery System of the DAVIC reference model. Aspects such as configuration management, fault management and performance management are addressed. An object model supporting these functions is also presented. Figure 7-1 shows the Delivery System Control Plane Model, taken from ISO/IEC 16500-1.

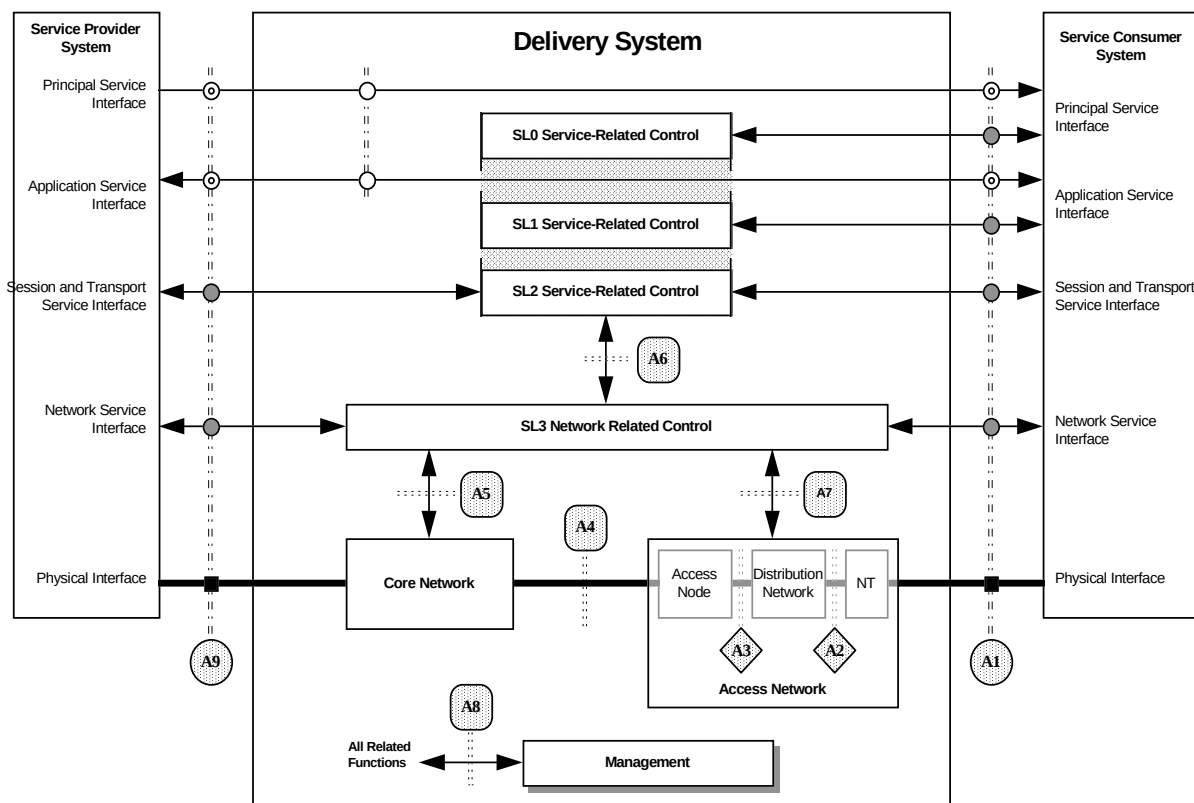


Figure 7-1 — Delivery System Control Plane Model

Services that need to be managed are called broadband services as it is assumed that the core network is a SDH/SONET and ATM based network. Examples of the services considered are Video On Demand (VoD), News On Demand (NoD), Internet Access, etc. The Access Network itself may use various technologies. Currently the technologies that are envisaged for the Access Network are cabled networks such as Hybrid Fiber Coax (HFC), copper networks such as Asymmetric Digital Subscriber Line ADSL and passive optical networks such as FTTC.

In the access network information model, the scope of an Access Network includes an access node (e.g., such as a Host Digital Terminal - HDT) and its subtending distributed components (e.g., such as the Optical Network Units - ONU, Network Terminals - NT, and the fiber, cable or copper pair). It also includes the physical and logical resources within the access node and its subtending components. The resources considered include hardware, software, transport termination points (TPs) of the various transport layers (e.g., SDH or PDH, ATM, DAVIC Information Flow) at the A4 interface (i.e., with the core network) and A1 interfaces (i.e., with the CPEs), intra access network transport TPs, Cross-connections that support nail-up video services. In addition, it also includes logical resources that support the management of the access network.

Clause 7 is organized as follows : first, the access network architecture is considered. This first part sets the framework for the rest of the document. A second part describes the management architecture and functions of the Access Network. These functions are necessary in order to provision and monitor the resource and service

established on the access portion of the network. Lastly, the object model and some simple scenarios are presented in order to illustrate the previous parts.

7.2 Network Delivery Systems Architecture and Interfaces

Figure 7-2 below shows the logical view of the architecture and interface of a Delivery System. The Delivery System being shown is a Cabled Network Delivery System (NDS) defined for DAVIC 1.1. Other NDS and Non-Networked Delivery Systems are for future study. In the figure, no in-house network is considered. In other words the Set Top Box (STB) is directly connected to the Network Termination (NT), i.e. the A1* interface described in DAVIC 1.3.1a Part 4 is nil.

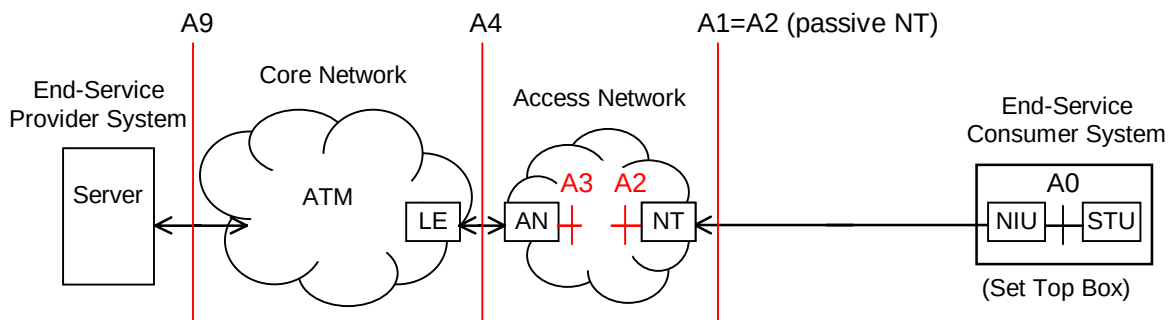


Figure 7-2 — Architecture of a Network Delivery System

Since the NT being considered in this specification is a passive NT, then the A2 reference point (medium and protocol) coincides with the A1 reference point. Depending on the technology, the A3 interface may be identical to A1. For instance, in the ADSL technology, A3 is identical to A1, however for HFC, A3 is different than A2 in terms of medium and lower layers protocol (fiber versus coax).

7.3 Access Network Management Architecture

The model presented here allows for defining an Access Network Management Information Base (MIB) which represents the Access Network resources that are visible to a Network Management System (NMS) in the S5 flow for managing the Access Network across the A8 management interface. The model supports all the management scenarios described in DAVIC 1.3.1a Part 4. That is, the model can be used by a NMS to manage the Access Network regardless of whether the NMS also manages other subsystems. In the management scenarios, Element Management Systems (EMS) may be introduced in conjunction to the NMSs. Figure 7-3 is based on management scenario 5 of DAVIC 1.3.1a Part 4. In this figure an EMS is introduced. The EMS may be provided in order to manage the components of the Access Network.

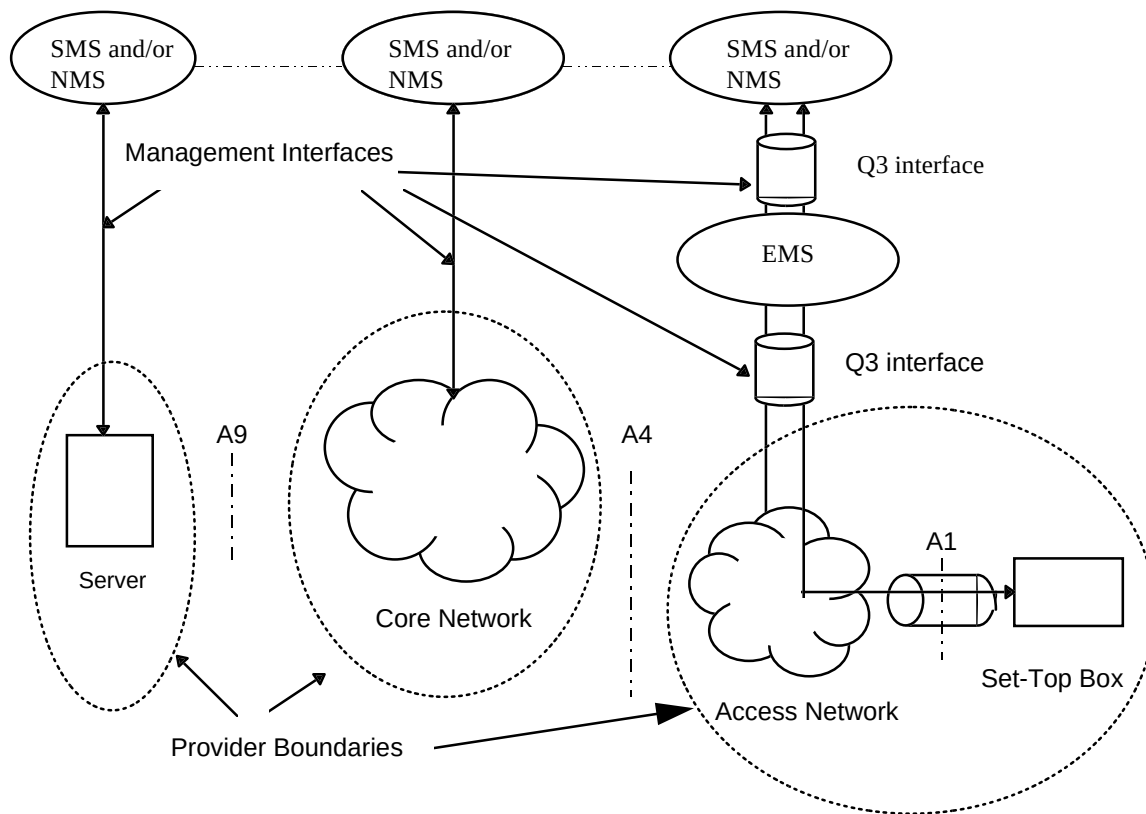


Figure 7-3 — Network Management Architecture - An Example

The Access Network resources that need to be managed include hardware and software resources. Resources that are of particular interest in the S5 flow are those needed for supporting the S1, S2, S3, and S4 flows. Figure 7-4 shows the DAVIC reference points, transaction flows and functional entities are relevant to the Access Network management interface. Details of these DAVIC components can be found, in particular, in ISO/IEC 16500-1 Figure 7.4-1 (Delivery System Control Plane Model) and Figure 8.0-1 (Functional Entities and Relationships).

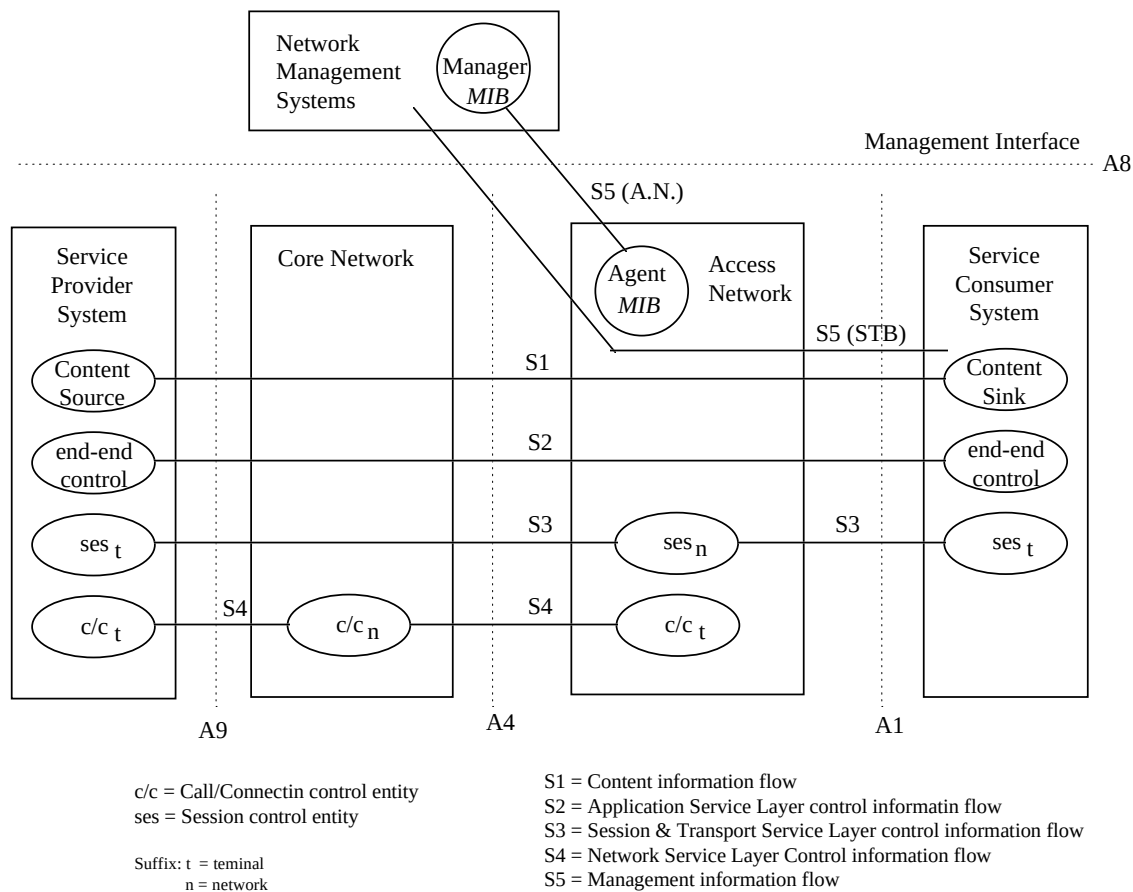


Figure 7-4 — Context of Access Network Management Interface

In Figure 7-4, the Session control entity ses_n and the Call/Connection control entity c/c_n are shown as located in the Access Network. This is one of the physical scenarios, namely Physical Scenario #1, shown in ISO/IEC 16500-2 subclause 9.2. It should be noted that this is not the only physical scenario supported by the model. The Access Network supports more functionality in this physical scenario than in other scenarios. Therefore, the model should be able to support the other physical scenarios also.

This section also models the access network resources that support interface initialization (i.e., the one using DIIP) of the Set-Top-Boxes (STB), the S3 and S5 flows. The S3 flow supports service related control (such as DSMCC UN Config, DSMCC UN Session, and Switched Digital Broadcast Channel Change). The S5 flows support the management of the subtending STBs and the Access Network itself.

The model presented here is a CMIP-based information model. It is an extension to the existing CMIP-based information models with DAVIC specific object classes defined in this document. Many managed object classes defined in ITU-T Recommendations, ATM Forum and industry specifications are reused.

7.4 Access Network Management Functions

Management of the Access Network through the A8 interface provides the functions that allow a manager to monitor and control the network resources. The functions are partitioned according to configuration management, fault management, performance management, accounting management, and security management.

S5 flow is related to network management. Only configuration, fault and performance management are addressed in this version of this part of ISO/IEC 16500. Management of the Core Network and the End-Service Provider System (Server) is logically separated from the management of the Access Network. However, as shown in the management scenarios in ISO/IEC 16500-1, in a physical implementation, the Access Network, Core Network,

and/or Server may be managed by the same system. It is assumed that accounting functions are performed outside the Access Network. Security management is for future study.

7.4.1 Configuration Management Functions

The features and functions that the Access Network Management should provide encompass static network representation as well as provisioning of network resources.

Following is a list of functions that should be implemented for configuration management:

- Functions that support service management system Work Orders (WO) to set up and provision or tear down equipment and end points within a communication circuit.
- Software version management: allow the control and monitoring of the software versions that are currently in place in the Network nodes.
- Dynamic software upgrade. Download of software release. An automatic switch-over is performed by the Network Nodes when the software download is complete.
- Memory backup and restoral. This involves backing up the components of the Access Networks and to store the configuration including ports parameters, cross connects etc.
- Node turn-up : Support the initial installation of a new node in the access network by offering the ability to download initial parameters that are needed. The download may be either a binary image or a series of messages to set up essential parameters.

7.4.2 Fault Management Functions

In the Access Network, the fault management should aid at detecting hardware or software problem in a non-ambiguous way. In order to achieve this, the essential functions that need to be provided by the Access Network may be summarized as follows:

- Management of alarm filters. The Access Network should support functions to filter events and notifications. Alarm Filtering is used to filter the alarm notification depending on the contents of the alarm such as the type and cause of the alarm, the source of the alarm, the severity prior to the reporting, and/or logging of alarms
- Alarm Severity assignment: to associate a perceived severity to alarms, which may be generated by the Network Node. As an example, a non-service affecting event may be reported as a Warning or Minor alarm, while service affecting events may be reported as Major or Critical. The Operations interface should support requests to assign and modify a severity to each possible alarm.
- Alarm storage and retrieval through history logs.
- Support Loopback testing functions.

7.4.3 Performance Management Functions

Performance Management (PM) includes detection of Threshold Crossing Alerts and Trend Analysis. Its role is to help analyze the performance of the network and the Quality Of service provided by the network.

Some of the features associated with performance management in Access Network are listed below:

- PM data collection: the functions that support assignment of periodic PM data interval, suspend and resume the PM data collection, reset a PM data, and schedule the PM data collection.
- Storage of PM data: functions to support assignment of history duration, read (possibly using some filtering criteria, e.g. read only non-zero data) the PM data storage from the history logs, and delete the PM history data.
- Threshold monitoring: the functions that accept a PM threshold and report a threshold crossing.
- PM data reporting functions: This function refers to the ability of reporting PM data either on a scheduled basis or on an on demand basis. Functions to turn on or off the scheduled PM data report.

7.5 Access Network Management Protocol Stack

ISO/IEC 16500-5 (High and mid-layer protocols) recommends either CMIP ITU-T X.711, SNMP RFC 1157, or SNMPv2 RFC 1902 shall be used as a protocol suite to manage the Access Network.

Interworking of SNMP based network elements and CMIP based network elements may be supported as defined in Clause 6 (System Management Architecture) above.

The object model presented later in this section is described in GDMO (ITU-T X.722) and therefore implemented on a CMIP stack described in ISO/IEC 16500-5.

7.6 Management Information Model Overview

7.6.1 Managed Object Classes

In the access network information model, the scope of an Access Network includes an access node (e.g., such as a Host Digital Terminal - HDT) and its subtending distributed components (e.g., such as the Optical Network Units - ONU, Network Terminals - NT, and the fiber, cable or copper pair). It also includes the physical and logical resources within the access node and its subtending components. The resources considered include hardware, software, transport termination points (TPs) of the various transport layers (e.g., SDH or PDH, ATM, DAVIC Information Flow) at the A4 interface (i.e., with the core network) and A1 interfaces (i.e., with the CPEs), intra access network transport TPs, Cross-connections that support nail-up video services. In addition, it also includes logical resources that support the management of the access network.

This version of the specification provides the basis for a generic information model for the access network. In future specifications, extension to the model for specific access network architectures may be made, e.g., through subclassing. Table 7-1 identifies the object classes that form the basis of the generic information model. These object classes are either defined in this document or specified in other documents (international standards or industry). In the table, the object classes are also grouped into fragments for related functionalities.

Table 7-1 — Object classes in the Access Network Information Model

Fragment	Object Class	Source
Access Network	managed Element R1	ITU-T M.3100
Hardware	equipment R1	ITU-T M.3100
	equipment Holder	ITU-T M.3100
	circuit Pack	ITU-T M.3100
Software	software Unit	ITU-T X.744
	software Distributor	ITU-T X.744
Video Transport Specific Termination Points	multimedia TTP Bidirectional/Sink/Source	Clause 7.7
	service Related UN Channel CTP Bidirectional	Clause 7.7
	service Related UN Channel TTP Bidirectional	Clause 7.7
	access Network Management Channel CTP Bidirectional	Clause 7.7
	access Network Management Channel TTP Bidirectional	Clause 7.7
	cpe Management Channel CTP Bidirectional	Clause 7.7
	interface Initialization CTP Bidirectional	Clause 7.7
	interface Initialization TTP Bidirectional	Clause 7.7
SDH/SONET Specific Termination Points (Note 1)	Optical SPI TTP Bidirectional	ITU-T G.774
	Electrical SPI TTP Bidirectional	ITU-T G.774
	rs CTP Bidirectional	ITU-T G.774
	ms TTP Bidirectional	ITU-T G.774
	ms CTP Bidirectional	ITU-T G.774
	aug Bidirectional	ITU-T G.774
	au4 CTP Bidirectional	ITU-T G.774
	vc4 TTP Bidirectional	ITU-T G.774
	au4 4c CTP Bidirectional	Bellcore GR-1114
	vc4 4c TTP Bidirectional	Bellcore GR-1114
PDH Specific Termination Points	ds3 Line TTP Bidirectional	ANSI T1.240
	ds3 Line CTP Bidirectional	ANSI T1.240
	ds3 Path TTP Bidirectional	ANSI T1.240
	ds3 PLCP Path TTP Bidirectional	ATMF af-nm-0027
	ds3 PLCP Path CTP Bidirectional	ATMF af-nm-0027
ATM Specific Termination Points & Resources	tc Adaptor TTP Bidirectional	ATMF af-nm-0027
	vp CTP Bidirectional	ATMF af-nm-0027
	vp TTP Bidirectional	ATMF af-nm-0027
	vc CTP Bidirectional	ATMF af-nm-0027
	vc TTP Bidirectional	ATMF af-nm-0027
	interworking vc TTP Bidirectional (for non-ATM A1)	ATMF af-nm-0072
	aalProfile	ATMF af-nm-0071
	dss2 Sign Channel Tp	Bellcore GR-1114
	atm Saal Uni Protocol Profile	Bellcore GR-1114
	uni (or GR-1114: uniBCR)	ATMF af-nm-0027

Table 7-1 — Object classes in the Access Network Information Model (Cont.)

Fragment	Object Class	Source
Nail-up Connection	fabric R1	ITU-T M.3100
	mp Cross Connection	ITU-T M.3100
	cross Connection	ITU-T M.3100
Video Service Related	broadband Drop	Clause 8
	cpe	Clause 8
	cpe Authorization	Clause 8
	broadcast Program	Clause 8
	broadcast Program Feature	Clause 8
Generic Management Support	event Forwarding Discriminator	ITU-T X.721
	log	ITU-T X.721
	object Creation Record	ITU-T X.721
	object Deletion Record	ITU-T X.721
	attribute Value Change Record	ITU-T X.721
	state Change Record	ITU-T X.721
Fault Management	alarm Record	ITU-T X.721
	alarm Severity Assignment Profile	ITU-T M.3100
	current Alarm Summary Control	ITU-T Q.821
	testActionPerformer	ITU-T X.745
PDH Specific Termination Points	Generic Performance Monitoring Objects	ITU-T Q.822
	SDH Performance Monitoring Objects	ITU-T G.744-01 /06
	SONET Performance Monitoring Objects	ANSI T1.119-02
	PDH Performance Monitoring Objects	ANSI T1.247
	ATM Performance Monitoring Objects	ATMF af-nm-0027

Note 1:

These objects are needed if SDH or SONET is used between the core network and the access network.

7.6.2 Object Class Relationships

For video-specific object classes, their inheritant relationship and naming relationship are shown in Figure 7-5 and Figure 7-6 below. For object classes that are defined in other documents, the inheritant and naming relationship can be found in the corresponding source documents.

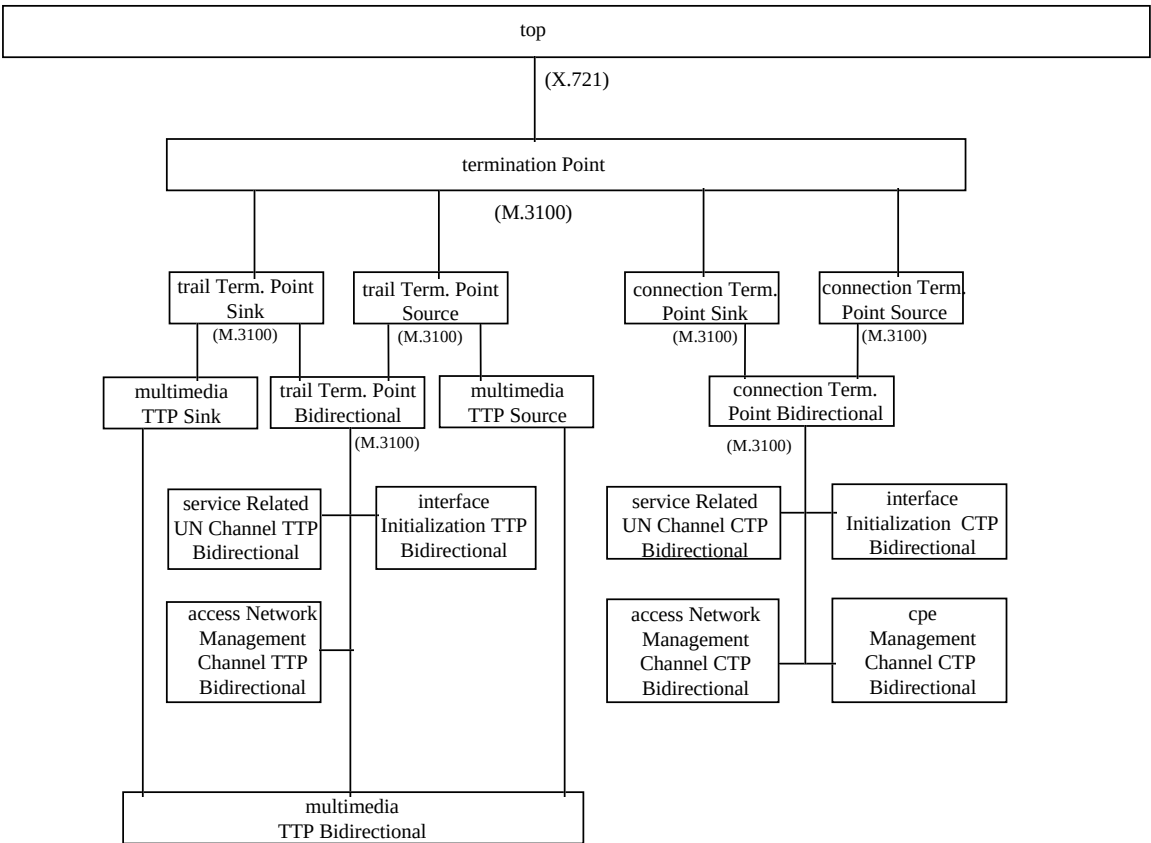


Figure 7-5 — Inheritance Relationship of Video-Specific Object Class

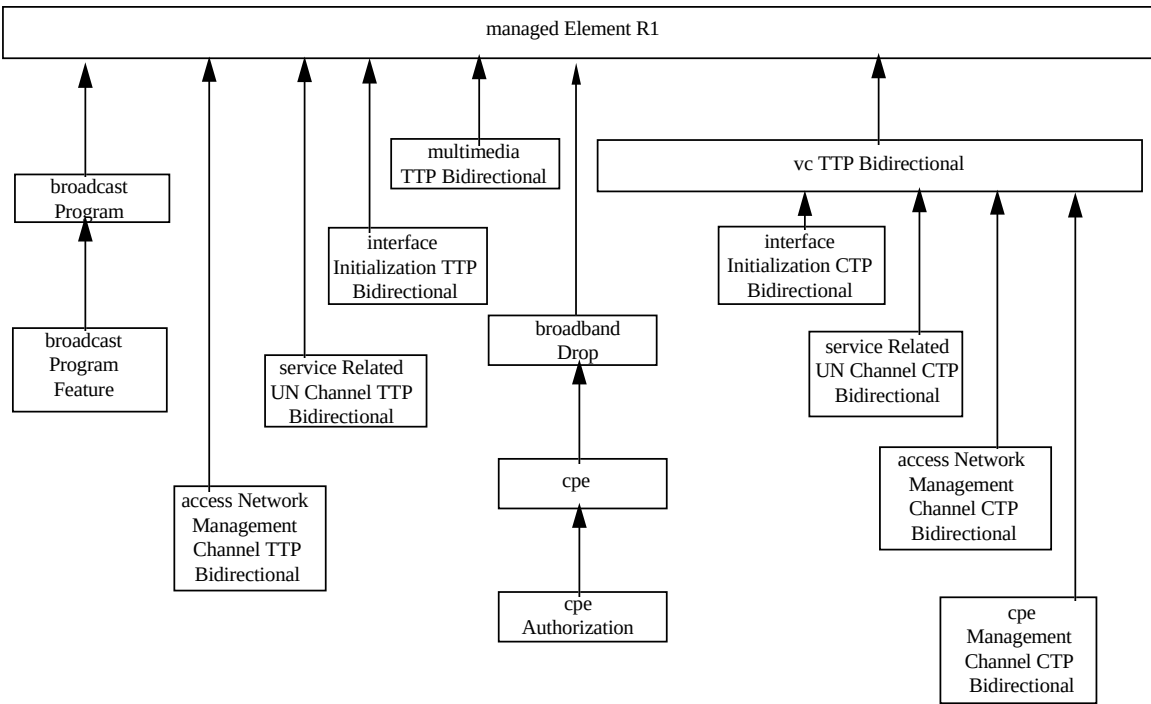


Figure 7-6 — Naming Relationship of Video-Specific Object Class

The following figure shows the containment relationship of the physical components of a access network. It also shows the cardinality of each association. The local root of the access network is represented by a

managedElementR1 object, which contains an equipmentR1 object representing the access node. The access node in turn contains multiple ONUs (represented by the equipmentR1 objects). Each ONU in turn contains multiple Network Terminals (NT), which are also represented by instances of the equipmentR1 object classes. Within the access node, ONUs and NTs, the shelf (or slot) and plug-in card are represented as instances of equipmentHolder and circuitPack.

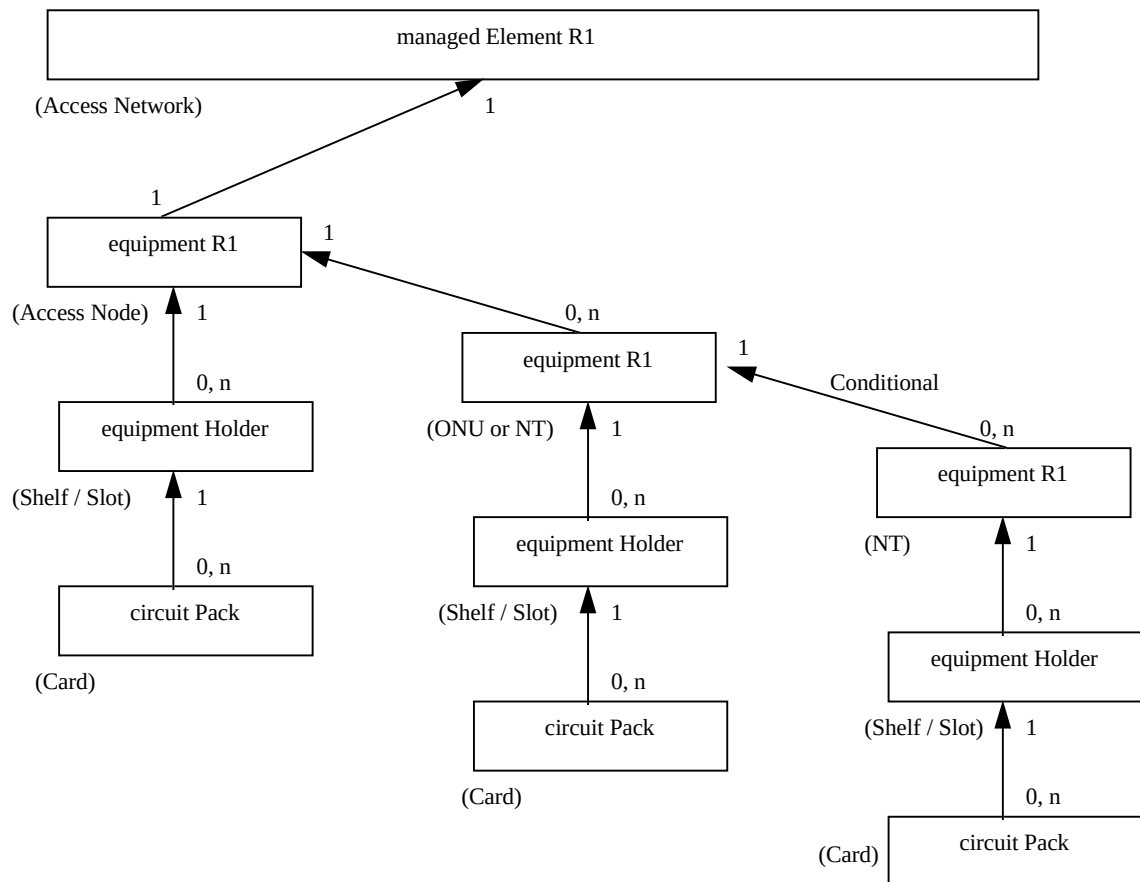


Figure 7-7 — Example of Physical Components Entity Relationship.

The following figure shows the relationship among the termination points. Only the video-specific termination points and their directly associated termination points are shown. Therefore the SDH/SONET and PDH termination points are not shown in the figure. In general, TTP (trail termination point) objects are contained directly in the Managed Element. TTP and CTP (connection termination point) are associated with each other through the downstreamConnectivityPointer and upstreamConnectivityPointer. A trail is terminated/originated with two TTP objects. An instance of tcAdaptorTTP at the A1 interface (i.e., toward the CPE) is supported by an instance of multimediaTTP object. An instance of tcAdaptorTTP at the A4 interface (i.e., toward the core network) is supported by an instance of vc4TTP or other SDH/SONET object.

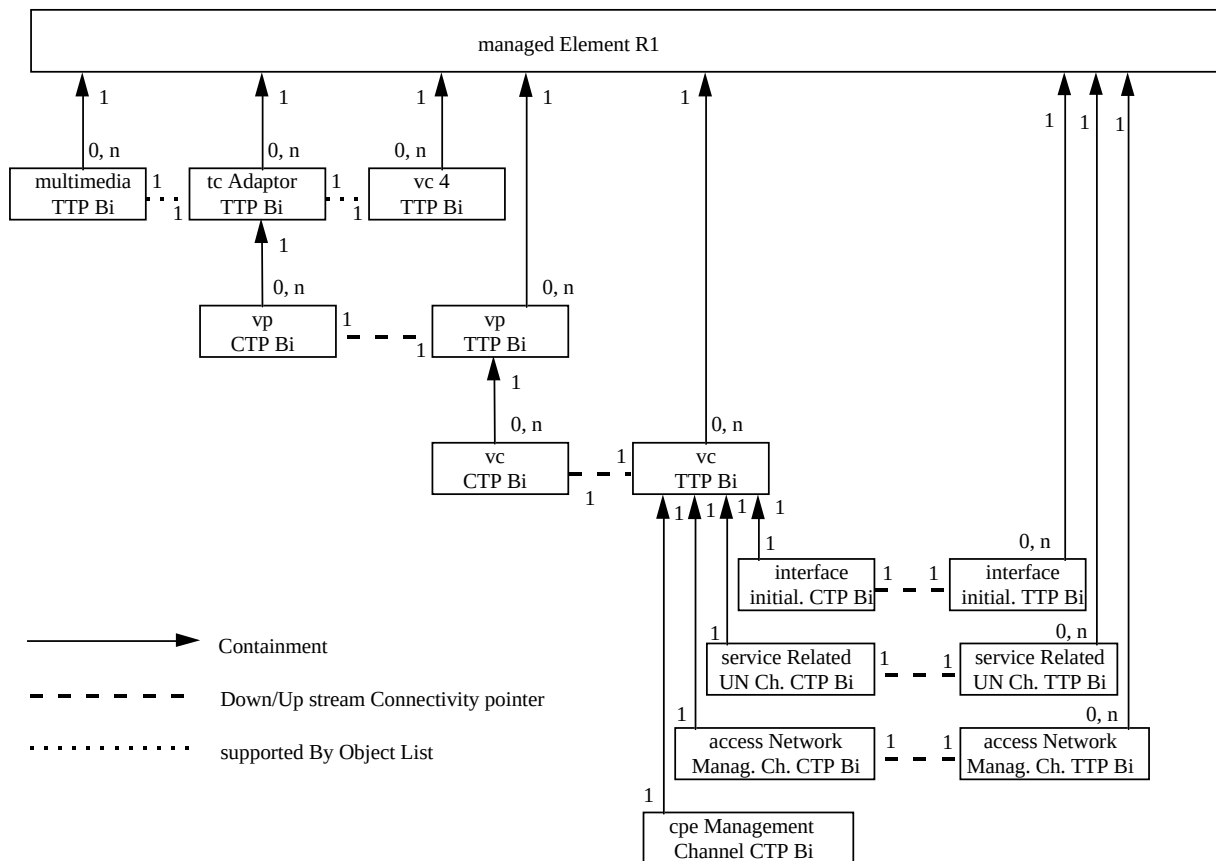


Figure 7-8 — Entity Relationship of Termination Points

The following figure shows the relationship between transport termination point objects and their underlying hardware resources. In general, TTP objects are supported by hardware objects, such as circuitPack.

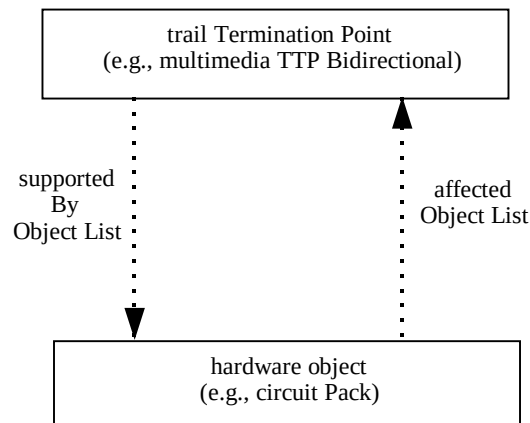


Figure 7-9 — Entity Relationship of TTP and Hardware

The following figure shows the relationship of the fabric, mpCross-connection, cross-connection, and termination point objects. In the Point-to-Multipoint cross connect, transport information is sent from a termination point sink object to one or more termination point source objects. It should be noted that the sink and source characteristic of a termination point is from the perspective with respect to the exterior of the network element (or access network in this case). That is, a termination point sink object is where the transport information from the network terminated. On the other hand, the termination point source object is where the transport information to the network originated. Inside of the network element (or the access network in this case), transport information received from the network at the termination point sink is cross connected to a termination point source and transmitted to the network.

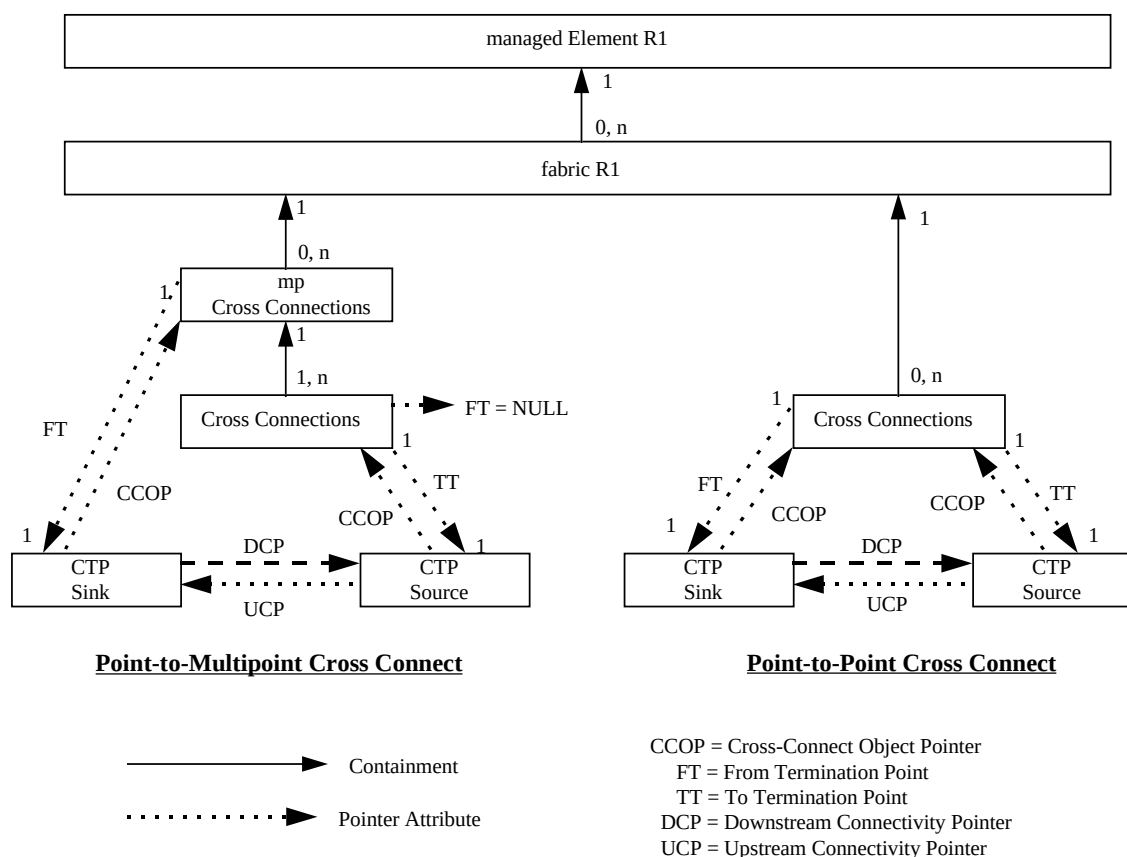


Figure 7-10 — Entity Relationship of Cross-Connect

7.6.3 Application of the Model to DAVIC Information Flows

The transport model of the Access Network is based on the generic functional architecture of transport networks described in ITU-T G.805 and the generic network information model defined in ITU-T M.3100. Two major types of object classes are used for the transport function of the Access Network, namely Trail Termination Point (TTP) object classes and Connection Termination Point (CTP) object classes. A trail is an entity in a transport layer network, which is responsible for the integrity of transfer of information from one or more other layer networks. A connection is an entity, which is responsible for the transparent transfer of information between its two end points, namely the CTPs. A connection is a component of a trail. Several connections can be bundled into a higher rate trail. A sequence of one or more connections are linked together to form a trail. A connection may be either uni- or bi- directional. A trail is composed of two TTPs and one or more connections and associated CTPs.

The Access Network system management information model consists of object classes representing the transport configuration, hardware and software resources of the Access Network. It also includes object classes to support system management of the Access Network. A managing system manages the resources of the Access Network through managing instances of these object classes.

The following subsection describes the information model of an Access Network for supporting the transport configuration of information flowing through the Access Network. In the information model, object instances are used to represent resources or functions of the Access Network. These instances are related to each other through containment and optionally through referencing. Figures are used to illustrate the relationship. In the figures in this section, object instances are illustrated as boxes. A containment relationship is depicted pictorially as a box containing other box. A referencing relationship is shown using arrows pointing from the referencing object to the referenced object.

7.6.3.1 Initial Transport Configuration

Figure 7-11 shows the initial transport configuration of an Access Network. The Access Network is modeled as an instance of the managedElementR1 object class and represented by the outermost box in the figure. There are several factors that determine the transport configuration of an Access Network: whether ATM is employed at the A1 interface (i.e., at the consumer side of the access network) for carrying the DAVIC information flows (e.g., S1, S2, S3, S4, S5 and the DIIP flows), whether PDH or SONET/SDH is used at the A4 interface (i.e., at the core network side of the access network) for the physical transport of the information flows, and whether the Session control entity (sesn) and Call/Connection control entity (C/Cn) are located in the Access Network. In the figure, both SDH/SONET and PDH are shown in the same figure, instead of using several figures, with the understanding that it is not required for an Access Network implementation to support both transport technologies at the same time.

At the A4 interface, if SDH/SONET technology is used for the physical transport, then the SDH termination point objects (namely optical SPI TTP Bidirectional or electrical SPI TTP Bidirectional, rs CTP Bidirectional, rs TTP Bidirectional, ms CTP Bidirectional, ms TTP Bidirectional, aug Bidirectional, au4 CTP Bidirectional or au44c CTP Bidirectional, vc4 TTP Bidirectional or vc44c TTP Bidirectional) will exist.

If PDH technology is used for the physical transport at the A4 interface, the PDH termination point objects will exist in the Access Network. In the figure, PDH objects for the case of DS3 are used (namely, ds3 Line TTP Bidirectional, ds3 CTP Bidirectional, ds3 Path TTP Bidirectional, ds3 PLCP Path CTP Bidirectional, and ds3 PLCL Path TTP Bidirectional).

It is assumed that in both the SDH/SONET and PDH cases, ATM is used for carrying the S1, S2, S3, S4, and S5 flows. The ATM termination point object (namely, tc Adaptor TTP Bidirectional, vp CTP Bidirectional, vp TTP Bidirectional, vc CTP Bidirectional, and vc TTP Bidirectional -- or its subclass interworking VC TTP Bidirectional) will exist at the A4 interface.

At the A1 interface, the access lines (e.g., copper pair, coax cable, or fiber) connect the service consumers with the Access Network to support the physical transport of information flows. In the Access Network, the origination and termination function of an access line is modeled as a multimedia TTP Bidirectional (or an-multimedia TTP Source for broadcast only access network) instance. It is also assumed that the A1 interface is ATM-based.

For simplicity, only one A4 side vp TTP Bidirectional object and one A1 side vp TTP Bidirectional object are shown in the figure and all the vc CTP Bidirectional objects are contained in these two objects. In reality, there may be more than one vp TTP Bidirectional objects on both sides.

In the initial stage, for each access line at the A1 interface, there shall be one DAVIC Interface Initialization connection (STB interface initialization using the DAVIC Interface Initialization Protocol, DIIP, for establishing S3), multiple S5 connections (one for each STB). For each access line, the DIIP connection is shared by all its service consumers. At the A4 interface, there shall be one S5 connection for the Access Network itself and multiple S5 connections (one for each STB). The CTPs of these connections are modeled as interface Initialization CTP Bidirectional, cpe Management Channel CTP Bidirectional, and access Network Management Channel CTP Bidirectional.

In the Access Network, the function of formulating/originating and terminating/processing the DIIP messages is modeled as instances of interface Initialization TTP Bidirectional. An interface Initialization TTP Bidirectional object and an interface Initialization CTP Bidirectional object are associated with each other using the downstream Connectivity Pointer and upstream Connectivity Pointer attributes of both objects. In the figure, only the downstream Connectivity Pointers are shown.

The function of formulating/originating and terminating/processing the S5 flow for managing the Access Network is modeled as instances of access Network Management Channel TTP Bidirectional. A access Network Management Channel TTP Bidirectional object and an access Network Management Channel CTP Bidirectional object are associated with each other using the downstream Connectivity Pointer and upstream Connectivity Pointer attributes of both objects.

The Access Network is responsible only for the transparent transfer of the S5 flows that belong to the STBs. Therefore the TTPs of these S5 flows do not exist in the Access Network. The Access Network is responsible for connecting the A4 side cpe Management Channel CTP Bidirectional with the A1 side cpe Management Channel CTP Bidirectional for completing the end-to-end STB S5 flows. The connecting relationship is indicated by the downstream Connectivity Pointer and upstream Connectivity Pointer attributes of both objects.

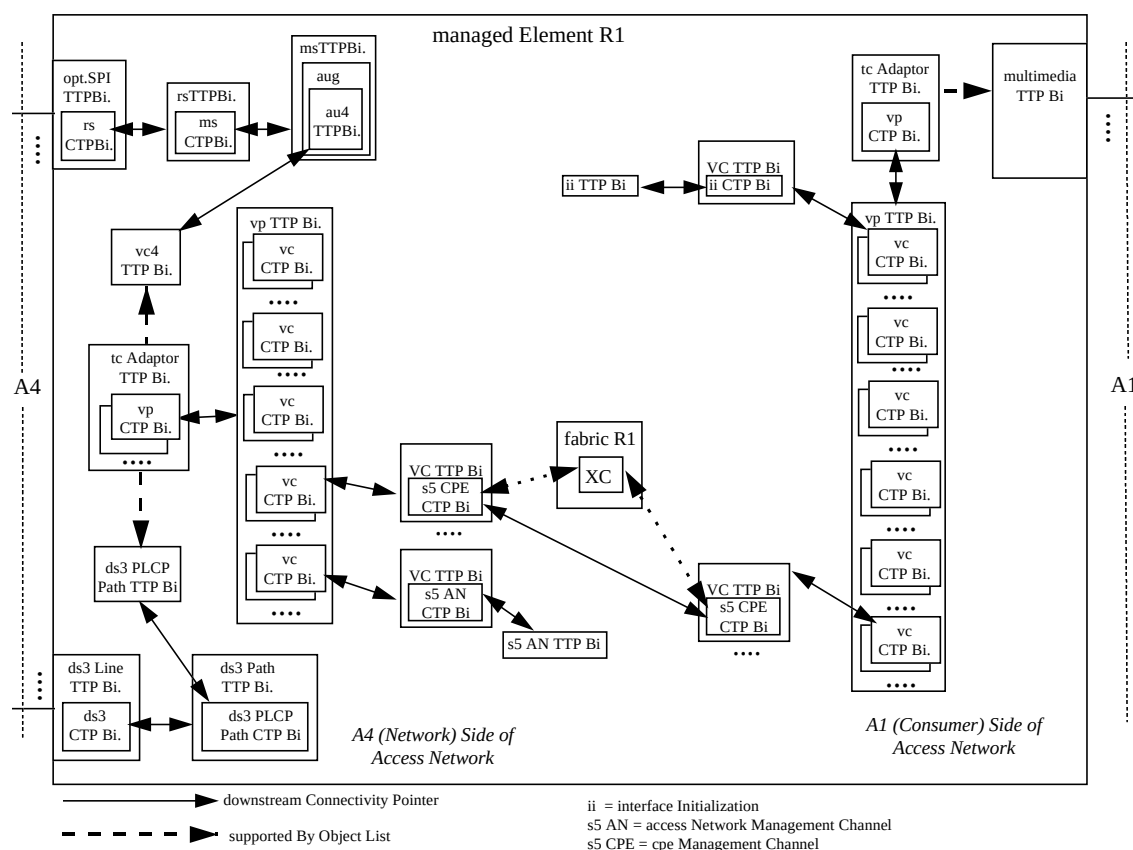


Figure 7-11 — Access Network Initial Transport Configurations

7.6.3.2 Transport Configuration for S3 Flow

Figure 7-12 shows the configuration of the Access Network when the S3 connections have been established. The S3 connection is set up using DIIP.

The CTP of the S3 connections are modeled as service Related UN Channel CTP Bidirectional. In the figure, it is assumed that the Session control entity ses_n is not located in the Access Network. If ses_n is located in the Core Network, the scenario is described in Physical Scenario #2 (where the Call/Connection control entity C/Ct is located in the STB) and Physical Scenario #3 (where C/Ct is located in the core network) of ISO/IEC 16500-2. In both cases, the Access Network is responsible for transparent transfer of the S3 flow, i.e., directly connecting the A4 side and A1 side CTPs with each other.