ETSI TR 101 477 V1.1.1 (2000-06)

Technical Report

Guidelines for the use of ETSI TS 101 674-2

Reference

DTR/EASI-00006

Keywords

ATM, interface, interoperability

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

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 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://www.etsi.org/ipr).

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 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 jointly produced by ETSI Project ATM Services Interoperability (EASI) and Eurescom P813.

The present document was developed by EURESCOM P813 as Deliverable 1 and made freely and publicly available to ETSI EASI for publication.

It was appreciated that a solely technological NM solution would be inadequate, and therefore the solution has been designed starting from a "business model" and a "processes model". These models provide descriptions of methodologies and "roles" considered relevant for managing all aspects of ATM interconnection services.

Potential benefits

The present document, positioned as a detailed guidelines document in support of a formal ETSI technical specification TS 101 674-2 [2], is aimed at supporting operators considering the introduction of ATM interconnect services to other operators. It provides operators with a starting point for understanding the processes and NM technologies needed to establish and manage these interconnected ATM networks.

It allows an operator to understand the context and rationale for:

- the general business models for achieving interconnection;
- the pre-service processes needed to establish an inter-operator agreement;
- using ETSI and ITU-T specifications to achieve the interconnection of NM Systems.

It is intended that the present document is used in conjunction with a multilaterally agreed Standard Interconnect Agreement (SIA) and an agreed "Code of Practice" used as the basis of ***bilateral contracts*** between co-operating operators. These are provided in the Broadband Service Operator Interconnect Handbook [3].

The descriptions and solutions contained in the present document are aligned with known requirements for ATM service creation and management in a complex and interconnected marketplace. These include the ability to inter-connect operator's networks at the ATM VP, and VC levels, using automated management interfaces. These can be used as an infrastructure for a range of end user services such as: voice, those based upon IP protocols such as IP VPNs, and access technologies such as ADSL. NM technical solutions are aligned with both current and envisaged interconnection processes, and use a realistic business model for ATM inter-connect service introduction. The technical solutions described are based on existing or planned enhancements to public standards, and should therefore influence the equipment vendors in the design of products suitable for ATM interconnection services.

Specific technical areas considered and solutions provided

The present document provides identification, discussion and/or specifications for technical and operational requirements for the NM solution to support ATM interconnection services. The use of Telecommunications Management Network (TMN) and Open Systems Interconnection (OSI) principles and standards is generally assumed, although the principles and processes can be readily adapted to use of other technologies - such as CORBA and IP technologies (e. g. sockets, ftp, HTML, XML).

All management functional areas of the TMN model, including Configuration, Fault, Performance, Security and Accounting are considered in relation to the requirements for ATM interconnection services. Management solutions are described and in some cases, problems and limitations are identified where further study is required.

In summary, the present document provides:

In the main part

- A definition of the Technical Principles of the ATM Interconnection Services.
- A Business Model for describing a set of Roles that can be performed by Operators in operating ATM Interconnect Services.
- A description of "what" requirements there are on: the processes and roles that have to co-operate in managing the establishment of ATM Interconnect Service, and the administration of the Interconnection Service and its operation. A major requirement that was identified is traffic and capacity planning processes.

In annexes A to E

- Descriptions are provided for "how" various requirements can be met and detailed data models are elaborated. In addition, the principles for designating ATM connections and further details on security management processes are discussed.

In annexes F to N

- Proposals for interworking processes operating between automated and manual NM interfaces are provided together with additional information supporting matters described in the main part of the present document.

1 Scope

The present document contains detailed guidelines to be used in association with ETSI TS 101 674-2 [2].

It provides additional details for a "Framework Solution" for Network Management (NM) to support interconnections between European ATM network management platforms utilized for the provision of (semi-) permanent Virtual Path and Virtual Channel connections. It addresses NM requirements, processes and interface specifications. The Framework for Inter-operator Processes and Interface Specifications covers all NM functional areas where network interoperability and agreements are needed to support ATM interconnection services.

The information contained in the present document is restricted to a level of functionality which is considered to be practicable for an initial phase of implementation, - i.e. a "Phase 1" specification. The present document identifies working details that need to be agreed between operators to establish interconnect services.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETSI TS 101 674-1: "Technical Framework for the provision of interoperable ATM services; Part 1: NNI-Interface User and Control plane specification (including network functions and service aspects) Phase 1".

[2] ETSI TS 101 674-2: "Technical Framework for the Provision of Interoperable ATM Services; Part 2: Network Management (X-Interface) Specification for Phase 1 Implementation".

[3] EURESCOM P813 Deliverable 3: "Broadband Service Operator Interconnect Handbook".

[4] ETSI ETS 300 298-1: "Broadband Integrated Services Digital Network (B-ISDN); Asynchronous Transfer Mode (ATM); Part 1: B-ISDN ATM functional characteristics [ITU-T Recommendation I.150 (1995)]".

[5] ETSI ETS 300 298-2: "Broadband Integrated Services Digital Network (B-ISDN); Asynchronous Transfer Mode (ATM); Part 2: B-ISDN ATM layer specification [ITU-T Recommendation I.361 (1995)]".

[6] ETSI EN 300 820-1: "Telecommunications Management Network (TMN); Asynchronous Transfer Mode (ATM) management information model for X interface between Operation Systems (OSs) of a Virtual Path (VP)/Virtual Channel (VC) cross connected networks; Part 1: Configuration Management".

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

[8] EURESCOM P408 Pan-European TMN - Experiments and Field Trial Support Deliverable 6: "Specifications of the Xcoop Interface for ATM Network Management: (Tests specified in D6 Volume 4 Annex 3: Laboratory Methods and Abstract test suites for validation of the Xcoop interface".

[9] EURESCOM P612 Deliverable 2, Volume 2 (1998): "TMN X-interface Specifications for Trouble Ticketing".

[10] ETSI EN 300 820-2: "Telecommunications Management Network (TMN); Asynchronous Transfer Mode (ATM) management information model for the X interface between Operation Systems (OSs) of a Virtual Path (VP)/Virtual Channel (VC) cross connected networks; Part 2: alarm management".

[11] EURESCOM Project P811 Deliverable 1 (1999): "Reference Framework for OSS Interconnection".

[12] ITU-T Recommendation I.371 (1996): "Traffic control and congestion control in B-ISDN".

[13] ITU-T Recommendation M.1400 (1997): "Designations for International Networks", including Amendment 1.

[14] ATM Forum Traffic Management Specification, version 4.1, 1999.

[15] EURESCOM Project P707: General information in Deliverables 2 and 3.

[16] EURESCOM P813 Deliverable 4: "Requirements for network management of switched ATM services and IP VPN Quality of service".

[17] ITU-T Recommendation X.700 (1992): "Management Framework For Open Systems Interconnection (OSI) For CCITT Applications".

[18] ITU-T Recommendation I.751 (1996): "Asynchronous transfer mode management of the network element view".

[19] ETSI ETS 300 469 (1998): "Broadband Integrated Services Digital Network (B-ISDN); Asynchronous Transfer Mode (ATM); Management of the network element view [ITU-T Recommendation I.751 (1996)]".

[20] ITU-T Recommendation X.721 (1992): "Information technology – Open Systems Interconnection – Structure of management information: Definition of management information".

[21] ITU-T Recommendation M.3100 (1992): "Generic network information model".

[22] ETSI ES 200 653: "Telecommunications Management Network (TMN); Network level generic class library".

[23] ITU-T Recommendation I.630 (1998): "ATM protection switching".

[24] "Towards Resilient Networks and Services" (undated), P. Georgatsos and Y. T'Joens, from Guideline NIG-G5 of the NIG Chain (taken from the EU ACTS projects).

[25] EURESCOM P612 Deliverable 1, Volume 3, Annex B (1997): "Harmonised rRequirements for trouble ticketing".

[26] ITU-T Recommendation M.1530 (1992): "Network maintenance information".

[27] ITU-T Recommendation M.3208.1 (1997): "TMN management services for dedicated and reconfigurable circuits network: Leased circuit services".

[28] ITU-T Recommendation X.790 (1995): "Trouble management function for ITU-T applications".

[29] ITU-T Recommendation M.1540 (1994): "Exchange of information for planned outages of transmission systems".

[30] ITU-T Recommendation M.1550 (1992): "Escalation procedure".

[31] ITU-T Recommendation M.1560 (1992): "Escalation procedure for international leased circuits".

[32] ETSI EN 300 820-3: "Telecommunications Management Network (TMN); Asynchronous Transfer Mode (ATM) management information model for the X interface between Operation Systems (OSs) of a Virtual Path (VP)/Virtual Channel (VC) cross connected networks; Part 3: VP Performance management ".

[33] EURESCOM Project P708, Deliverable 2 (1999): "Xcoop Specification for ATM VP Performance Management".

[34] EURESCOM Project P708 Deliverable 1, Part 1: "Usage Measurements for Accounting Management – The Xcoop Interface". Also Deliverable 3 (1999): "Specification of accounting Management for the Xcoop Interface".

[35] ITU-T Recommendation D.224: "Charging and Accounting Principles for ATM/B-ISDN".

[36] EURESCOM Project P710: General reference to all Deliverables.

[37] EURESCOM Project P708, PIR7.3 version 1 (1999).

[38] EURESCOM Project P708 Deliverable 5 (1999): "Proposed enhancements to ETSI standards (EN 300 820-1 and EN 300 820-2)".

[39] OMG CORBA 2.2/IIOP Specification (1998). Available at: http://www.omg.org/library/c2indx.html and: ftp://ftp.omg.org/pub/docs/formal/98-07-01.pdf.

[40] ETSI TS 101 675-1: "Technical Framework for the Provision of Interoperable ATM Services; Network-Network Interface (NNI) User and Control Plane Specification". (Including Network Functions and Service Aspects) Phase 2".

[41] ETSI TR 101 673 (V1.1): "Technical Framework for the Provision of Interoperable ATM Services; Overview".

[42] Void.

[43] ITU-T Recommendation E.191 (1996): "B-ISDN numbering and addressing".

[44] ITU-T Recommendation E.164 (1997): "The international public telecommunications numbering plan".

[45] ITU-T Recommendation D.170 (1998): "Monthly telephone and telex accounts".

[46] ITU-T Recommendation D.285 (1996): "Guiding principles for charging and accounting for intelligent network supported services".

[47] ITU-T Recommendation D.232 (1997): "Specific tariff and accounting principles applicable to ISDN supplementary services".

[48] ITU-T Recommendation D.230 (1995): "General charging and accounting principles for supplementary services associated with international telecommunication services provided over the Integrated Services Digital Network (ISDN)".

[49] ITU-T Recommendation D.225 (1997): "Charging and accounting principles to be applied to frame relay data transmission service".

[50] ITU-T Recommendation D.212 (1996): "Charging and accounting principles for the use of Signalling System No. 7".

[51] ITU-T Recommendation D.211 (1998): "International accounting for the use of the signal transfer point and/or signalling point for relay in Signalling System No. 7".

[52] ITU-T Recommendation D.210 (1994): "General charging and accounting principles for international telecommunication services provided over the Integrated Services Digital Network (ISDN)".

[53] IETF RFC 2078 (1997): "Generic Security Service Application Program Interface, Version 2" - J. Linn.

[54] ITU-T Recommendation E.735 (1997): "Framework for traffic control and dimensioning in B-ISDN".

[55] ITU-T Recommendation G.805 (1995): "Generic functional architecture of transport networks".

[56] ITU-T Recommendation I.356 (1996): "B-ISDN ATM layer cell transfer performance".

[57] ITU-T Recommendation I.357 (1996): "B-ISDN semi-permanent connection availability".

[58] ITU-T Recommendation I.610 (1995): "B-ISDN operation and maintenance principles and functions".

[59] ITU-T Recommendation M.1510 (1992): "Exchange of contact point information for the maintenance of international services and the international network".

[60] ITU-T Recommendation M.1520 (1992): "Standardized information exchange between Administrations".

[61] ITU-T Recommendation M.1535 (1996): "Principles for maintenance information to be exchanged at customer contact point (MICC)".

[62] ITU-T Recommendation M.3010 (1992): "Principles for a Telecommunications management network".

[63] ITU-T Recommendation M.3100 (1995): "Generic network information model", including Corrigendum 1.

[64] Void.

[65] ITU-T Recommendation M.3400 (1997): "TMN management functions".

[66] ITU-T Recommendation O.191 (1997): "Equipment to measure the Cell Transfer Performance of ATM connections".

[67] ITU-T Recommendation Q.813 (1998): "Security Transformations Application Service Element for Remote Operations Service Element (STASE-ROSE)".

[68] ITU-T Recommendation Q.822 (1994): "Stage 1, Stage 2 and Stage 3 Description for the Q3 interface - Performance management".

[69] ITU-T Recommendation X.741 (1995): "Information technology - Open Systems Interconnection - Systems management: Objects and attributes for access control".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

ATM Access Point: means by which a subnetwork offers external interfaces to other subnetworks. It is associated with an end point of an IPPL

ATM Gateway: represents an ATM access point in one subnetwork, which is associated with an ATM access point in another subnetwork for the purpose of topological interconnection

Connection: ATM cell transport entity which is capable of transferring information transparently between connection points. A connection defines the association between the connection points and the connection points delimit the connection

Connection Admission Control: set of actions taken by the network at the connection set up phase (or during connection re-negotiation phase) in order to establish whether a virtual channel connection or a virtual path connection can be accepted or rejected

Data Communications Network (DCN): dedicated network used to interconnect operators' network management platforms supporting automated X.easi interface processes. (The DCN may be configured as a "closed user group" among these operator's management platforms.)

Inter-PNO Physical Link (IPPL): represents a physical link that offers bi-directional transmission capabilities and connects two subnetworks. Each InterPNOPhysicalLink is terminated by two ATM Access Points which are in charge of emitting failures related to the link or to the access point itself. An IPPL can be realized by any transmission capability (SDH, PDH etc.)

Link: "topological component" which describes the fixed relationship between a "sub-network" and another "sub-network" or "access group". It is defined by an access point on one subnetwork, which is associated with an access point on another subnetwork

NNI.easi interface: network to network interface in the User and Control Planes, specified in TS 101 674-1 [1]

Q-interface: non-specified interface used in a generic sense in the present document to mean any competent means by which an operator manages its internal network technology

Subnetwork: "topological component" used to effect routing and management. It describes the potential for "sub-network connections" across the "sub-network". It can be partitioned into interconnected "subnetworks" and "links". Each "subnetwork" in turn can be partitioned into smaller "sub-networks" and "links" and so on. A "subnetwork" may be contained within one physical node. In the present document this partition is not used

Subnetwork connection: Subnetwork Connection is capable of transferring information transparently across a subnetwork. It is delimited by connection termination points at the boundary of the subnetwork and represents the association between these connection points. It can be a VP or a VC connection

Trouble Ticket: report used to exchange information about the resolution of faults, degradations or provisioning problems between operators. Refer also to ITU-T Recommendation X.790 [28] for a definition of Trouble Management and Trouble Reporting

Virtual Channel Connection: ATM cell transport entity formed by a series of connections between the end-points. A Virtual Channel Connection is contained in a Virtual Path Connection. However, over the management interface, this containment need not always be visible

Virtual Path Connection: ATM cell transport entity formed by a series of connections between the end-points. A Virtual Path Connection can contain one or more Virtual Channel Connections. However, over the management interface, this containment need not always be visible

3.2 Abbreviations

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

AACC	Association Access Control Component
ABR	Available Bit Rate
ABT-DT	ATM Block Transfer capability with Delayed Transmission
ABT-IT	ATM Block Transfer capability with Immediate Transmission
ACSE	Association Control Service Element
AE	Application Entity
AESA	ATM Forum End System Addresses
AM	Accounting Management
API	Application Programming Interface
AR	Availability Ratio
ASN.1	Abstract Syntax Notation.1
ASP	ATM Service Provider
ATC	ATM Transfer Capability
ATM	Asynchronous Transfer Mode
ATM-CP	ATM Connectivity Provider
ATMF	ATM Forum
ATM-SP	ATM Service Provider
BW	Bandwidth
CAC	Connection (or Call) Admission Control
CANCAN	ACTS project, Contract Negotiation and Charging in ATM
CBR	Constant Bit Rate
CCR	Chargeable Cell Rate

CDR	Connection Detail Record
CDV	Cell Delay Variation
CDV(T)	Cell Delay Variation (Tolerance)
CER	Cell Error Rate
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CM	Configuration Management
CMIP	Common Management Information Protocol
CMISE	Common Management Information Service Element
CMR	Cell Misinsertion Ratio
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CPN	Customer Private Network
CTD	Cell Transfer Delay
CUG	Closed User Group
DBR	Deterministic Bit Rate
DCE	Data Communication Equipment
DCN	Data Communications Network
DN	Distinguished Name
EASI (or easi)	ETSI project ATM Services Interoperability
EDI	Electronic Data Interchange
EN	European Norm
ETNO	European Public Telecommunications Network Operators' Association
EURESCOM	European Institute for Research and Strategic Studies in Telecommunications
FM	Fault Management
FTAM	File Transfer, Access and Management
GDMO	Guidelines for the Definition of Managed Objects
GIOP	General Inter-ORB Protocol
GOM	Generic Object Model
GoS	Grade of Service
GSS	Generic Security Services
GSSC	Generic Security Services Component
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IN	Intelligent Network
IOC	Inter-Operator/International Operations Centre
IOU	Inter-operator Operations Unit
IP	Internet Protocol
IPPL	Inter-PNO Physical Link
IPsec	Internet Protocol security
ISA	Interconnect Service Establishment
ISD	Interconnect Service Definition
ISDN	Integrated Services Digital Network
ISO	Interconnect Service Operation
ITU-T	International Telecommunications Union, Telecommunications Standardization Sector
JAMES	Joint ATM Experiment on European Services
LAN	Local Area Network
LC	Link Connection
MAE	Management Application Entity
MBR	Maximum Burst Rate
MBS	Maximum Burst Size
MCR	Minimum Cell Rate
METRAN	Managed European Transmission Network
MF	Management Function
MO	Managed Object
MoU	Memorandum of Understanding
MSC	Management Service Component
MTBO	Mean Time Between Outages
MTP	Medium Term Planning
NE	Network Element

NM	Network Management
NMF	Network Management Forum (now the Telemanagement Forum TMF)
NNI	Network to Network Interface
NNI.easi	Network to Network Interface to ETSI Project EASI specification given in [1]
NPC	Network Parameter Control
NRT (or nRT)	Non Real Time
NSAP	Network Service Access point
OA	Operations Agreement
OAM	Operations and Maintenance
OCPT	Operational Contact and Procedural Template
OMG	Object Management Group
OMT	Object Modelling Technique
ORB	Object Request Broker
OS	Operations System
OSE	Operational Support Entities, ("manual" interface)
OSI	Open Systems Interconnection
OSS	Operations Support System
PA	Process Administrator
PCP	Process Control Point
PCR	Peak Cell Rate
PDH	Plesiochronous Digital Hierarchy
PM	Performance Management
PNO	Providing Network Operator
POI	Point of Interconnect
PSAP	Permanent Service Access point
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Channel
PVCCTP	Permanent Virtual Channel Connection Termination Point
PVP	Permanent Virtual Path
PVPCTP	Permanent Virtual Path Connection Termination Point
QoS	Quality of Service
RFS	Request For Service
ROSE	Remote Operations Service Element
RT	Real Time
SALC	Security Audit Log Component
SBR	Statistical Bit Rate
SCC	Security Control Component
SCR	Sustainable Cell Rate
SDH	Synchronous Digital Hierarchy
SDL	Specification and Description Language
SECBR	Severely Errored Cell Block Ratio
SES	Severely Errored Second
SH	Security Handler
SIA	Standard Interconnect Agreement
SMC	Service Management Centre
SMDS	Switched Multi-megabit Data Service
SNC	Subnetwork Connection
SNMP	Simple Network Management Protocol
SP	Service Provider
SPC	Signalling Point Code
SS7	Signalling System No. 7
STASE-ROSE	Secure Transformation Application Service Element – Remote Operations Service Element
STM-1	Synchronous Transport Module – 1
STP	Signal Transfer Point
SVC	Switched Virtual Channel
TCP/IP	Transfer Control Protocol/Internet Protocol
TMN	Telecommunications Management Network
T-PNO	Transit-PNO
UBR	Unspecified Bit Rate
UNI	User to Network Interface

UPC	Usage Parameter Control
VA-SP	Value Added Service Provider
VBR	Variable Bit Rate +(rt = real time or nrt = non-real time)
VC	Virtual Channel
VCC	Virtual Channel Connection
VCCC	Virtual Channel Cross Connect
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VP	Virtual Path
VPC	Virtual Path Connection
VPCC	Virtual Path Cross Connect
VPCTP	Virtual Path Connection Termination Point
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VPTTP	Virtual Path Trail Termination Point
X.easi	NM interface being specified in the present document
X.user	NM interface between PNO and VA-SP or other consumer
Xcoop	X.easi (as named in other cooperative X-interface specification projects)
X-interface	TMN network management interface
XML	eXtensible Markup Language

4 General introduction

4.1 Overview

The present document provides a "Framework Solution" in the form of guidelines to network management specifications and to supporting multi-lateral documentation for the practical achievement of inter-operability between European ATM networks, and between their associated management platforms, or Operations Support Systems (OSSs). It specifically acts as a detailed set of "Guidelines" to TS 101 674-2 [2].

It covers the processes and functions for the efficient management of interconnected ATM networks which align with technical specifications (for the user, control and network management planes respectively) being developed by the ETSI EASI project [1], [2].

Available network management standards for ATM services focus on the automation of operational processes. The present document also examines pre-service processes that are necessary between co-operating operators to establish the interconnection of their ATM networks prior to operational use. Operational NM interfaces should be specified in the context of these pre-service processes to ensure efficient and cost effective ATM-based service provision from the points of view of operators and customers alike. These pre-service interconnection processes take a great deal longer time to complete, than in-service connection provisioning, using the automated network management functions described later.

The provision of interconnected ATM services has to be considered within the current European trading environment. This is characterized by a liberalization process that has been initiated by the EU. The exact stage of liberalization in each EU member state varies and different regulations are in place concerning the issue of licences to operate telecommunication networks. For this reason, the Business Model, proposed in the present document, separates the provision of network services - such as ATM connections - from value added service provision, since in some EU states this distinction is an important part of the regulatory environment.

4.2 Relationship of the present document to other ETSI and EURESCOM documents

The present document is part of a set of documents from ETSI and EURESCOM in relation to the specifications for Phase 1. Figure 1 shows the relationship of the present document to the others:

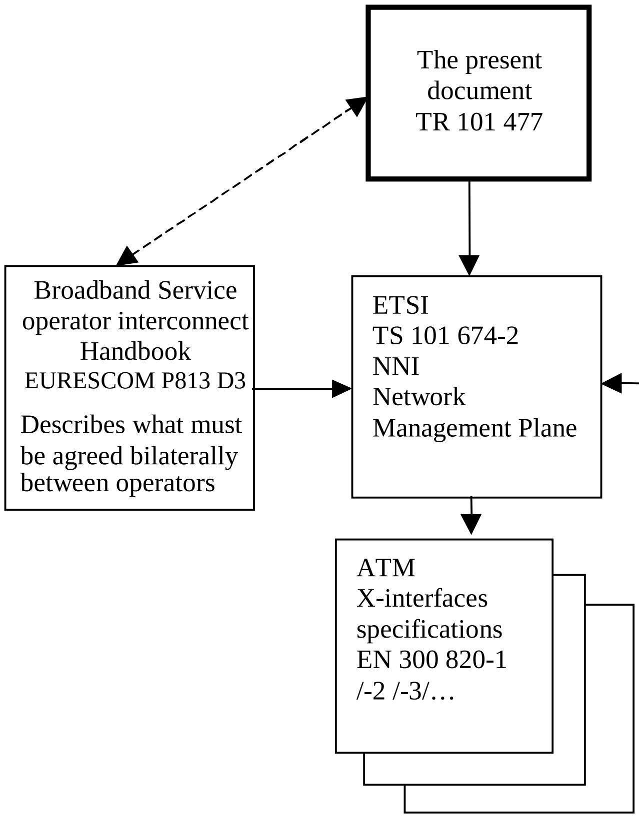


Figure 1: Relationship of the present document to other EURESCOM and ETSI documents

The combination of TS 101 674-1 [1] and TS 101 674-2 [2] provides the full technical specification for the Network to Network Interface covering the User, Control and Management Planes.

The present document provides guidelines to the application of [2], the specification of the NNI for Network Management Plane and in doing so, references other applicable standards such as the EN 300 820-1 [6] for the X-Interface.

In addition to these specifications and guidelines there is a need to document and agree some aspects of the interface, particularly operational aspects, on a bilateral basis. The Operator's Handbook [3] provides the overview and checklist for the aspects that have to be agreed ***bilaterally***.

4.3 Structure and organization of the present document

The scope and content of the present document, together with the relationship to the principal ETSI Phase 1 specification documents, is summarized in figure 2.

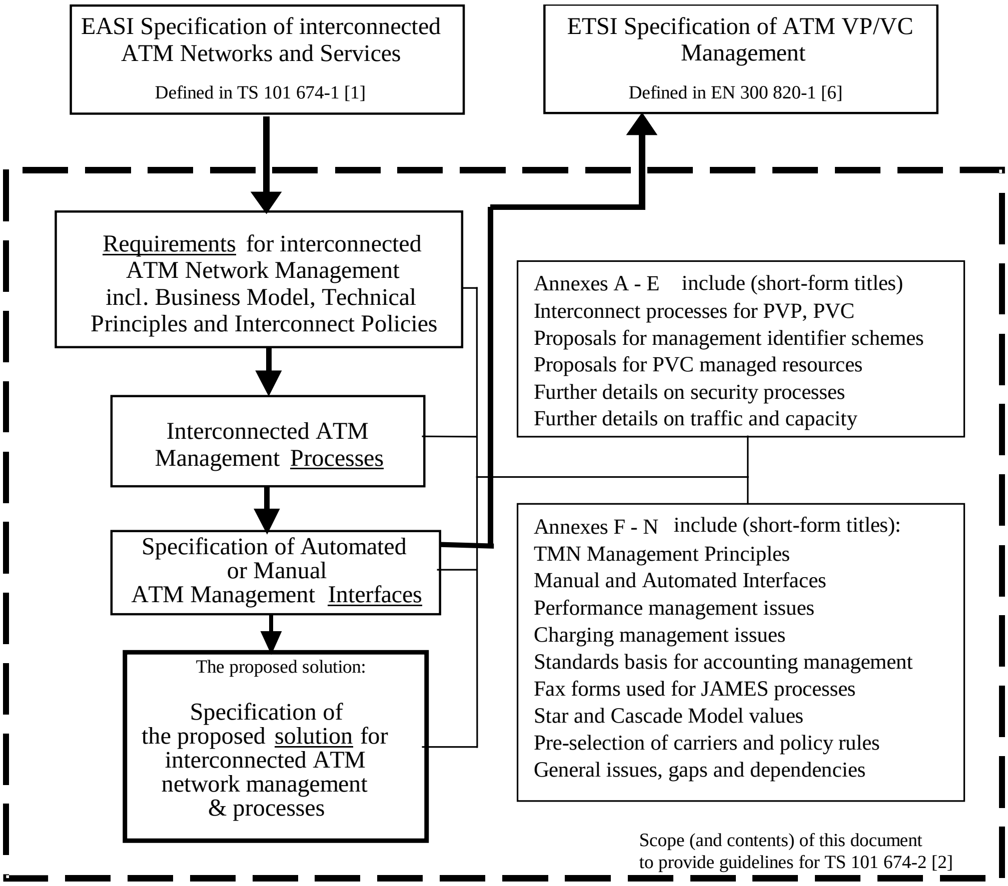


Figure 2: Derivation of the proposed Network Management Solution

The initial step is to develop the requirements for interconnected ATM network Management. These are based upon an assessment of the requirements arising from [1], and also general requirements that are captured in the form of a Business Model and interconnect policies. These are captured in clauses 6 and 7.

These requirements are used to determine the ATM Interconnect Management processes for both Pre-Service and In-Service process areas. These are covered in clauses 8 and 9.

For those processes where automated interfaces are required the present document develops solutions. The emphasis in Phase 1 is placed on the in-service inter-operator network management interface, "X.easi". This is introduced in subclause 5.4 and specifically addressed in clause 9. The solutions are mainly based upon references to Standards.

A potential limitation to the solution derivation model shown in figure 2 is that there is no indication of what part of the standards is mandatory and what part is optional or how the model can be extended (e.g. by the use of "conditional packages"). Where possible, these aspects are described in various text clauses in the present document.

A NM "solution" for interconnected ATM services would be deficient without a description of (i) a data model for supporting inter-operator processes and (ii) implementation and testing issues. Clauses 10 and 11 respectively provide information and requirements in these two areas.

In addition to the clauses listed above, which comprise the main part of the present document, a series of annexes have been developed. The annexes A - E provide significant additional details in the following areas: (A) Management processes for provisioning and repairing PVP and PVC connections (B) Management identifier schemes (C) proposals for extensions of PVP to PVC managed resources (D) security processes and (E) traffic and capacity management processes. Annexes A - E should be regarded as an integral part of the description of the NM solution for operators interested in implementation and operation of the management interface described in the present document. Annexes F to N are not an integral part of the Phase 1 solution but may be regarded as relevant and useful background information.

NOTE: Concerning annex C above, the term "extension of PVP to PVC managed resources" is used, because the PVP model is described in an existing standard, whereas the PVC part is new.

5 Technical principles for ATM interconnection services

5.1 Overview

The requirements and solutions for ATM Management and Operations Support Systems are driven from an understanding of the ATM interconnect services offered between operators. Clause 5 addresses the interconnect services from both the ATM Bearer and Management Plane perspectives.

More specifically, clause 5 describes the technical principles identified with ATM interconnection services. This includes ATM bearer capabilities, ATM interconnect services definition, "X.easi" nomenclature definition, a description of the network management parameters, the TMN and related technology basis for the NM specification, definitions of manual and automated interfaces and the requirements for the NM (X.easi) interface.

5.2 ATM bearer capabilities

The present document is concerned with the following two types of ATM bearer capabilities which may require inter-operator processes for end-to-end management.

Permanent Virtual Circuit Service

Permanent Virtual Circuits are pre-configured logical connections between two ATM systems. They may of either the Virtual Path or Virtual Channel type.

Switched Virtual Circuit Service

Switched Virtual Circuits are logical ATM connections established via signalling. They will usually be of the Virtual Channel type.

The ATM bearer capability distinguishes two types of connections (whether permanent or switched): Virtual Channel (VC) and Virtual Path (VP). Individual ATM connections between two adjacent ATM systems are referred to as VC Link Connections and VP Link Connections. The VP (or VC) Link may therefore be defined as the entity which connects two subnetworks where the VP (or VC) identifier is terminated or translated.

End-to-end connections are referred to as Virtual Channel Connections (VCCs) and Virtual Path Connections (VPCs). All connections should be associated with a defined Quality of Service (QoS) and defined ATM Transfer Capability (ATC), - refer to subclause 5.3.

A single ATM physical interface will support multiple VPCs, each of which will contain multiple VCCs. Implementing VPCs aids the manageability of the ATM network. Traffic management, rerouting and possibly switching may be based on these VPCs.

The concepts of VPs, VCs and underlying physical links are depicted in figure 3 from the point of view of a single physical interface. Each such entity will have a unique identifier ascribed to it for operational purposes (which is not elaborated here).

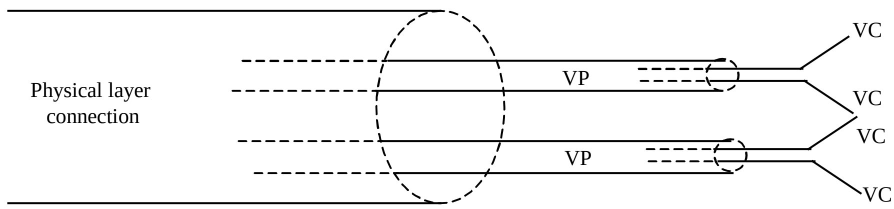


Figure 3: Virtual Paths and Virtual Channels within the physical layer

The ATM bearer capabilities are aligned with the technical capabilities required by [1], which are listed in the following bullets:

- **The transmission level.** Transmission should be possible using virtual path connections (VPCs) or virtual channel connections (VCCs).

- **The connection type.** Connections can be permanent or semi-permanent. It should be possible to extend the specification to switched (on demand) connections, if required (Refer to comments in the bullets of subclause 9.1.3 for further comments about management requirements for switched services.).

  Permanent/semi-permanent virtual connections are to be supported on virtual path connection level and on virtual channel connection level.

  (For Phase 1, switched virtual connections should only supported on a virtual channel connection level.)

  Permanent/semi-permanent virtual channel connections (and switched virtual channel connections, if required) should be transported in different virtual path connections.

- **The connection configuration.** Connections can, in principle, be point-to-point or point-to-multipoint. In Phase 1, support of point-to-multipoint connections is not required.

- **The direction of transmission.** Transmission can be unidirectional (i.e. without any reverse information transport) or bi-directional. When bi-directional, transmission can be symmetric or asymmetric. At the NNI.easi interfaces, all modes of transmission, as defined in ETS 300 298-1 [4] and ETS 300 298-2 [5] should be supported.

- **The quality of service (QoS).** The QoS classes required to be supported are defined in table 5.2 of [1].

- **The ATM transfer capability (ATC)**. The ATCs required to be supported are defined in table 5.2 of [1].

5.3 Definition of ATM interconnect services

The provisioning of ATM end-to-end services across multiple interconnected ATM networks requires definition of the interconnect services. In the present document the ATM interconnect service is defined as "the capability to provide ATM connectivity across a particular network". The ATM interconnect service distinguishes two components:

(1) the ATM interconnect transport service (defined by the User and Control Plane);

(2) the ATM interconnect management service (defined by the Management Plane).

The scope of both (1) and (2) needs to be agreed between interconnecting operators as part of the Interconnect Service Definition process described later in clause 7.

The ATM interconnect service can be offered as:

(i) Originating Carrier Service (i.e. a connection service from an A Endpoint to an adjacent operator's network);

(ii) Transit Carrier Service (i.e. a connection service from an adjacent operator's network to the network of another adjacent operator, across their own network).

Destination Carrier Service (i.e. a connection service between an adjacent operator's network and a Z Endpoint).

The destination carrier service may be associated with the terminating connectivity provider described in clause 6.

The present document is principally concerned with the ATM interconnect management service (2) whereas (1) is described in [1].

The interconnect management service involves establishment, maintenance and release of subnetwork connections amongst two or more administrative domains, as well all associated processes in order to meet a customer service requirement.

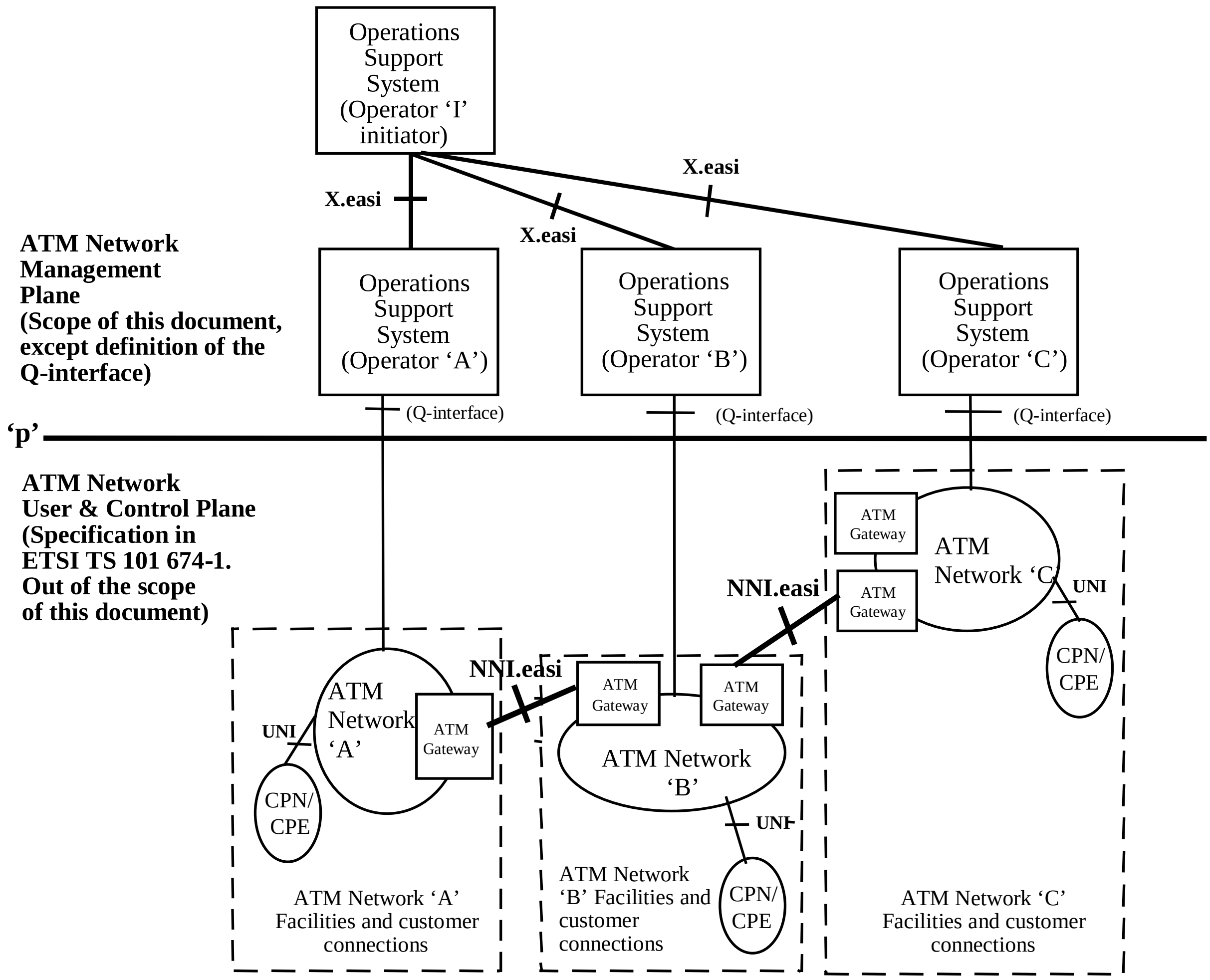
5.4 "X.easi" Definition

In the present document the term "X.easi" has been chosen to reference all proposed network management functions between operators, covering both automated real-time and manual capabilities for the "ATM interconnect service operation processes". This term is a placeholder description which is expected to be strongly related to the established ITU-T TMN "X interface". The use of the term "X.easi", at this stage, avoids the need to be prescriptive about whether such interfaces are completely manual or automated, or some hybrid.

5.5 Network management parameters

Figure 4 shows the concepts, resources and "planes" which may be considered in the context of the provision of ATM services which span two or more operator's network domains. Some terms are defined later in the present document. The part shown **above** the heavy line "p" represents the network management plane which is required to manage ATM networks and services defined in [1].

In order to define the scope for the Phase 1 specification, the X.easi interface is specifically restricted to management of the operational processes (as described in clause 9). The pre-service processes, described in clauses 7 and 8, are necessary inter-operator bi-lateral and multi-lateral activities associated with the provision of ATM interconnection services but are not within the definition of the X.easi management interface for the Phase 1 specification.



Legend:

X.easi	Network Management interface between operators' Operations Support Systems
CPN/CPE	Customer Private Network / Customer Premises Equipment
NNI.easi	Network-to-Network Interface (specified in [1])
UNI	User-to-Network Interface (specification not specified)
(Q-interface)	Management interface to the network technology in each operator domain This is proprietary to each operator and not defined or specified in this document.
NOTE	The 'I' and 'A' operators may be one and the same organisation.

Figure 4: Concepts, resources and planes for ATM networks and services

Figure 4 shows the general case of an initiating operator (I) in addition to the originating operator (A), by comparison with the NM description in the equivalent figure in [1]. Operator (I) is included in the network management specification in order to align with the European standard [6]. In many cases, the "I" and "A" operators may be one and the same organization (as assumed in [1]) but may equally well be different organizations.

As the end to end connections are established across multiple subnetworks, the Operation Support systems of the A, B and C operators are responsible for, *originating connections, transit connections and terminating connections* respectively and the I operator is responsible for arranging the *end to end connection between A Endpoint and Z Endpoint, that is, the connections of direct interest to the end customer(s).*

Furthermore, operators I, A, B and C in figure 4 map onto the *I-CP, A-CP, T-CP* and *Z-CP* roles defined in the Business Model (figure 5), described in subclause 6.3. It may be presumed that many interconnecting operators would wish to act in any of the I, A, B or C roles shown in figure 4, according to the configuration of any given PVP or PVC connection and would wish to provide management services such as PVP/PVC establish, release, reconfigure, modify [6] etc in relation to any of these four roles. The management services, defined in relation to each of the four roles, are required to support PVP, PVC etc services provided by the interconnected ATM networks plane.

The specification of the interconnected ATM networks plane (the part shown **below** the heavy line "p" in figure 4), is defined in [1], except for the User-to-Network interface (UNI). Interactions with entities such as "Value Added Service Providers" are not shown in figure 4 but described later in association with the interconnect business model and figure 5.

5.6 TMN and Technology basis for the X.easi interface specification

5.6.1 The TMN basis for the interface specification

The proposal for the network management interface specification, identified as "X.easi" in the present document, is based upon the ITU-T Telecommunications Management Network (TMN) Architecture and principles, derived from ITU-T Recommendation M.3010 [7]. The concept behind a TMN is to provide an organized architecture to achieve the interconnection between various types of operators for the exchange of management information, using an agreed architecture with standardized interfaces including protocols and messages. One such interface is the TMN X-interface. This is derived from the "x reference point" described in [7] and is pertinent for the establishment, maintenance and release of ATM Virtual Path (VP) and Virtual Channel (VC) connections which span several operator's ATM domains. The term "X.easi", is derived from these concepts.

Some additional detail on TMN concepts is provided in annex F.

TMN architecture also defines the Q-interface, derived from the q reference point in [7] and other standards. Simplistically, this interface is operator-internal. It is between an operator's OSS and its network technology, including switches. These interfaces are essential but are the responsibility of each operator and its technology supplier and, as such, are outside the scope of the present document. For efficient ATM interconnection, it must be presumed that suitable Q-like interfaces are available to operate in association with the relevant X.easi interfaces. (Refer also to the architecture and associated comments in figure 4.)

The present document recognizes that some operator's operations support systems (OSSs) are manual and this factor influences the technical capabilities of the X.easi interface. The concepts of manual and automated TMN management interfaces are described in subclause 5.6.2.

5.6.2 The technology basis for the interface specification

The "automated" interface specifications, described in clause 9 and elsewhere, are based on the presumed use of a CMIP and GDMO based implementation of the interface. The practical use of such technology has been demonstrated in other EURESCOM projects [8], [9].

The present document aims to provide a management interface specification which may or may not rely on the use of a CMIP and GDMO implementation. In other words, the specifications and principles described in the present document should be applicable to any suitable technology basis, although the descriptions have the established basis of CMIP/GDMO in mind. CMIP/GDMO should therefore be considered as a reasonable **example** of the technology solution but not necessarily the sole choice.

Many of the concepts of network management, for the "ATM interconnect service operation processes" described later (specifically with figure 8), are associated with the deployment and use of "X.easi" interfaces which are: "Manual", "Fully-automated", or "Semi-automated". Subclauses 5.6.2.1 and 5.6.2.2 describe the use of these terms.

5.6.2.1 Manual interface

The term "manual interface" is generally appropriate when management information between operators is exchanged between identified persons according to predefined procedures. Such procedures may be subdivided into two basic categories:

Existing manual procedures:

> those procedures already in place between operators, for which operators are already trained and standard forms exist (typically, a fax, phone, file transfer or e-mail based interface).

Future manual procedures:

> procedures for exchange of management information related to functionalities not currently supported for which, therefore, no existing procedures exist.

5.6.2.2 Automated Interface

An interface is defined as "automated" when both a formal specification and a formal protocol are defined for the exchange of management information between operators, using computer-based technology. The following refinements also apply:

Fully-automated management interfaces:

> these interfaces have automated management links to the underlying ATM network, thus allowing: management operations requiring an intervention on the real network to be performed with a minimum of human effort and in a minimum amount of time (real time). The duration of "real time" is defined case by case, but, in general it would not be sufficient to allow any human intervention that would dramatically slow down the procedure. Fully-automated interface response time-outs are calculated on the basis of these assumptions.

Semi-automated interfaces:

> these interfaces have management links which have the same characteristics and functionality as fully-automated interfaces, except that there are no automated communications to the underlying network technology. From the point of view of an OSS interacting with a system offering a semi-automated interface, there are no differences from a fully automated one, except for longer time-outs for interacting with network resources.

(For simplicity, interfaces considered in the present document are generally described as either "manual" or "automated". The refinement to "fully-automated" or "semi-automated" is only used when addressing time-out issues).

Further discussion on the operation of manual, automated and semi-automated interfaces is presented as a series of "Case Studies" on degrees of automation of interconnect in annex G.

5.7 Requirements and Management Functions for the X.easi interface

5.7.1 Requirements for the X.easi interface

Requirements identified for the efficient usage of the proposed X.easi interface are:

The ability to manage all ATM interconnect service-operational network management capabilities listed in subclause 5.2 and derived from [1]. (Note that this specifically applies only to the "Interconnect Service Operation Processes" described in clause 9).

The ability to manage all and any combination of ATM ATC service classes and Quality of Service classes listed in [1], where there is a requirement to cross network operator domain boundaries. This requirement is subject to the availability of suitable network resources and an agreed policy for ATM service provision priorities in the event of a shortage of resources.

The ability to integrate use of the interface for management of service operations with processes associated with pre-service interconnect definition, establishment and administration. Accordingly, requirements for the X.easi interface include:

Specification of the X.easi management interface (clause 9) for the exchange of all in-service interconnect operations processes, data and information flows.

Physical implementation, testing and operation of the X.easi interface.

An automated X.easi interface must have a manual alternative. This would provide a fall-back position in the event of failure or a basic capability for new operators to achieve interconnection where automation is not possible initially. Some refinement in definition of the management function capabilities of the interface are provided in the subclause 5.7.2.

5.7.2 Management Functions for the X.easi interface

The full specification of the proposed X.easi interface should include the following interconnect service operation processes (or management functions, in TMN terms [7]) for the Phase 1 solution.

- Configuration Management.
- Fault Management including Trouble Ticketing.
- Exchange of inter-operator performance reporting information.
- Exchange of inter-operator accounting reporting information.
- Security services to secure the above procedures against TMN network management OSS threats and fraud.

(Refer to subclause 9.1.3 and table 6 for discussion on options for automated and manual processes for the functions listed in the above bullets).

6 Business Model and Business Policy Issues

6.1 Introduction and Overview

Clause 6 considers possible business objectives, models and policy issues for which operator interconnection processes are required to support and deliver ATM services.

6.2 Business Objectives

The Business objectives are:

1) To allow the rapid provision and operation of flexible end to end ATM based services across multiple network operators by:

   - Providing specifications that allow the interconnection and consequent inter-operation of the Network operators' Network Management Applications and Operations Support Systems that are managing an operator's ATM Network.

   - Providing specifications that are designed to support the functions of the NNI.easi interface [1]. In particular, by providing specifications that are aligned to the scope of [1] and designed to be up-issued in alignment with the phased up-issues from [1].

2) To provide excellent ATM-based services to customers. These include:

General

The main objective for service and network management is to provide ATM-based customer services and at the same time, optimize costs and resource usage to operators and other service suppliers. Business objectives should therefore include adequate provision of the following (bullet) items in order to support services:

Guaranteed bandwidth

Use best endeavours to ensure that the customer bandwidth requirements are sufficiently planned by means of traffic and capacity planning processes in order to provide the basis for supplying guaranteed bandwidth requirements.

(Traffic and associated capacity planning for it is described in detail in subclause 8.3.2 and elsewhere in the present document.)

Guaranteed service availability

To endeavour to guarantee service availability the service-provider must have efficient planning of a recovery strategy and how to achieve such strategy. This should include, where necessary, strategies agreed with interconnected operators.

Guaranteed service assurance

The goal will be to avoid inconvenience for the customers by means of detecting and correcting any kind of malfunctions and errors before there is a noticeable effect on customer service. Automation of fault recovery by automatic protection mechanisms should be implemented wherever practicable (whilst noting that automated network resilience strategies are specified as an option in the Phase 1 requirement in [1]).

Guaranteed performance on service

To endeavour to guarantee the performance, the quality of service should be constantly monitored and be supported with availability of back-up resources which can be rapidly activated on performance degradation.

Guaranteed access to network services

This service would require a combination of a strategy for avoiding or minimizing network congestion and a planning strategy for optimizing the availability of network resources.

Ensuring the availability and confidentiality of Service Level Agreements

Practical service level agreements should be available for all involved parties to any service provision and issues of confidentiality should be treated as being of the highest importance.

Real-time information availability to customers

Real-time information, including statistical information, should be available to customers where it relates to quality of service (such as fault conditions and, perhaps, charging information).

Confidentiality and integrity of management information

Other parties who have no direct involvement in a particular customer's service request, including competitors who might be interconnected at service management and/or network management levels, should have no information about that customer's connection requests, connections which are provided, related billing or customer care.

6.3 Business model (roles)

6.3.1 Scope and objective

The delivery of Pan-European ATM services across the networks of multiple operators is a complex process which involves many different parties. European ATM Service Introduction therefore requires a business model which describes the responsibilities of each party involved, and the business relationships amongst them. The objective of subclause 6.3 is to describe a business model, which should be acceptable to interconnected operators and other service providers, for European ATM Service Introduction.

The following approach is used for defining the business model:

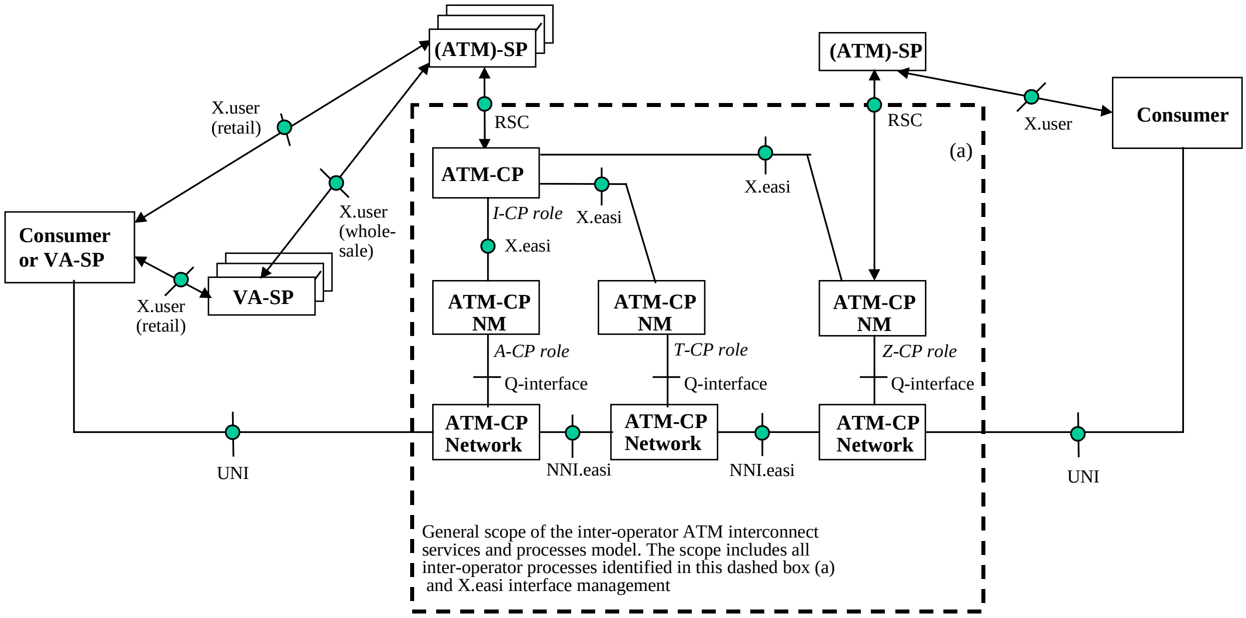
- characterization of responsibilities and roles;
- characterization of reference points between responsibilities or roles corresponding to business relations;
- characterization of the interactions allowed across interfaces corresponding to business agreements and/or information exchanged between legal entities.

Ensuring compatibility with and support of the User and Control Plane specification defined in [1].

The relationship between the proposed business model responsibilities or roles and commercial organizations is not prescribed by the business model. This means that a commercial organization can act in more than one role described in the business model. For example, it is possible that a PNO can act in both connectivity and service provider roles defined below.

6.3.2 Overview of the business model

The proposed business model for European ATM Service Introduction is presented in figure 5. The business model represents an overall framework for the provisioning of managed bandwidth ATM transport services across multiple interconnected ATM networks. The business model presents a positioning of the ATM interconnect service, which consists of both the ATM interconnect transport services and the ATM interconnect management services. Most importantly, the scope of the present document is restricted to that shown in the dashed box (a). The other responsibilities/roles and reference points are for information only.



Legend:
VA-SP: Value Added Service Provider
(ATM)-SP: ATM Service Provider
ATM-CP: ATM Connectivity Provider
NM: Network Management
X.user: Interface from PNO to VA-SP or other consumer
UNI: User to Network Interface
I, A, T, Z role: Initiating, Originating, Transit, Destination connectivity provider role

● Reference point coincides with interfaces in some cases and interconnect contractual arrangements in all cases where the interface is between two different organisations

RSC: Reference point between (ATM)-SP and ATM-CP

Figure 5: Business Model for ATM Interconnect Services, including

Roles and Interfaces

A PNO, as introduced and described in subclause 4.1, can play some or all of the roles described in figure 5 and explained in the text below. (The roles are more fully described in subclause 6.3.3.)

In this business model it should be noted that:

- Connectivity Providers (CP) have responsibilities for providing ATM Connections of various types;
- Within the scope indicated by this proposed business model, the Initiating CP may be facilities based or not, and the Originating, Transit and Terminating CPs must be facilities based. The *I-CP* may also require a specific telecommunications operator's licence, for offering non-facilities based services, in some countries.

The ATM Connectivity Providers acting in the *A-CP*, *T-CP* and *Z-CP* roles, have responsibility for originating, transit or destination service connections. The organizations performing this role and having this responsibility must be facilities based and have physical connection capabilities. Such ATM-CPs may also require licences in some European Countries.

The Initiating ATM Connectivity Provider (*I-CP*) has responsibility for initiating end to end connections between A Endpoints and Z Endpoints.

The ATM Service Provider, (ATM)-SP, in addition to ATM, may provide other connectivity services based on other technologies such as Frame Relay, ADSL,… (ATM)-SPs may require licences in some European Member States.

Value Added Service Providers (VA-SP) are shown separated from (ATM)-SP and ATM Connectivity Providers because some EU States have different licensing and rules governing the scope of Service Provider activities. It is often the case that VA-SPs do not have any networking infrastructure and do not require any licences whereas it is possible in other states that one organization can perform the ATM-CP, The (ATM)-SP and the VA-SP roles with or without a licence. This model supports all possibilities and focuses on the connectivity aspects which are mostly regulated.

The "X.user" reference point represents a service management interface between the management system of an (ATM)-SP and that of a Value Added Service Provider (VA-SP) or directly with that of the private network management system owned by an ATM service consumer (or "end-user"). Definitions of the X.user interface or the UNI are out of the scope of the present document.

Table 1 characterizes the reference points and summarizes the "allowed interactions" in the business model.

Table 1: Characterization of business model reference points and interactions

Reference Point	Characterization	Allowed Interactions
X.easi interface	*I-CP* ATM-CP to *A-CP*, *T-CP* or *Z-CP* ATM-CP NM	Peer-to-peer network management information exchanges.
RSC	(ATM)-SP to ATM-CP (*I-CP* role) or ATM –CP NM (*Z-CP* role)	(ATM)-SP and ATM-CP network management interactions required to support requests for End to end Endpoint connections. Such interactions are usually a local matter between the respective (ATM)-SPs and operators performing the *I-CP* and *Z-CP* NM roles.
NNI.easi	ATM-CP to ATM-CP	Peer-to-peer (inter-operator) ATM network interconnection interactions as defined in [1].
UNI	ATM-CP Network to ATM consumer	Network operator to ATM consumer network interconnection interactions (definitions are out of scope of the present document).
X.user	(ATM)-SP to VA-SP (wholesale) or ATM consumer (retail); or VA-SP to ATM consumer, or other VA-SP, (retail)	(ATM)-SP, VA-SP and Consumer, service management interactions (definitions are out of scope of the present document).

6.3.3 Business Model Roles

A description of the roles associated with the business model (figure 5) is provided in the following bullets. It should also be noted that all interactions between organizations acting in the roles described below require contractual arrangements to be in place.

(ATM) Service Provider ((ATM)-SP)

This role is responsible for providing and selling the ATM service to end consumers or Third Parties such as Value-Added-Service Providers (VA-SPs). This includes the establishment of administrative and contractual agreements with these parties and an initiating ATM Connectivity Provider (ATM-CP). For interconnected ATM services, in particular, the (ATM)-SP would take responsibility for accepting a Consumer request and ordering the necessary resources from its associated ATM-CP to achieve the required end-to-end connectivity for the Consumer. It is possible that this service provider sells packages of ATM and other network connections (frame relay, ADSL,..) and for this reason it is designated as (ATM)-SP as opposed to ATM-SP.

Initiating ATM Connectivity Provider (ATM-CP)

This role (denoted by *I-CP* in figure 5) is responsible for provisioning managed bandwidth ATM transport services from ***A Endpoint to Z Endpoint*** across multiple interconnected ATM networks. It achieves this by utilizing the services of other Connectivity Providers that offer connection services for originating, transit or destination connections. The initiating ATM-CP may or may not possess network facilities.

ATM Connectivity Provider (ATM-CP)

The ATM Connectivity Provider (ATM-CP) is responsible for providing the ATM Interconnect Service to other ATM-CPs. To this extent the ATM Connectivity Provider can support one or more of the following services:

- Originating Carrier Services from an A Endpoint to an adjacent operator's network.
- Transit Carrier Services between two networks that are adjacent to that of the ATM-CP.
- Destination Carrier Services between an adjacent operator's network and Z Endpoint.

The ATM Connectivity Provider is further divided into:

1) the ATM-CP Network sub-role. This sub-role is responsible for offering the ATM interconnect transport service to other ATM-CPs;

2) the ATM-CP Network Management (NM) sub-role. This sub-role is responsible for offering the ATM interconnect management service to other ATM-CPs.

ATM Connectivity Providers acting according to the roles identified in (i), (ii) and (iii) above are respectively denoted by *A-CP*, *T-CP* and *Z-CP* in figure 5.

A "traditional" network operator or "PNO" would be the obvious example of an organization acting in the ATM-CP business model role.

Value-Added-Service Provider (VA-SP)

This role is responsible for adding value to the basic ATM and other transport services. Examples of Value-Added-Services are data networking services over ATM, Virtual Private Networking (VPN) services, Video Conferencing services, Virtual Private Network provision and management, LAN interconnect services, Multimedia Mail services, and Video On Demand services. VA-SPs may co-operate to produce a selection of services to the Consumer. Furthermore, VA-SPs are independent from ATM-SPs but may need to interact with some or many of them and may also need interconnections to ATM-CPs (not shown explicitly in figure 5), in order to fulfil contracts with the Consumer.

ATM Service Consumer (AS-C)

This role is responsible for consuming (i.e. using) ATM-based services (including value-added services), according to agreed contractual arrangements. Examples of organizations that perform this role are other Service Providers or large companies (which may, for example, require interconnection with their own privately-managed ATM networks in order to establish LAN interconnection with a similar private ATM network).

6.3.4 General comments concerning the relationships between roles and organizations

As previously stated the business model does not prescribe the relationship between the proposed roles and organizations.

One organization can perform several of the above roles, but it is also possible that each role is performed by only one organization.

There is little benefit in separating various ATM Service Consumer roles as these roles reduce to one of scale (or the amount of consumer demand for services). Nevertheless, separation of roles reflects the developing market situation. However, industry costs could be increased due to the need for multiple interfaces between all the various organizations which might be involved.

Some possible additional business model roles:

Some additional roles, which may be added to the proposed business model (figure 5), can be identified. These are outside the general scope of the ATM interconnect services described in clause 7 but should not be overlooked in the broad scheme of such service provision and are described as follows:

Connected end-partner

The connected partners in an end-to-end connection. The end-Partner may be a consumer or a Service Provider sending/receiving data from a content Provider. The connection may be used:

- uni-directionally to receive information ("pull");
- uni-directionally to send information ("push");
- bi-directionally, typically for inter-active communication. Communication properties in different directions may be different.

One of these partners is the partner requesting the connection. The partners can agree, which partner is the responsible for the payment. The model should be adaptable to multi-partner sessions.

Payment handler ("Trusted Third Party"):

Acts as a payment collection service to or for consumers. Such a trusted third party could be useful to accumulate payments from many consumers and reduce the number of payment processes between the various organizations involved.

Merchant Customer Care Handler:

This is a role to which the Consumer may delegate alarm handling, performance monitoring, additional security services, etc.

6.3.5 Summary of the business model roles

The workings of the business model may be summarized as follows:

i) The ATM Connectivity Provider is responsible for ATM network operations and the provisioning of managed bandwidth ATM transport services.

ii) The ATM Connectivity Provider acts as a contractor leasing network capacity to one or more initiating Connectivity Provider(s). In turn, an ATM-Service Provider leases network capacity from a selected (i.e. contracted) ATM (initiating) Connectivity Provider.

iii) The ATM Service Provider is responsible for providing and (re-)selling the ATM service to end Consumers or Third Parties such as Value-Added-Service Providers (VA-SPs).

iv) All interactions between different organizations acting in the roles described above require contractual arrangements to be in place.

v) In figure 5, only a single Initiating ATM-CP is shown connected to a respective (ATM)-SP whereas there may be multiple connections of this type. Since the consumer does not have a direct contract with Initiating ATM-CPs, the ATM-SPs may be in a position to select which Initiating ATM-CP to use (usually for the case where the initiating ATM-CP and the (ATM)-SP are different organizations).

The scope of most of the remainder of the present document is concerned with, the management of interconnect processes and interconnections between various ATM-CPs (using the X.easi interface). However, it should be noted that many well-resourced operators could choose to act simultaneously in the roles of (ATM)-SP, Initiating ATM-CP, and all other (A, T, Z) ATM-CP roles. Many of the requirements to complete the pre-service as well as the in-service ATM interconnect services and processes, described in clause 7, relate to both forms of provider.

6.3.6 Concluding remarks about the business model

The business model shows a significant number of relationships between roles according to which "organizations" can act. The model is considered to be indicative of the minimum number of identifiable roles and required interactions consistent with provision of interconnected ATM services in the emerging multi-operator market. Therefore the business model, as proposed, may claim to establish the principles of ATM interconnection and the associated contractual roles but may not be completely comprehensive in regard to anticipated market developments.

For the business model, some policy issues apply, which are discussed in subclause 6.4.

6.4 Business Policy Issues

6.4.1 Scope

Subclause 6.4 considers business policy issues for the management of resources (e.g. PVP, PVC, SVC) which are required to support semi-permanent reservations that traverse several network operators' domains. To protect the interests of the operators involved (i.e. to prevent "invasiveness"), and to prevent misunderstandings, a business policy has to be defined which proposes the (general) framework and constraints that apply for inter-connection.

Business policy should also require agreements for an Interconnect Service Definition (ISD) which could include a Standard Interconnect Agreement (SIA) comprising a number of parts that cover the (network level) Interconnect Services, and the OSS Interconnect Services. The latter includes Operations and Maintenance, Billing and Payments, and Planning and Operations. The SIA and an agreed "Code of Practice" should be used as the basis of bilateral contracts between cooperating operators. In general, generic processes suitable for industry-wide interconnect service establishment should form the basis for any inter-operator interconnect agreement. (Refer also to clauses 7 and 8.)

6.4.2 Business policy for an organizational model to support VP/VC connections

Business policy for provision of interconnected ATM-based services should align with an acceptable, workable and implementable organizational model for the "stakeholders" – i.e. the ATM service providers, connectivity providers, other resource providers and consumers.

The business model proposed in figure 5 and associated text, relates to the requirements for management of an ATM-based service. Such a service can be provided on the basis of an "I-PNO", acting in the ATM-CP role, taking an order (from a consumer or VA-SP) and ordering the required connections from T and Z-PNOs, using the X.easi management interface. The configuration of the I-, A-, T-, and Z-PNOs (ATM-CPs) shown in figure 5 aligns with the ETSI "Star" organizational model defined in [6] and the management interfaces between each of them may be defined as "X.easi" interfaces. This standard [6] also specifies the possible use of a "Mixture" model which is a combination of star organization and peer-to-peer (cascade) organization for ATM service provision.

As an ATM service introduction policy statement and on the basis of European standards [6], it seems appropriate to propose the following normative statement:

"Interconnected ATM service management shall be organized in alignment with the ETSI star model for Phase 1 service introduction. (Migration to a Mixture organizational model shall be available for Phase 2 service introduction)".

In association with this statement, various implementational issues for both organization of ATM interconnections and transfer of management information should be considered. These issues are discussed in clause 11 – Implementation and testing issues.

The star model is defined by reference to figure 6. The entities in this figure map to those shown in the Connectivity Provider (CP) roles of the Business Model, figure 5, in that the I-PNO is the ATM-CP, and the A, T, T' and Z-PNOs with their subnetworks, are ATM-CP NMs. The A-user and Z-user are ATM consumers or VA-SPs.

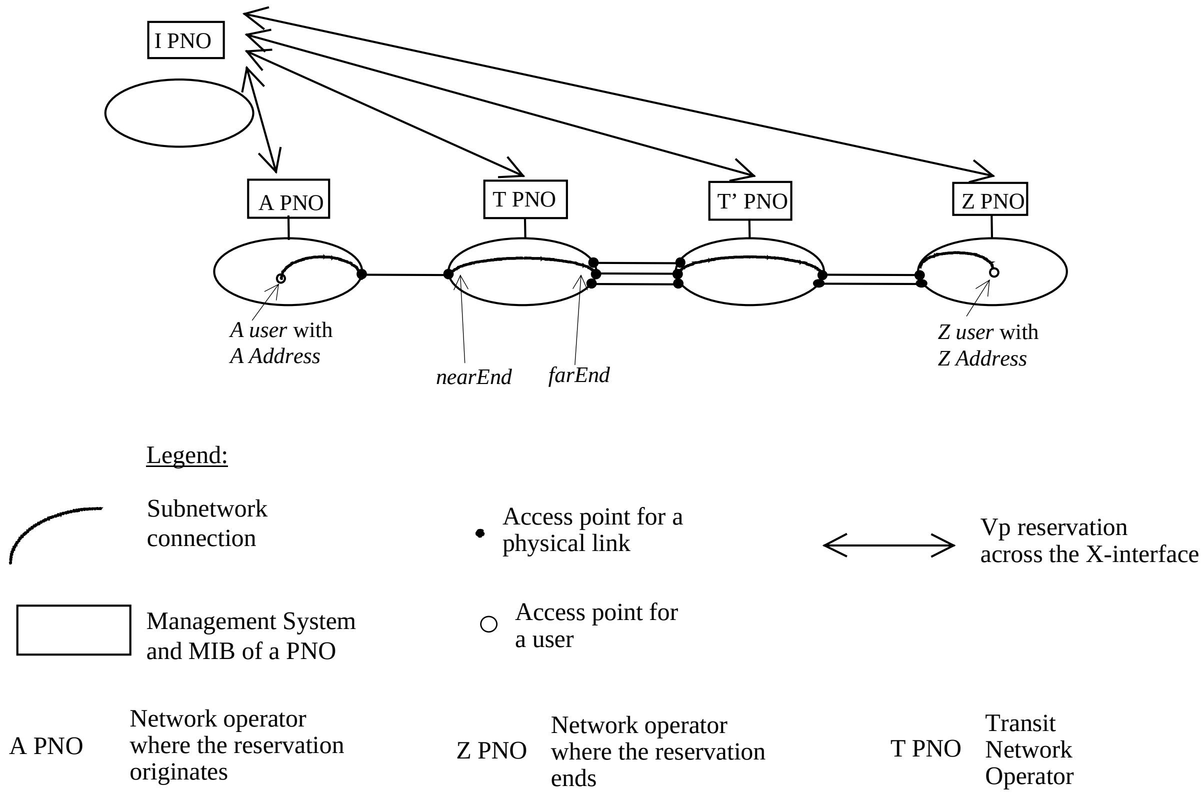


Figure 6: The "star" organizational model for interconnected ATM service management

Figure 6 shows the "I-PNO" as a separate operator from the "A-PNO". In many operational cases, the I- and A-PNO could be expected to be the same operator. T and T' are two adjacent "Transit" operators.

Note that the term "operator" is used generically in subsequent text to mean either an ATM-SP, ATM-CP or VA-SP as related to the business model described previously in subclause 6.3. (There is no intention in the present document to indicate the scope or range of business practices or roles which any organization might choose to provide in the general area of ATM interconnect services, or to be prescriptive about any operator's naming policies.)

Whilst noting the above discussion, it should be recognized that recommendation of the star organizational model for management of interconnected ATM services remains to be agreed at a business level between cooperating European operators and has not been tested in a commercial situation using automated interfaces.

Additional policy issues should be considered in relation to use of the X.easi interface as follows:

- Any two operators that want to interconnect should have a service contract. Therefore they have to agree on items including: X.easi management requirements, Implementation Agreements, bandwidth allocation and management, maximum failure recovery time targets, Quality of Service (QoS), service availability etc.

- For an automated interface, OSI Management (CMIP etc.) should be used, unless an alternative protocol solution can be agreed. (Refer also to subclause 11.3.)

- For a manual interface, X.easi management communication is very likely to be based on a simple fax-based messaging process. (Refer to annex G for further details.)

- The network elements that belong to the network of one operator cannot be accessed or controlled by other operators. (This may be contrasted with the specifications for Reconfigurable Leased Circuits services described in ITU-T Recommendation M.3208.1 [27].)

- The internal topology of a subnetwork should not generally be known to other interconnected operators. (Refer to figure 7 and associated text for clarification of this.)

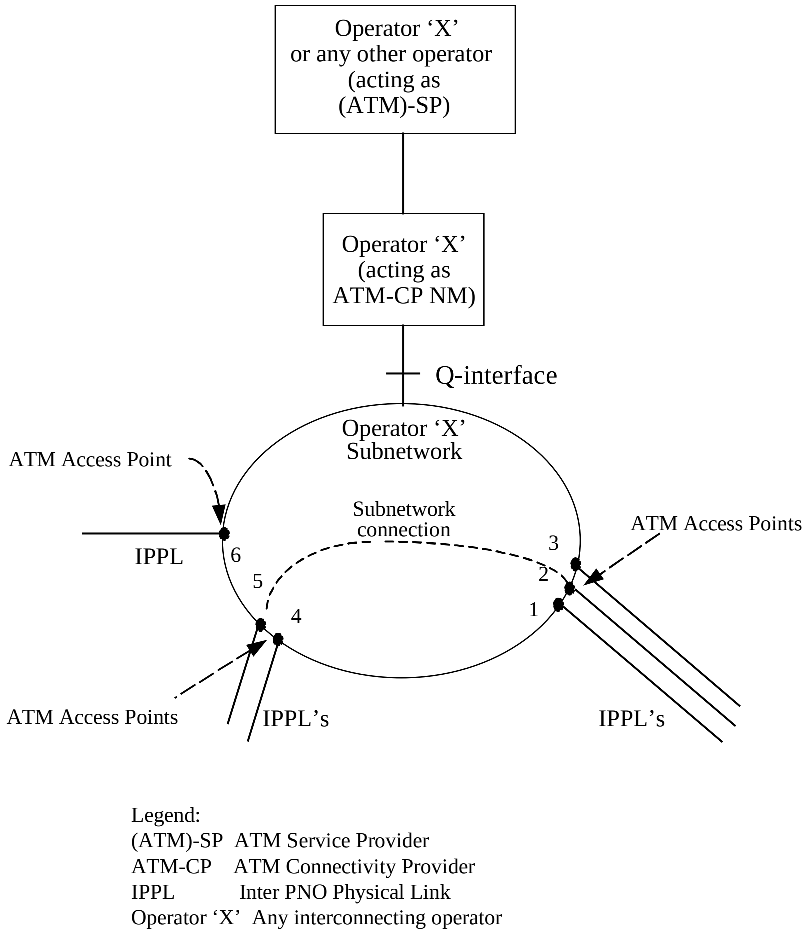


Figure 7: Example of a subnetwork showing ATM Access Points and external links

Figure 7 provides clarification of the policy on what is the extent of the shared information between interconnected operators: The roles of (ATM)-SP and ATM CP NM are shown specifically to align to the business model (figure 5). In this example, the view on Operator 'X''s ATM-CP resources that other providers have is: Only the ATM AccessPoints on the edge of Operator 'X''s network and the links (IPPL's) between Operator 'X''s subnetwork and other interconnected networks are "visible". The (ATM)-SP has a view of Operator 'X''s ATM-CP NM processes but not of the network or its specific interconnections.

Service-contracts (or bi-lateral agreements) between any two operators may be based on the use of "standard template documents" but certain details may be are proprietary to that pair of operators and are likely to be different for any other pair of operators.

When seeking information from another operator, the enquiring operator can only get information about the reservations and messages that refer to itself. This implies that messages about reservations must only be sent to the operator that made the reservations. This requires "access control" for security. Note, however, that failures in IPPL's should be broadcast [10] to other interconnected operators using an automated X.easi management system.

An operator must properly identify itself before it can make a management request of any kind. This requires "authentication" for security.

The initiator of an ATM-reservation has the freedom to decide which subnetworks shall be included in the route over the various networks. An operator has the right to refuse a reservation when the net of the Initiator is not a part of the overall reservation [6].

X.easi interface definitions do not include the Q management interface specifications.

ATM VP/VC reservations made using the X.easi interface should be established within a framework of previously made bi-lateral traffic forecasting agreements (refer also to subclause 8.3).

Levels of responsibility for use of the X.easi interface should be defined:

For instance, operators acting as ATM-CPs may have operational requirements to request more modifications in interconnected ATM VP/VC subnetworks than VA-SPs or other consumers are. This could follow an alarm indication [10], congestion situation affecting VP/VC performance or a request for bandwidth modification, for example.

Responsibility for management of the (IPPL) links between any two operators should be agreed on a mutual and bi-lateral basis.

Pending European and national legislation might enforce a customer "carrier pre-selection policy" – i.e. allow much greater choice (where a choice exists) for customers as to which operator transports ATM based traffic where interconnect agreements exist*. This area is for further study.

*** (For an overview of carrier pre-selection cases, refer to annex M)**

7 ATM Interconnect service processes model

7.1 Overview

Clause 7 introduces a model which summarizes all the pre-service and in-service interconnect process activities necessary to create and manage capacity for the support of ATM-based networks and services. This approach is based upon the results of EURESCOM Project P811 and is documented in [11].

7.2 Definition of the ATM interconnect processes model

The ATM interconnect processes model is sub-divided into the following four (bulleted) areas:

Interconnect Service Definition (ISD)

The interconnect service definition should include the technical specifications for interfaces, agreements and codes of practice to be used between operators.

Interconnect Service Establishment (ISE)

This is the set of Pre-service processes by which each pair of operators negotiate a specific interconnect service and bring it into service. This would normally include a programme of pre-service testing and validation.

Interconnect Service Administration (ISA)

This covers the processes by which each operator keeps the other updated with changes to aspects of the physical provision of the interconnect service, e.g. new links, points of interconnect (POI), new switches. Lists of manual and automated interfaces and associated statuses should also be maintained within this process area.

Interconnect Service Operation (ISO)

This covers the routine OAM processes for keeping the Service operational for individual customers. This could include use of an automated X.easi management interface for the configuration and maintenance of an ATM VP, for example.

The model presumes that an "industry process", denoted within box (a) of figure 8, will initiate the interconnect service definition and the technical specifications. Other processes and sub-processes, as depicted in figure 8, need to be defined to support the industry process.

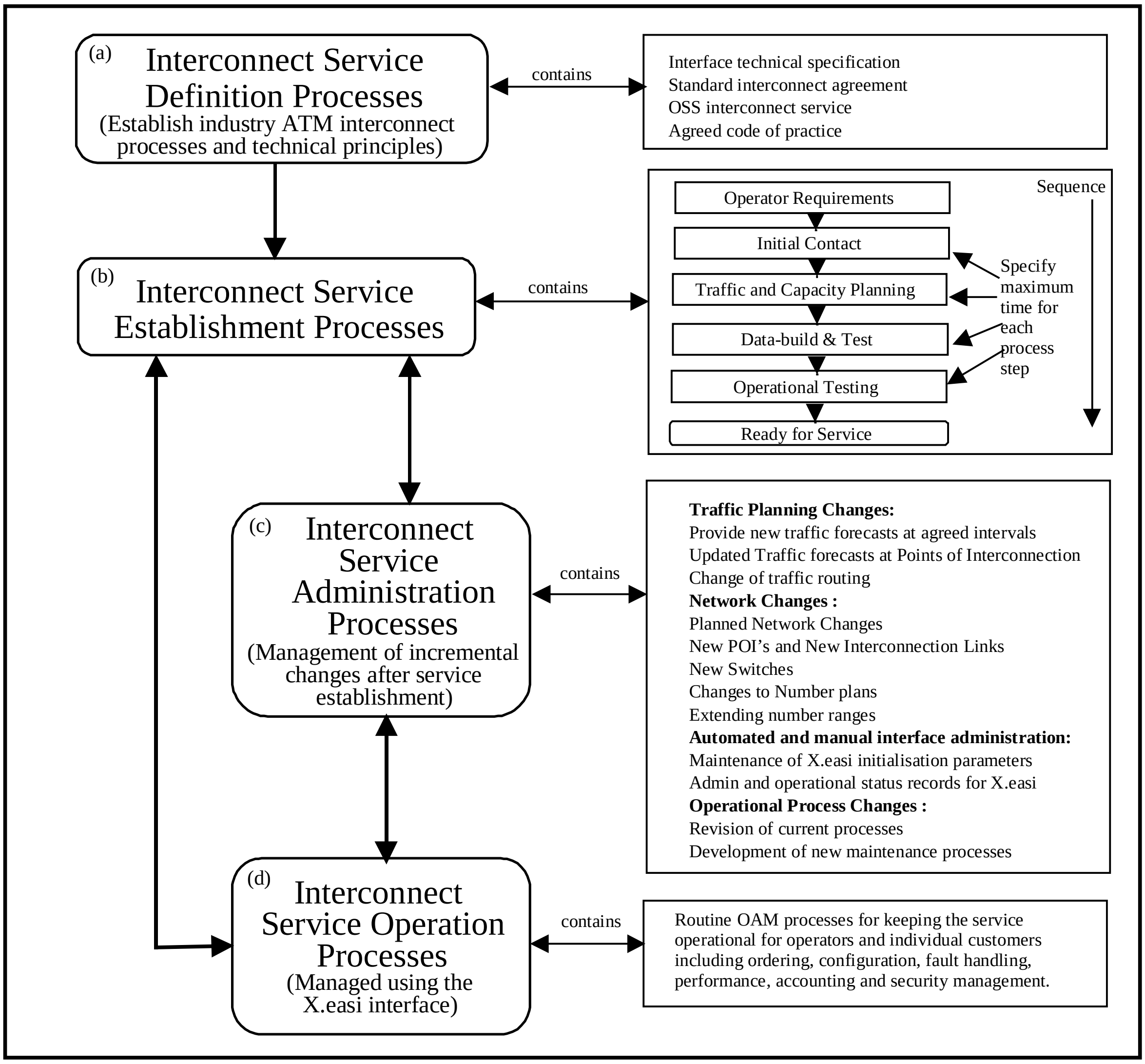


Figure 8: TM interconnect service processes model

Investment in planning and network resources to support ATM service provision is a business decision for each operator.

From an operational point of view, for each of the four main Interconnect Services shown in figure 8 boxes (a), (b), (c) and (d), an assessment should be made of the desirability for them to be managed by automated processes between operators OSS's.

Note that automation of most of the interconnect services listed in boxes (a), (b) and (c) of figure 8 would require a detailed specification and validation process which extends well beyond that currently available for virtual path provision as defined in [6]. (For the present document, interconnected network and management resources are assumed to be in place already.)

Accordingly, for Phase 1, it is realistic to conclude that the pre-service interconnect processes identified in figure 8 boxes (a), (b) and (c), are manual and mostly bi-lateral (between pairs of co-operating operators). The in-service interconnect service operation processes identified in box (d) may be managed by automated or manual processes using the X.easi TMN-based interface. The interface should be suitable for multi-operator management of interconnected ATM-based services, in alignment with the concepts introduced in figures 4 and 5.

(For later phases of interconnected ATM service introduction, it is reasonable to suggest that more functions of the X.easi interface, box (d) may be automated and several of the interconnect service processes in boxes (a), (b) and (c) could be specified as optional automated processes.)

Clauses 8 and 9 describe various parts of the ATM interconnect services and processes model in greater detail.

8 Pre-service interconnect service processes

8.1 Introduction

Clause 8 provides additional detail on the three "pre-service" interconnect service processes introduced in clause 7 and figure 8. Specifically, the subclauses 8.2 to 8.4 respectively elaborate on the details, scope and requirements of:

- Interconnect Service Definition (ISD) processes;
- Interconnect Service Establishment (ISE) processes;
- Interconnect Service Administration (ISA) processes.

The In-Service Interconnect Service Operational (ISO) Processes are described in clause 9.

8.2 Interconnect Service Definition (ISD) processes

Subclause 8.2 provides more detail on the processes shown within box (a) of figure 8.

The ISD processes are needed to establish the framework of major changes, or introduction of new technology in the infrastructure that can not be handled by the other processes. The result will be part of interconnect agreements between different connectivity providers.

The model requires that an "industry process" initiates the Interconnect Service Definition and the technical specifications. This joint EURESCOM/ETSI initiative can be regarded as fulfilling this requirement for European ATM Interconnect. The ISD processes should include the technical specifications for interfaces to be used between operators, e.g. transmission link interfaces, signalling interfaces, data communications network to support an automated X.easi interface (where implemented), etc.

The technical principles usually include: policies, and some form of top-level planning, routing and traffic/service capacity forecasting. (More specific details on these areas are provided within the ISA processes area, subclause 8.4.)

8.3 Interconnect Service Establishment (ISE) processes

Subclause 8.3 provides more detail on the processes shown within box (b) of figure 8. The ISE processes are needed to put into operation the framework specified by the ISD processes. Establishment (configuration) of ATM VP/VC services is handled by the ISO processes (described in clause 9).

Details on the ISE process are augmented in The "Operators Handbook" [3]. This provides a check list of the agreements that have to be made bilaterally as part of the ISE process. It is essential that the areas for bilateral agreement - e.g. policies, contact points, etc - are completed in the ISE process as they are pre-requisites for the smooth execution of the ISO processes.

8.3.1 Overview of the ISE Processes

Interconnect service establishment (ISE) processes include processes in which each pair of operators negotiate a specific interconnect service and bring it into service. This would normally include a programme of pre-service testing and validation.

A set of operator requirements and a further refinement of processes listed in box (b) of figure 8 is presented in table 2.

Table 2: Elaboration of the set of ISE Processes

Operator Requirements	Initial Contact	Traffic and Capacity Planning	Data build and test	Operational Testing	Ready for Service
technical specification and principles for the interconnect service	requests interconnect service contract	discuss and exchange traffic and capacity planning information	undertake initial data build information exchanges for POIs	ensure that an agreed test plan is available	use the X.easi interface for ATM service configuration and related activities. Ready for use of the ISO Processes
licence permitting use of interconnect services	identifies contact points (persons responsible for enacting processes)	provide traffic forecasts and Points of Interconnection (POIs)	confirm completion of data build (for POIs, switches, routing, etc)	undertake tests of CM for VP/VC connections	
necessary carrier identity codes (Operator identity, routing codes, SPCs etc)	identifies specific service establishment process forms and documents	provide network information such as CC7, SPC and routing prefixes		test availability of other management processes (e.g. FM, AM…)	
	formally requests an Interconnect service from a supplying operator	plan network resilience, performance and QoS criteria		confirm and agree that operational process tests are completed	
		plan network resource introduction to support forecast traffic (Refer to subclause 8.3.2)		exchange "Ready for Service" certificates	

8.3.2 Traffic and Capacity Planning – detailed description

Subclause 8.3.2 describes:

- the scope of traffic and capacity planning;
- the requirements for traffic and capacity planning;
- the principles for traffic and capacity planning;
- the processes for traffic and capacity planning.

Additional detail on traffic and capacity management processes is provided in annex E.

8.3.2.1 Scope of traffic and capacity planning

Traffic and capacity planning is needed to plan the medium term capacity requirements of Operators *networks* and the *links between those networks* in support of the following: ATM Interconnection Services, ATM Connection Types and ATM Transfer Capabilities/QoS Classes.

The definitive statement of the ATM User Plane requirements that have to be supported by NM in Phase 1 is to be found in [1]. An informative summary follows.

8.3.2.1.1 ATM Transfer capabilities and QoS classes

The ETSI NNI specification [1] identifies the following ATM transfer capabilities to be supported in Phase 1 (table 3).

Table 3: Associations between ATM Transfer capabilities and QoS classes

ATC name	QoS class	ATM Transfer Capability (ATC) definition	Equivalent ATM Forum service category and conformance definition
DBR (Deterministic Bitrate)	QoS class 1	Category based on maximum (Constant) bandwidth allocation	CBR (Constant Bitrate)
SBR 1 (Statistical Bitrate configuration 1)	QoS class 1	Category based on average (statistical) bandwidth allocation without priority control	rt VBR.1 (real time Variable Bitrate)
SBR 1 (Statistical Bitrate configuration 1)	QoS class 2	Category based on average (statistical) bandwidth allocation without priority control	nrt VBR.1 (non real time Variable Bitrate type 1)
SBR 2 (Statistical Bitrate configuration 2)	QoS class 3	Category based on average (statistical) bandwidth allocation with priority control - tagging not applied	nrt VBR.2 (non real time Variable Bitrate type 2)
DBR (Deterministic Bitrate)	QoS class U	Category based on non-guaranteed bandwidth allocation	UBR.1 (Unspecified Bitrate type 1)

NOTE: The remainder of this clause uses ATM Forum terminology (for traffic engineering).

8.3.2.1.2 Physical versus the ATM Layer Traffic and Capacity Planning

The User and Control Plane specification [1] describes the characteristics of both the ATM Layer and the supporting Physical layer options. Capacity planning is needed at the:

Physical Layer for E3 PDH and STM-(n) SDH realizations

ATM Layer for VPC **and** ATM Layer for VCC.

("ATM types" is a short-form to describe the combined Connection Type and ATC/QoS. Such terminology could be useful to describe the available ATM service offerings.)

The present document restricts planning to that required for the ATM Layers and assumes that the linkage to the Physical media layer is dealt with elsewhere by current planning procedures for PDH and SDH. However the ATM layer planning will place requirements on the Physical layer and these are captured in the requirements listed below. Part of the ATM Layer Planning requires that the ATM VP's are mapped onto the Physical Layer. This requires planning information to be available about the Physical Layer to ensure that resilience and diversity are achieved with ATM Layer Connections.

In [6] the links between operators are modelled as follows:

Inter PNO Physical links – these represent ATM requirements on the Physical Layer.

PNO Network ATM Access Points that model the end of the physical links at the subnetwork gateways.

The number of PNO VP/VC subnetwork connections and their type/characteristic is the main purpose of ATM Layer Traffic and capacity planning for supporting the User Plane traffic.

8.3.2.2 Requirements for traffic and capacity planning

8.3.2.2.1 Overview

One of the important aspects of the Interconnection Service Establishment Process is that operators should agree not only the interconnect services that they will offer one another but also the types, location, ATM traffic forecasts and capacity of that interconnection. This process also provides updates to those agreed interconnect service capacities as connection traffic grows, new points of interconnection are established and when points of interconnection are withdrawn. It is for this latter reason that it is necessary to forecast the number of PNO Network ATM Access Points.

8.3.2.2.2 Requirements

Forecasting process:

A process is needed between operators that forecasts and provisions/orders bulk interconnect capacity so that when an individual ATM connection is requested, be it a PVP, PVC, Soft SVC or SVC, that adequate capacity exists at the POIs between the operator subnetworks.

Allowed bandwidth granularity:

Bandwidth requests are not allowed to be infinitely variable but should be selected from an enumerated set (e.g.64 kb/s, 128 kb/s….1 Mb/s, 2 Mb/s…….10 Mb/s, 15 Mb/s). I.e. the bandwidth must be allocatable in reasonably manageable "modules".

Interconnection modelling:

The interconnection is required to be modelled at multiple layers. A model is needed to show the relationships between different forms of interconnection at different levels e.g. physical cable layer, Optical layers, Multiplexer layers and interconnect connection layers such as ATM PVP.

Capacity planning:

Capacity planning within an individual operator's network is out of scope of this process definition. However operators will need to link these interconnect process to their internal processes in order to ensure that satisfactory end to end service is provided to customers.

Exchange and capability of orders:

"Orders" are required to be exchanged between operators formally requesting the provision of specific forms of interconnect capacity at specific locations/routes at specific points in time. The orders should be capable of being negotiated progressively prior to their formal commitment (this may be defined as a pre-order process). Orders should be capable of including several interconnect service requests that are to be delivered as a package. These may be for the same type of interconnect capacity at different locations or of different ATM Transfer types and QoS Classes.

Addressing and circuit identifier schemes:

These schemes should align with applicable ITU-T and ETSI standards. Refer to annex B.

Planning models:

The planning models should permit forecasting intervals for each layer to be agreed independently between operators and should permit forecasting intervals to be agreed bilaterally between operators.

NOTE: It should not be assumed, for any individual point of interconnect, that capacity continuously grows. In some cases, as operators open new physical interconnection or chose to route connections differently capacity may drop at one point but grow elsewhere.

8.3.2.3 The principles for traffic and capacity planning

Traffic and capacity planning should include recognition for the fact that ATM networks may carry a mixture of traffic types and QoS classes.

In order to meet acceptable targets for services offered to the end customer there have to be agreements between operators on the way in which they plan the required end-to-end links. For Phase 1, the star organizational model [6] should be used for establishing connections so it is mainly under the control of the Originating PNO as to how the end to end QoS is achieved.

The JAMES project produced the "Guidelines and the design rules for ATM Network planning". This does address the important issues of how traffic can be mixed and how overbooking can be introduced to achieve network efficiency. This is a very important capability on costly long haul international routes.

These Guidelines impact:

The calculations and rules used in the Traffic and Capacity Planning forecasts and processes.

The way in which operational support systems respond to request for available capacity and instruction to request/reserve capacity for specific connection types, ATM Transfer Capabilities and QoS Classes and for specific *Source Traffic Descriptors*.

It seems that the principles for the calculations and rules to be used for Capacity Planning Models should be restricted to the following three alternatives, which are presented in table 4:

Table 4: Summary of restrictions for capacity planning

On demand capacity	Forecast capacity	Pre-reserved capacity
An initiating operator requests capacity without making any prior capacity reservations or forecasts. QoS and availability are on a "best endeavours basis" and the costs charged by the other operator(s) are determined on a connection by connection basis working to a formally published price list (which may be varied from time to time).	Operators exchange forecasts of the capacity they expect to require broken down by ATM traffic classes, QoS, and Destination Area (such as ITU-T Recommendation M.1400 town codes [13]). QoS and availability are guaranteed for the forecast levels. And the costs charged like the "on demand capacity" procedures. QoS may be maintained for agreed levels of overbooking such as 120 % of forecast. Outside these bilaterally agreed limits QoS is not guaranteed. Under-booking by some bilaterally agreed margin may incur financial penalties.	Each operator reserves logical capacity amongst itself and other operators for which it pays a set of leasing charges. Connections are established across this logical capacity network and transaction charges my be levied for each configuration, modification, reconfiguration or release request.

The extent to which capacity planning and the restrictions proposed in table 4 is a co-operative activity between Operators depends upon the business model adopted for the relationship between the PNOs.

In the case of "Pre-reserved capacity", where the A-PNO pre-purchases the capacity from another operator on the inter-PNO links, the A-PNO can control the traffic mix precisely and therefore accepts responsibility for any overbooking and the consequent delay and QoS degradations.

For the other two capacity planning models - "On demand capacity" and "Forecast capacity" - both parties need to co-operate in both the Traffic and Capacity forecasting and the reservations allocation processes to ensure that satisfactory throughput and QoS targets are achieved. In these cases bilateral agreements will be needed that agree which planning rules and guidelines are to be adopted.

The present document should provide a basis for multilateral agreements on a minimal set of overbooking guidelines that operators may support. Other more aggressive overbooking procedures may be adopted by bilateral agreement.

8.3.2.4 ATM traffic management

The traffic management functions should be implemented according to ITU-T Recommendation I.371 [12] (and ATMF Traffic Management Specification [14] wherever appropriate).

Guidelines and design rules should be chosen from those determined in the JAMES Deliverable.

8.3.2.5 ATM Connection Admission Control

ATM Connection Admission Control (CAC) is defined as the set of actions taken by the network at the connection set up phase (or during connection re-negotiation phase) in order to determine whether a VCC can be accepted or rejected. This process also determines whether a new connection can be accepted without violating the QoS for existing connections. The CAC definition is specific to each operator's network, and is out of the scope of the present document.

As an example for CBR services, CAC should specify that the maximum allowed load on a 34Mb/s physical link will be 72 000 ATM cells/s for CBR services and for VBR-nrt services. This assumes a "conservative" use of bandwidth according to the formula:

$BW_{max} = \rho * L$ (where $\rho = 0,9$, BW_{max} = maximum bandwidth that can be allocated by CAC, L = linkrate = 80 000 ATM cells/s)

This will be a typical value to choose but the actual choice of ρ will be a matter for bilateral agreements between operators.

For VBR traffic the statistical nature of the traffic should be taken into account for the determining the effective bandwidth.

An example of calculations for CAC for a VBR connection is shown below:

For a VBR connection an effective bandwidth (BW_e) can be calculated such that:

$$\mathbf{SCR} \leq \boldsymbol{BW_e} \leq \mathbf{PCR}$$

SCR is the Sustainable Cell Rate and PCR is the Peak Cell Rate of the connection. For a CBR connection BW_e = PCR.

The idea is that a VBR connection with effective bandwidth BW_e has the same effect on performance as a CBR connection with PCR = BW_e ("greedy" sources are assumed). BW_e is calculated with this objective. It depends on the burstiness and the buffer size.

The CAC will now be:

$$\sum_{i} (BW_e)_i \leq \rho * \text{linkrate}$$

where the summation is over all virtual connections on the link and ρ is as above (i.e. ρ = 0,9). This formula is valid for any combination of CBR and VBR connections.

8.3.2.6 Overbooking

As interconnect capacity, especially international, is a limited and expensive resource, the concept of overbooking of the connections across the inter-operator interfaces should be supported in the Phase 1 NM solution.

Overbooking relies on the fact that statistically the bandwidth at any one given time will not be fully utilized. Overbooking implies that QoS no longer is no longer guaranteed. In a first phase it may be applied to get a better link utilization, but it must be done with care. The overbooking factor should be based on experience, but if traffic conditions change quickly buffers can overflow. A safer way to get higher network utilization may be to encourage users with appropriate applications to use ABR services.

Certainly, an overbooking factor of 1 must be accepted for the CBR service. However, an overbooking factor of N may be used for VBR-nrt service, whereby the effective bandwidth (BW_e) booked on the inter-operator (international link) is given by the following formula:

$$BW_e = 1/N \sum_{K=1}^{n} (SCR_{VBR\text{-}nrt})_K + \sum_{J=1}^{m} (PCR_{CBR})_J$$

where:

n and m represent the maximum number of VBR 1-nrt and CBR connections configured on the link

N represents the overbooking factor. SCR = sustainable cell rate, PCR = peak cell rate

The value of N should be defined bilaterally but use of a minimum value of 1,5 during Phase 1 is recommended.

8.3.2.7 ATM QoS design parameters

Quality of Service limits need to be agreed between interconnected operators. The following bullets describe traffic management aspects related to QoS.

Maximum number of subnetworks traversed

The number of subnetworks traversed to support an ATM interconnection service (in Phase 1) is recommended not to exceed four up to and including the interconnect gateways. (This is based on current experience in the provision of International Private Leased Circuits.) Simplistically, that would provide for a maximum of one A-PNO, one Z-PNO and two T-PNOs supporting the connection. For CBR the problem is not critical because CBR traffic queues should be definable and easily manageable. However VBR traffic may well be delayed if the network is busy.

Link loading – unprotected links

CBR traffic should not exceed 80 % on any single physical link. Simulations have shown that a relatively small CBR buffer could cause cell loss if more than 80 % of the traffic is CBR and all CBR traffic jitters as much as the default Cell Delay Variation (CDV) tolerance allows. The value 80 % depends on the CLR requirements and is normally configurable in CAC. A value from 80 % to 90 % is normal ($0,8 \leq \rho \leq 0,9$). The reason we get cell loss is that ATM is asynchronous and even CBR will not have a constant rate in the network (inter-arrival times are not constant).

It is proposed to keep the total loading significantly below 100 % of physical link capacity as this allows for the VBR traffic to be statistically multiplexed while probably remaining within the target cell loss figure.

Link loading – links with protection

Historically physical link loading has been kept to 80 %. (Note that the 80 % referred to here is probably due to different reasons then the 80 % mentioned under the previous bullet.)This allowed for re-routing in the event of failure and for traffic growth during the timelag for ordering and installing new equipment.

However with physical links protected by SDH backup in milli-seconds or PDH restoration within one hour the need to limit physical link loading for re-routing is not considered to be essential.

Conversely if physical links are heavily loaded there is a risk that VBR+ traffic may not be supported. Often, however, connections may not be active and it is believed that a high overbooking factor may be achievable in practice. This will need to be agreed on a bi-lateral basis between operators and should take into account the service options being supported e.g. ABR.

Additional information on the detailed capacity planning rules and processes is provided in annex E. Other design parameters not related to QoS may be required but have not been identified within the scope of the present document.

8.4 Interconnect Service Administration (ISA) processes

The ISA processes are defined in order to provide an administrative structure for efficient operation of ATM interconnection processes and services, especially in the area of management of incremental changes after initial service establishment has been completed.

Subclauses 8.4.1 to 8.4.5 provide more detail on the processes shown within box (c) of figure 8 and describe:

- traffic planning changes;
- network changes;
- automated and manual interface administration;
- operational process changes.

8.4.1 Traffic planning changes

Traffic planning changes are required to optimize the use of available capacity or to influence planning for new capacity. Areas for which processes for the exchange of information between interconnected operators are required include:

- traffic forecast changes at agreed intervals;
- traffic forecast changes at Points of Interconnection (POI);
- traffic routing changes.

8.4.2 Network changes

Information about network changes should be exchanged where any aspect of the interconnected network between any two operators is altered.

Areas for which processes are required for the exchange of network change information between operators include:

- Planned network changes (including planned down time for maintenance and alterations to the network resources).
- New POI's, switches and new interconnection links. For example, the addresses and identities of the gateway switches and inter-PNO physical links should be exchanged.
- Changes to numbering plans, including extensions of number ranges.

8.4.3 Automated and manual interface administration

An essential administrative process is that of maintaining details of interconnect service operation process interfaces – basically the automated or manual X.easi interfaces (introduced in subclause 5.6.2).

The processes identified for the automated and manual interface administration area include:

- maintenance of X.easi interface initialization parameters;
- administrative and operational status records for the X.easi interface;
- converting X.easi functionality from manual to automated management (or vice-versa).

As both manual and automated X.easi interfaces may be supported for most management functions (e.g. Configuration, Fault etc), the automated and manual interface administration service must support:

- processes to set up communication between OSSs or between OSEs;
- processes to keep trace of an Administrative Status, reflecting the current status of an OSS or an OSE in terms of availability, automation and level of management services supported;
- processes to declare an OSS "temporarily out of service", thus setting up OSE functionality, with the reverse at the end of the OSS unavailability period;
- processes to monitor the performance of the various management services (required if response times are part of any inter-operator Service Level Agreement).

NOTE: The processes described above require different kinds of information to be exchanged depending on whether it concerns OSS or OSE, but in both cases the exchange is "manual".

Table 5 provides examples of the information exchange process details relating to the OSS and OSE cases for automated and manual interface initialization, administrative status and operational state. (Many of the terms listed in the OSS column are elaborated in clause 9.) Note that table 5 lists examples of information recommended to be kept and most often exchanged by each operator but this is dependent on inter-operator agreements in each bi-lateral case.

Table 5: OSS and OSE parameters, statuses and operational states

	OSS (automated X.easi interface)	OSE (manual X.easi interface)
Initialization parameters	OSS contact name X.25 (or other DCN) address etc. (protocol parameters) Specification of Management Services functionality level list of minimum capabilities and requirements initial MIB	OSE contact name (maybe one per Management Service) fax, phone, mail address specification of Management Services functionality level list of minimum capabilities and requirements opening hours escalation point
Administrative Status values	install planned capability under interoperability test, gives list of interfacing Operators for which tests are completed under CM, FM, PM tests…can be decomposed, by Management Service, giving a list of interfacing Operators for which tests are completed in service, gives a list of Management Services supported with each interfacing Operator withdrawal of interfacing Operator planned, giving date	in service is the default value, gives list of Management Services supported with each partner
Operational state	enabled soon under maintenance (give date to switch on OSE) under maintenance (give date to switch back on OSS) disabled	Not applicable (a manual interface should be available when trained personnel are available)

A number of "non-functional" issues should be considered in relation to administration of the automated X.easi interfaces (OSS). Probably the most important is that interconnected OSSs rely on TMN platforms and DCNs (described elsewhere in the present document). Further, current TMN platforms support OSI-based applications which are difficult to get to inter-operate over the X.easi interface. Any changes in the configuration or capability of any platform is likely to require new inter-operator validation tests. As a consequence of any platform change, administrative status values in table 5 must be changed in response to information received and tests organized to validate that the new platform configuration is able to support ATM service management.

8.4.4 Operational process changes

Administration Processes are required for the following:

- revision of current processes;
- development of new maintenance processes.

In both cases, updates to established processes are involved. This should normally be accomplished by inter-operator agreements and the development of new process templates, where manual exchange of information by fax is involved. In the case of development of new maintenance processes, documentation updates in addition to fax template updates would probably be required.

Finally, it may be noted that EURESCOM Project P707 has considered automation of processes and interfaces in the general area of "Administration of Network Management" [15], which has general relevance to interconnect service administration processes, as described in the present document. For a "Phase 1 solution", automation of interfaces for the various administrative processes would seem to be unsuitable but such an enhancement for the Phase 2 solution should be considered in due course.

This concludes discussion of the interconnect service administration processes. Clause 9 considers the interconnect service operation processes.

9 In-service Interconnect Service Operations processes - the X.easi management interface

9.1 Introduction

Clause 9 provides a description of the in-service ISO processes which were introduced in the model shown in figure 8. The ISO processes are designed to provide and manage VP/VC services as a routing business operation. Particular consideration is given to the management requirements and functions which may be supported on an automated X.easi interface.

Subclause 9.1.1 provides general considerations for the X.easi interface. Subclause 9.1.2 considers the processes (or management functions) which are required and which may be operated by automated or manual implementations. Subclause 9.1.3 proposes which interconnect service operations processes should be considered for automation in Phase 1 and Phase 2 [16].

Subclauses 9.2 to 9.6 provide descriptions of the interconnect service operation processes which result in the exchange of data to support the well-known functional areas of Configuration (Ordering), Fault (ATM VP/VC alarms), Performance, Accounting and Billing and Security Management.

9.1.1 General considerations on automated and manual X.easi interfaces

It is a reasonable proposition that any process which may be undertaken using an automated management interface must also be able to be undertaken using a manual management interface.

Automation in the X.easi interface may be a phased process. That is, some interconnect service operations processes (management functions) may be introduced in Phase 1 using automated inter-operator processes whilst being supported by manual processes for other functions. For Phase 2, more or most of the interconnect service operations processes may be considered for automation.

In order to keep this description of the X.easi interface concise, heavy use is made of references to external documents covering requirements, technical specifications, standards and general operational procedures.

The descriptions of the ISO processes for the configuration and fault management functions of the X.easi interface are elaborated by reference to annex A. A consistent method of naming and addressing is considered in more detail in annex B.

9.1.2 Summary of X.easi interconnect service operation processes

Figure 9 illustrates the interconnect service operation processes (or Management Functions, in TMN terms) of the X.easi interface identified to provide real time processes, within and between operators, for the provision of ATM services. The X.easi processes are assembled within box (d) and shown interacting with the implemented ATM network, as specified by reference to [1].

Above the X.easi processes, the other pre-service interconnect processes defined in the ATM interconnect services and processes model, figure 8, are repeated without elaboration. Indeed, the boxes identified by (a), (b), (c) and (d) in figure 9 coincide with equivalents (a), (b), (c) and (d) shown in figure 8 and are repeated simply to re-emphasize the context of the X.easi management interface.

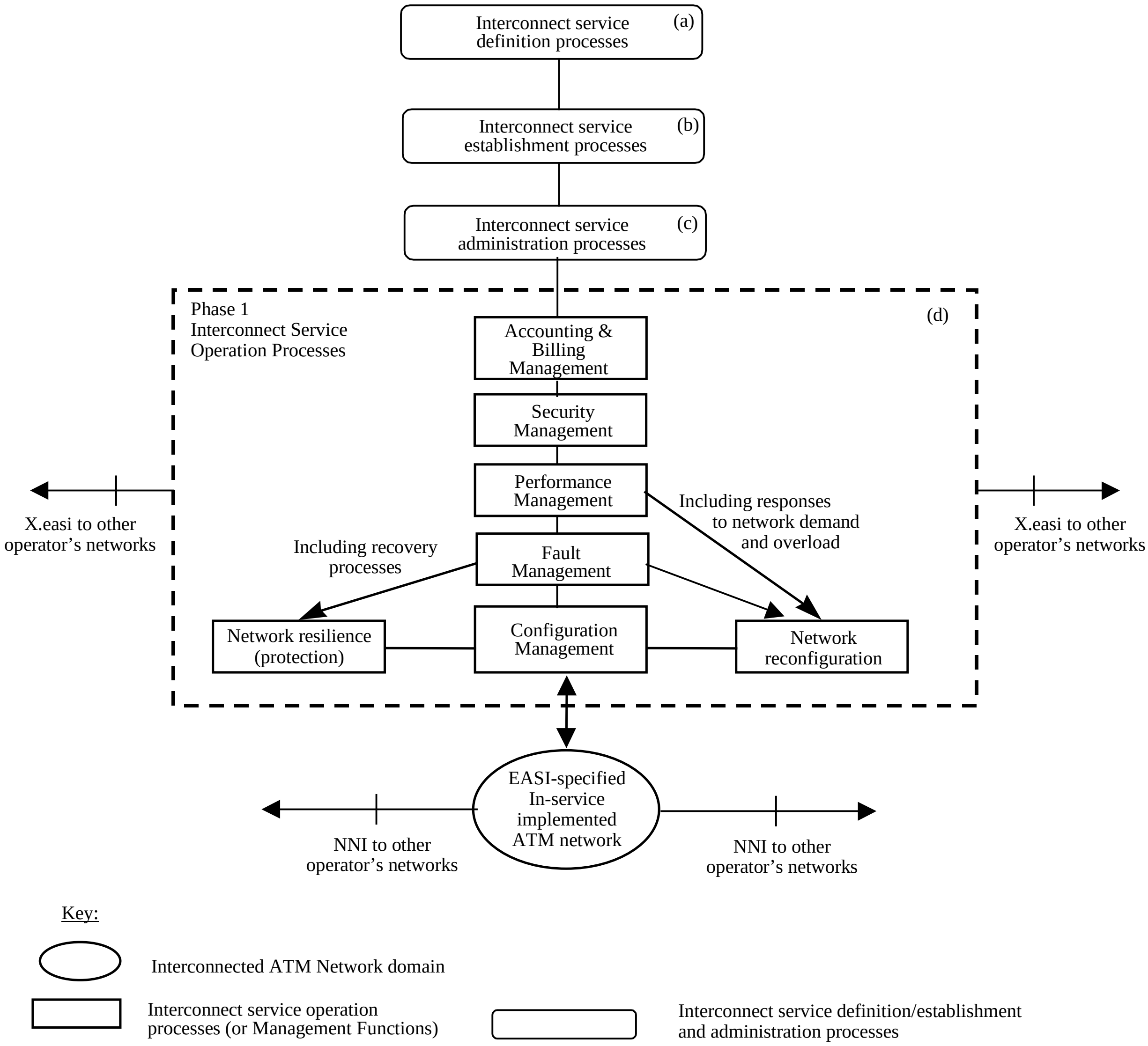


Figure 9: Summary of X.easi and other related interconnect processes

It is first necessary to consider various aspects relating to "automation" of the X.easi interface, including constraints and phasing issues. This is described in subclause 9.1.3.

9.1.3 A view on phased X.easi automation for ATM services

The proposition in the present document is to support highly available and resilient management processes (otherwise known as management functions) on the X.easi interface. This leads to the desirability to progressively automate various management processes, as indicated in table 6. A manual interface must always be available where deployment of an automated interface is recommended or technically feasible (to provide fall-back processes in the event of failure and as a general means of ensuring non-discriminatory management interface interconnection availability). Adequate security mechanisms must be provided for both manual and automated interfaces.

A summary of the Phase 1 X.easi interface specification requirements and recommendations for each ATM service capability is shown in table 6 and is accompanied by detailed explanatory notes.

Table 6: Summary of ATM Service Capability and recommended Automated/Manual options for Phase 1 service introduction

	Configuration Management	Fault and TT Management	Performance Management	Accounting Management
ATM Service Capability				
PVP	Automated	Automated	Manual (3)	Manual (2)
	Manual option (1)	Manual option (1)		
PVC	Automated	Automated	Manual (3)	Manual (2)
	Manual option (1)	Manual option (1)		
SVC	Manual (4)	Automated (5)	Manual (3), (4)	Manual (2), (4)
		Manual option (4)		

Descriptions of what is meant by "Manual" and "Automated" interfaces are provided in subclause 5.6.2, with a further elaboration in annex G. It is assumed that all automated and manual functions, processes and capabilities will only be deployed with an adequate security specification and solution in place. For table 6, the following 2 bullets are applicable:

- "Automated". This relates to an interface process which is operated using interconnected computer-based technology and is ETSI or ITU-T compliant with an available specification and validation documentation.
- "Manual" This related to an interconnect process which is operated using conventional technology such as faxes between operators and required a high degree of human involvement to accomplish all the associated processes.

It should be noted that all X.easi processes and functions, whether operated by automated or manual means, should have target times and associated process time-outs ascribed. Such times and time-outs should be considered as part of the non-functional requirements of the X.easi interface. General recommendations may be made and operators should establish limits as part of bi-lateral agreements.

NOTES for table 6:

NOTE 1: An automated X.easi interface process for Configuration Management and Fault Management and Trouble Ticketing is recommended for Phase 1 PVPs and PVCs. For PVCs, automation of the X.easi depends upon an extension to the current interface specifications (which are generally restricted to PVP at the present time). The Manual option must also be available.

NOTE 2: The issue of whether an automated X.easi interface for the exchange of Accounting Management records may be recommended, is still under consideration.

NOTE 3: For Phase 1, it is assumed that switches, or external measuring equipment could produce performance statistics which can be used for the manual exchange of performance data. (Refer also to annex H.)

NOTE 4: SVCs are established by signalling and the signalling to some extent substitutes for management plane functions. Switched services require different resources which need to be managed as compared with Permanent or Semi-Permanent connections. This is reflected in the NNI specification [1], which requires that switched virtual channel connections and permanent virtual channel connections shall be transported in different virtual path connections. Essentially the resources that have to be managed are signalling, routes and capacity together with the necessary customer service management aspects. The preliminary analysis of the network management requirements for (mandatory) switched services listed in [1] indicates that existing management solutions for PSTN management should provide a suitable basis for the Phase 1 solution in this area. Management requirements and issues should be considered in more depth in a related deliverable [4], mostly in regard to the Phase 2 solution. In any event the required processes for switched services are usually manual even for high volume services such as PSTN, and the pressure to automate management interfaces is most likely to be in the area of Fault Management/Trouble Ticketing. During Phase 1 this can be accommodated by bilateral agreements between operators that are providing the interconnected network capacity to support switched services. In other words, use of the X.easi interface, configured in the Star organizational model, is not specified for SVC services offered within Phase 1 of interconnected ATM service introduction.

NOTE 5: The current Trouble Ticketing standard provides fault codes for switched services. Accordingly, an automated interface may be considered as an option for Phase 1 but may be limited to bilateral messaging, as described above in note (4).

9.2 Configuration Management Processes

9.2.1 Overview to CM processes in relation to pre-service provisioning processes

Configuration Management processes are dependent on the completion of pre-service Provisioning processes which may be taken to include all network resource introduction activities required to give an operator the opportunity to offer and support ATM VP and VC services within and beyond its network domain. Beyond that, provisioning processes cover the initial requirements for meeting customer ATM service orders. These processes could include handling responses to customer requests for service and associated resource allocation. General customer and inter-operator contractual arrangements as well as billing and customer-complaint processes may be considered to come into the range of provisioning processes. In general, provisioning processes relate to resource availability whereas configuration processes relate to the creation of ATM VP or VC services.

9.2.2 Configuration Management

9.2.2.1 General requirements

Configuration Management is a process which should lead to the creation of virtual paths and virtual channels (VPs and VCs) to meet customer requirements. The process is dependent on a choice of the "organizational model" for interconnected operators. This choice is discussed in subclause 6.4, "Policy Issues", with the conclusion that the ETSI "Star" model should be recommended for Phase 1 ATM service introduction.

The organizational model provides a framework for the usage of X.easi interface relationships between operators. The choice of model has a strong bearing on the organization of all inter-operator network management procedures. It may be noted, for example, that the specifications developed and used in the JAMES and EURESCOM P408 [11], [8] X-interface specification and validations projects depended on a "Star" organizational model. By contrast, many of the currently operated correspondent services are generally organized using a "matched ordering procedure" which involves only two operators. Some details on the matched ordering processes are provided in annex A, which are based on the expectation of using manual procedures but which could be handled by automated procedures.

According to ITU-T Recommendation X.700 [17]: Configuration management:

- identifies;

- exercises control over;

- collects data from and provides data to open systems,

for the purpose of preparing for, initializing, starting, providing for the continuous operation of, and terminating interconnection services.

Configuration Management process definitions should be limited to the capabilities required for (semi-permanent) PVPs, PVCs and possibly SVCs for the Phase 1 solution, in response to the requirements of the ETSI EASI network specification [1]. (It should be noted that SVCs are not configured by management, but by the use of signalling. The configuration of the environment needed to support setup of SVCs, comprising setting up of signalling channels and identifying links for traffic, is provided by network management.)

The setting up of transmission links for permanent circuits is considered to be outside the scope of the present document and is probably adequately covered by reference to the current arrangements for provision of international private leased circuits.

9.2.2.2 Specifications for procedures and interfaces

The approach to Configuration Management should, as far as possible, be based on approved public standards and specifications. Currently, this means in practice, using EN 300 820-1 [6], ITU-T Recommendation I.751 [18], ETS 300 469 [19], and the underlying generic TMN and OSI specifications such as ITU-T Recommendation X.700 [17] ITU-T Recommendation X.721 [20], ITU-T Recommendation M.3100 [21] and ES 200 653 [22].

In order to implement automated interface management, applications based on the standards listed above should be profiled according to experience gained in the EURESCOM projects listed previously and the JAMES project with enhancements based on implementation agreements. Note that the JAMES document does not explicitly address the subject of configuration of SVCs or PVCs.

For manual interface solutions, a discussion of possible relevant procedures is provided in annex A, "Phase 1 ATM interconnect management procedures for Provisioning of PVP and PVC Connections and associated Maintain and Repair processes".

Configuration Management processes allow any initiating operator the ability to reserve, modify and release communications resources. The term "communication resources" is used to indicate resources that are directly involved in providing services to customers and that are provided by two or more interconnected operators. Examples of such resources are: PVPs or VPNs spanning the network domains of two or more operators. The processes to handle this are all performed from the initiating operator (irrespective of the organizational model chosen). Configuration Management provides management functionality, divided into six basic procedures (Establish, Release, Modification, Reconfiguration, Activate and Deactivate management functions) which are elaborated in annex A and also in the standard [6]. (Concurrent with the development of the present document, [6] is being enhanced by the ETSI TC TMN group to provide specifications for CM of PVPs with resilience and performance monitoring options. The anticipated enhancements do not affect the fundamental CM processes described in subclause 9.2 and should be viewed as a potential benefit for interconnected ATM service introduction.)

9.2.2.3 Interoperability requirements

Automated X.easi interfaces for the exchange of configuration information for PVPs should conform to all the mandatory requirements in [6], subject to any implementation agreements which may be necessary to effect the interface.

For manual X.easi interfaces, procedures based on the descriptions in annex A should be considered.

9.3 Fault Management Processes

Fault Management processes should be designed to deal with impairments in the network infra-structure. Processes should include responses to Performance degradation notifications, "ownership" of faults and their associated resolution, issue of and responses to "Trouble Tickets" and issue of and responses to alarm notifications exchanged over the X.easi interface. Accordingly, the Fault management processes described in the present document are of broader scope than recognized in the basic TMN organization defined in [7].

This set of Fault Management processes should also include a strategy for "network protection and resilience", as indicated in figure 9. However, implementation of a detailed and generally automated resilience strategy should be considered out of the scope of the Phase 1 specification but should be considered for the Phase 2 specification (although this position should be reviewed when enhancements to [6] are available from ETSI). Information relating to these (Phase 2) requirements may be found in [23] and [24]. The latter document [24] provides guidance on solutions for fault management in relation to the requirements for the various layers (e.g. application/ATM/SDH) involved in the provision of ATM services.

9.3.1 ATM VP/VC alarm reports and trouble ticketing processes

9.3.1.1 General requirements

Maintenance and repair processes depend on ATM VP or VC alarm reporting (otherwise known more generically as "Fault Management") together with the issue and activation of Trouble Tickets. All such processes depend on specification of the X.easi interface where inter-operator service operation processes are concerned.

The principle requirement is:

- To ensure the network maintenance and repair processes of interconnected ATM network operators (including the exchange of trouble tickets and failed connection alarm reports) are conducted efficiently and rapidly in order to minimize or eliminate out-of-service conditions.
- The general requirements for fault handling service operation processes performed across the X.easi interface are:
  - Recognition of a fault or performance degradation which affects ATM services.
  - Creation and reporting of problems between operators (Inter-operable trouble ticketing).
  - Recognition of repeat alarm conditions.
  - Co-operative localization of faults between operators.
  - Procedures for escalating repair processes (to higher management levels).
  - Clearing and cancelling of requests for testing following fault management processes.
  - Archiving of fault reports and trouble tickets.

These requirements have been considered in detail in the EURESCOM Project P612 [25]. A presumption has to be made that equivalent processes for manual and automated interfaces are available.

- The general requirements for exchanging alarm information, at the ATM VP level, are:
  - Raise alarm reports on failures on physical links interconnecting operators' subnetworks.
  - Raise alarms reports on (logical) subnetwork connections that are service-affecting.
  - Report when alarm conditions have been cleared.
  - The ability to inspect the Sent Alarm Logs (for automated interfaces) [10].
  - Support and meet ITU-T maintenance standards in M.1530 [26].

Most of these requirements are elaborated in the ETSI standard for ATM VP Alarm Management EN 300 820-2 [10]. Alternatively, requirements and solutions recommended in ITU-T Recommendation M.3208.1 [27] may be suitable. (The standard [10] is due to be revised by ETSI TC TMN but is not expected to be changed in management functionality. Descriptive changes only are anticipated.)

Clearly, the above requirements and associated processes need to be extended to the ATM PVC level, for which there is currently no suitable standards.

9.3.1.2 Specifications for processes and interfaces

When deploying an automated interface for management of interconnected ATM networks, the following requirements may be identified for alarm management and implementation of maintenance and repair procedures, including trouble ticketing:

- Trouble ticketing procedures and scenarios as described in [25].
- ITU-T Recommendation X.790 Trouble Management Function for ITU-T Applications [28].
- The detailed implementation profile for X.790 [28] provided in [25].
- Escalation and planned outage procedures as described in several ITU-T M-series recommendations [29], [30] and [31].
- The procedures and scenarios described in various EURESCOM projects and Standards documents relating to various ATM VP Alarm Management specifications [8], [10].

When deploying a manual interface the requirement may be based on:

The maintain and repair procedures, as documented in annex A (derived from the JAMES project).

9.3.1.3 Interoperability requirements

These requirements should be accomplished as follows:

- Manual X.easi interface processes should be based on the procedures elaborated in annex A.
- Automated X.easi interfaces for the exchange of alarm information should conform to all the mandatory requirements in [10].
- Verification of (automated) interoperability for failed VPs should be achieved using the specification and Abstract Test Suite in [8], or appropriate profile from this (noting that this is not a Standard).
- Automated X.easi interfaces for trouble ticketing should conform to all the mandatory requirements of EURESCOM P612, Deliverable 2 [9] (noting that this is not a Standard). Verification of interoperability for the trouble ticketing should be achieved using the Abstract Test Suite, also provided in EURESCOM P612, Deliverable 2 [9].

9.4 Performance and QoS processes

9.4.1 General requirements

In general, it is unlikely that automated performance management procedures for X.easi interfaces can be specified for Phase 1. However, some agreement on performance monitoring of services supported as part of the interconnect service operation processes should be agreed. Exchange of performance information between operators should therefore be expected to be achieved using a manual X.easi interface function in Phase 1. Bi-lateral agreements to support this should therefore be implemented.

Further discussion of the performance monitoring and management-related issues, to be considered in relation to Phase 1 ATM service introduction, is provided in annex H, in which both manual and automated X.easi interfaces are considered.

9.5 Accounting and billing processes

9.5.1 General requirements

Firstly, so far as the interconnect service operation process for accounting management is concerned, it needs to be made completely clear that the present document is not suggesting any common or prescriptive method for inter-operator ATM services charging or levels of charging. Indeed, the objective is just to provide indications of reasonable processes for exchanging service-usage accounting data between operators. Operators must consequently decide, on a competitive and business basis, how much to charge their end-users and interconnected ATM network providers.

Operators would generally seek payment for the use of their ATM network resources, irrespective of whether such use is as an originating, transit or terminating connectivity provider. For the Phase 1 specification, charging of end-users or other interconnected operators for provision of resources should use a flat rate system based on service definitions and parameters. (Usage-sensitive accounting methodologies should only be considered for the Phase 2 specification [35].) The exchange of associated management information should then be undertaken using a manual procedure as it would mostly be non time-critical. Some or all of the following ATM traffic parameters should be used to establish the basis for the "flat rate" accounting:

- Service class
- Quality of Service, including traffic parameters such as:
  - Minimum cell rate (MCR)

- Peak cell rate (PCR)
- Sustainable cell rate (SCR)
- Maximum burst size (MBR)
- Bandwidth
- Distance
- Duration
- Date and Time of Day

Accordingly, for the Phase 1 specification the following statement should be applicable:

"Operators shall ensure that bilateral agreements are in place for flat-rate accounting for Phase 1 service introduction. The basis of the agreements may vary according to the services and Quality of Service offered"

In order to minimize management overheads, operators should consider using the "Chargeable Cell Rate" (CCR) concept, which has been advocated by the ITU-T [35] to provide a pragmatic approximation for accounting, based on the parameters listed in the above bullets. A further description of the use of the CCR concept for inter-operator accounting and charging processes is provided in annex I. Some comments on the potential use of usage-based accounting are provided in annex N.

9.5.2 Specifications for processes and interfaces

ITU-T Recommendation D.224 [35] (or any subsequent authorized standard derived from this) for general charging and accounting principles for ATM, including the CCR simplification.

The accounting and settlement principles on which many currently available "traditional" interconnected telecommunications services, such as ISDN, frame-relay or X.25, are based are derived from a number of ITU-T "D-series" Recommendations. A superficial précis of these Recommendations is given in annex J in order to provide background and precedent for accounting processes.

9.5.3 Interoperability requirements

Manual X.easi interface processes for the exchange of accounting and charging information should be developed for semi-permanent PVP/PVC services in Phase 1. These should be based on use of service definitions and parameters and the ideas elaborated in [36]. (There would seem to be a requirement to develop an automated usage-based measuring and inter-operator accounting scheme in the event that SVCs are specified and implemented in Phase 1.)

9.6 Security processes

9.6.1 General requirements

Firstly, it is appropriate to acknowledge that many of the security requirements and proposed solutions discussed in subclause 9.6 and the associated annex D, have been provided from research conducted by the EURESCOM P710 [36] project.

For Phase 1 there is a presumption that the ATM interconnect services and processes will be supported by a mixture or choice of "manual" or "automated" inter-operator interfaces (refer to figure 8). Processes other than the interconnect service operation processes would usually be manual. The interconnect service operation processes may be specified with automated or manual processes or a mixture of such processes (refer to table 6). There is a presumption of deployment of more automated interface processes in support of a migration towards the prospective Phase 2 solution.

The use of manual or automated processes for the X.easi interface introduces the risk that information and resources will be compromised, lost or misused. The various management procedures described elsewhere in clause 9 are subject to differing types of threats and risks. The basis issues concerning manual and automated X.easi interfaces are discussed below:

X.easi manual interface requirements:

The general security requirements for a manual interface, which might typically be based fax communications between operators, are comparably moderate. Human involvement in any action resulting from such fax based communication will always be necessary. It should be presumed that cross-checks on signatures and follow-up telephone calls will take place on the slightest indication of any irregular or malicious communication involving any of the inter-operator processes detailed elsewhere in the present document. Manual procedures should be documented to deal with such situations which should include access control and authentication rules.

An alternative manual interface using Telex rather than fax communications could be a possibility as Telex machines usually have additional security resources built into the machine operation.

X.easi automated interface requirements

The most general and important requirement is that no X.easi automated interface between interconnected operators should be deployed without an adequate security specification and validation.

There is a requirement that automation of the X.easi interface would be expected to be based on operator's using interconnected computer platforms which support TMN applications and processes (refer to subclause 5.6 and annex F). Platform interconnection would need to be accomplished using a "Data Communications Network (DCN)". Typical technology for the DCN could be X.25 or ISDN based. It is the DCN, the TMN platforms and associated software applications which require adequate security solutions for all automated processes required to support ATM-based services provided by a multi-operator environment.

There is a requirement that the security policies associated with TMN platforms and the applications which they support, need to be addressed according to the requirements of each platform owner individually. The present document is mostly concerned with addressing the inter-operator DCN which, of course, is the technical basis for the automated interconnect service operation processes.

Table 7 summarizes the overall security service requirements which appear to be applicable for automated X.easi interface management processes. P710 developed the requirements from a risk analysis based on Configuration, Fault, Performance and Accounting management services which form the greater part of the ISO processes described elsewhere in clause 9.

Table 7: Security Service Requirements for ATM management

X.easi interface Security Services	Requirement Level	Comment
Peer-to-peer Authentication	High	Mutual authentication at the granularity of individual application or application entities is required.
Access Control at association establishment (*Only incoming access control is addressed*)	High	Access Control List scheme based on authenticated calling entity is preferred. Only incoming access control is addressed.
Access Control for requested management operations (*Only incoming access control is addressed*)	High	Access Control List scheme with supporting target granularity at the level of individual Managed Objects. Only incoming access control is addressed.
Access Control for notifications (*Only incoming access control is addressed*)	Low	Notifications should be accepted as long as they come from a known authenticated party.
Data Origin Authentication	Medium	The purpose of this service is to ensure prolonged authenticity of the communicating applications after association establishment has taken place. A full integrity service at application level will suite the same purpose.
Data Integrity Protection	High	
Data Confidentiality Protection	High	
Non-repudiation with proof of origin	Medium	Refer to the discussion in annex D.
Non-repudiation with proof of delivery	Medium/High	Refer to the discussion in annex D.

In table 7, "Access Control" and "association" refer to the inter-operation, via the DCN, of the TMN management platforms and their associated software applications. Other terms should be self-explanatory.

In addition to the X.easi interface security services listed in table 7, it is considered a requirement that local security services such as Security Audit Logging and optionally Security Alarm Reporting should be part of any automated inter-operator security system suitable for management of ATM-based services.

9.6.2 Proposed specifications for procedures and interfaces

An X.25 based data communications network (DCN) should be deployed between network management platforms supporting automated X.easi interface processes. No solution is proposed on the basis of an alternative DCN, such as TCP/IP although there is a presumption of possible migration to TCP/IP communication for Phase 2. The X.25 DCN should be used as a "closed user group" (CUG) with confidential exchange of X.25 addresses by non-electronic means, as the minimum level of security for Phase 1. The exchange and availability of operators' X.25 addresses should be undertaken within the Interconnect Service Administration Processes. Refer to subclause 8.4.3 and table 5.

In general, further Security Management specification work currently under development is discussed in [37].

9.6.3 Interoperability requirements

Specifications for Security Management, which might be appropriate for the X.easi interface, are mostly untested for commercial-strength effectiveness and interoperability in Europe at present, although EURESCOM P708 has undertaken some laboratory-based Security testing [38].

The minimum deployment and interoperability requirements identified are:

> Automated interoperable X.easi interfaces shall not be introduced unless "fit for purpose" security mechanisms are agreed, in place and validated.
>
> The choice of data communications network (e.g. X.25) will affect the design and solutions for all aspects of an automated X.easi interface.

This completes the description of the interconnect service operation processes and the X.easi interface.

10 Management data model for supporting inter-operator processes

10.1 Introduction to the data model

A "data model" is required in order to provide an ordered view of what resources the management system operates on and to provide a basis for encoding automated operations undertaken by that system on the resources being managed.

The "automated" interface specifications (for CM, FM management of ATM VPs etc.), described in clause 9, are based on the presumed use of a CMIP and GDMO based implementation, but that the principles could be applied to the use of other interface technologies.

There is a clear requirement to assemble and define the terms associated with the provision and management of ATM services which require operator interconnect processes, to identify resources and to correlate these with formal abstractions. This is subject of annex C of the present document. In annex C the data model of the management of PVPs is extended to support the management of PVCs. It should be notified however that the current standard for configuration management [6] only covers PVPs.

The scope clause 10 is the management view for ATM PVPs and PVCs with the required resources associated with a GDMO based object model which is traceable to established standards [4], [22]. It must be presumed that the principles can be extended to interface specifications based on non-GDMO descriptions, but that explicit development of solutions for these circumstances remain for further studies.

10.2 Object Classes

The data model for automated management of ATM VPs is described in a set of (managed) object classes defined in the base standard for configuration management [6] and in proposals for enhancements from annex C. These object classes are listed in the following 5 bullets and described in more detail in annex C:

- pnoVpSubnetwork;
- pnoVpSubnetworkConnection;
- pnoNWAtmAccessPoint;
- pnoVpCTP;
- interPnoTopologicalSubnetworkPair.

The next additional object classes are proposed in annex C for enhancement of [6]. No reference to a standard is currently available for this work. Refer to annex C for definitions and details**.**

- pnoVcSubnetwork;
- pnoVcSubnetworkConnection;
- pnoVpLinkConnection;
- pnoVCCTP;
- PnoVPTTP.

The first five object classes in the above lists are also utilized in the associated standard for ATM VP alarm management [10] and are traceable to [20].

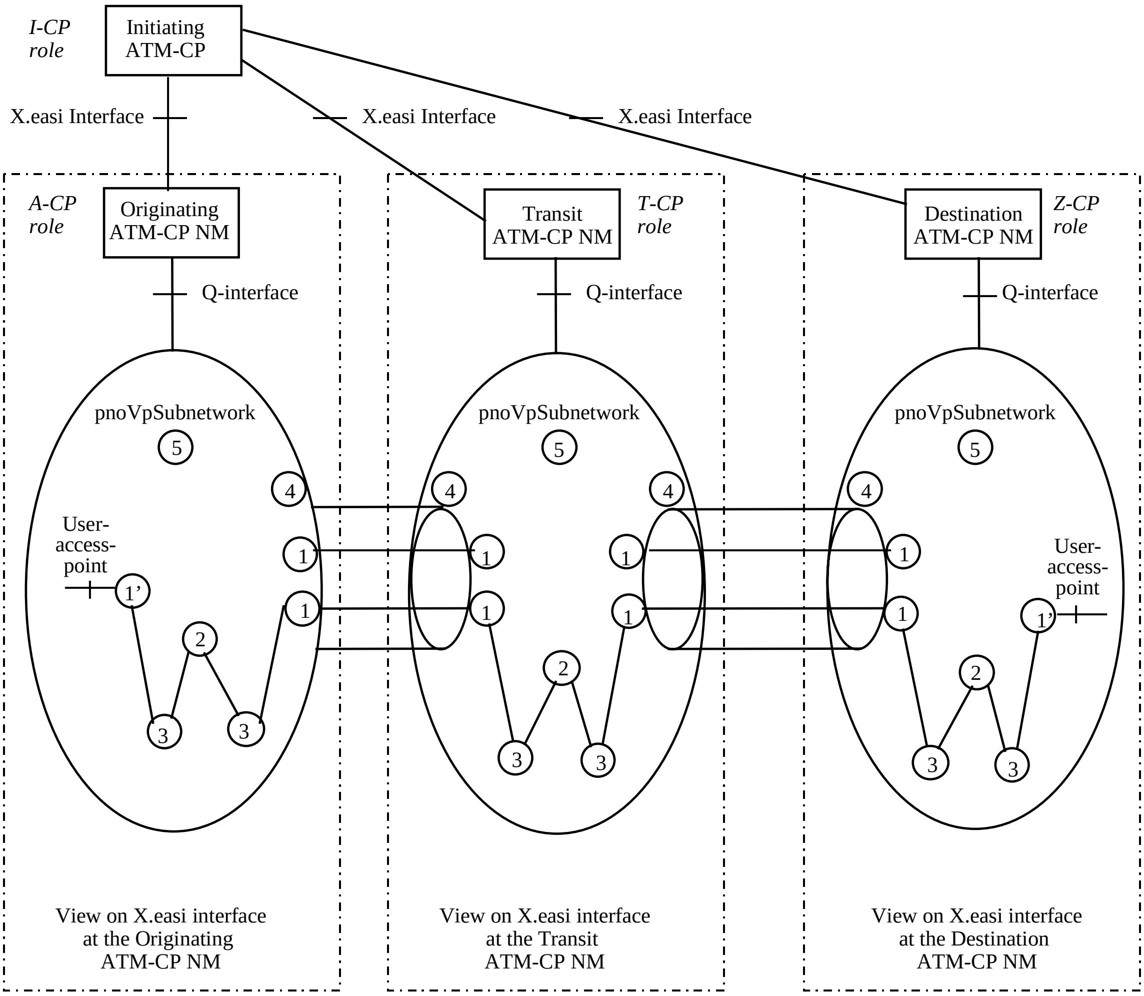
Annex C provides short descriptions of each of the object classes (noting that "PNO" is used instead of "ATM-CP", in order to align with the registered managed object definitions relating to [6] and [10], which provide a more detailed description of the data model).

10.3 Management view of object classes and ATM layer resources

The Management view on ATM layer resources deployed can be visualized by reference to figures 10, 11, 12 and 13. These figures help to clarify the mapping of the ATM connection types to the object classes necessary for automated management of interconnected ATM VP services.

10.3.1 Example of a VP User-to-user Connection Set-up

Figure 10 is an adaptation from a similar figure in [6] showing the management view after a User-to-user VP connection has been set up.



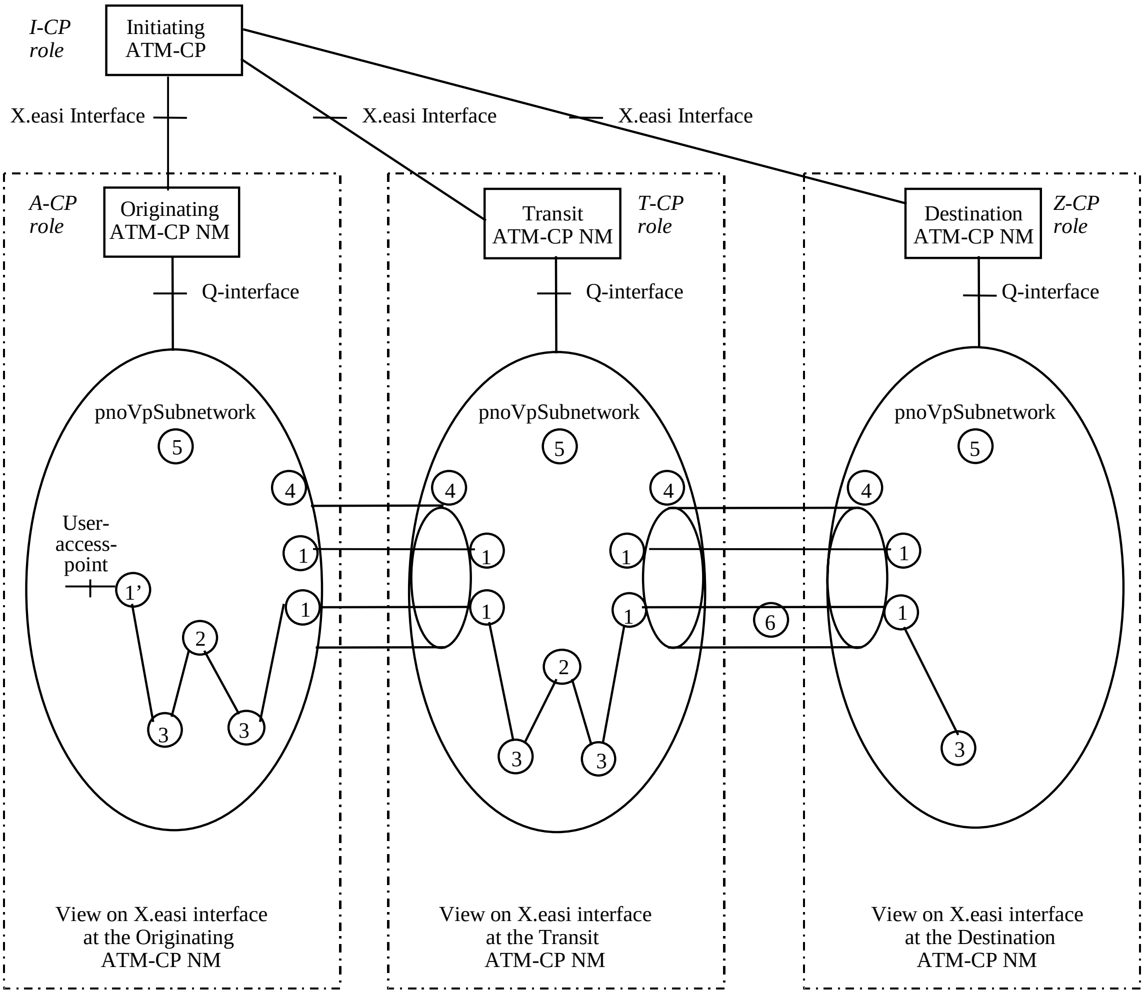
Legend:
1' pnoNWAtmAccessPoint for user access (no association with (4))
1: pnoNWAtmAccessPoint
2: pnoVpSubnetworkConnection
3: pnoVPCTP (VP Connection Termination Point)
4: interPnoTopologicalSubnetworkPair
5: pnoVpSubnetwork
ATM-CP: ATM Connectivity Provider
NM: Network Management
I, A, T, Z role: Initiating, Originating, Transit, Destination connectivity provider role

Figure 10: Management view of resources after a User-to-user VP set-up

Figure 10 shows the *I-CP's* view on the managed object classes described in annex C, in relation to the overall VP connection and the roles of the CPs. This figure includes a view of the connections to the user (customer) access points. In this example, only one transit ATM-CP is depicted but there could be several interconnected for a particular VP reservation. The adaptation from [6] provides alignment with the business model roles (figure 5), including the separated *I-CP* and *A-CP* NM roles and the X-interface re-designated as the X.easi interface. The user access points, shown attached to (1') are a representation of the UNIs and generally out of scope of the present document.

10.3.2 Example of a VP User-to-network Connection Set-up

Figure 11 is an example showing the management view after a User-to-user VP connection has been set up.



Legend:

1' pnoNWAtmAccessPoint for user access (no association with (4))

1:	pnoNWAtmAccessPoint	2:	pnoVpSubnetworkConnection
3:	pnoVPCTP (VP Connection Termination Point)	4:	interPnoTopologicalSubnetworkPair
5:	pnoVpSubnetwork	6:	VpLinkConnection

NM: Network Management ATM-CP: ATM Connectivity Provider

I, A, T, Z role: Initiating, Originating, Transit, Destination connectivity provider role

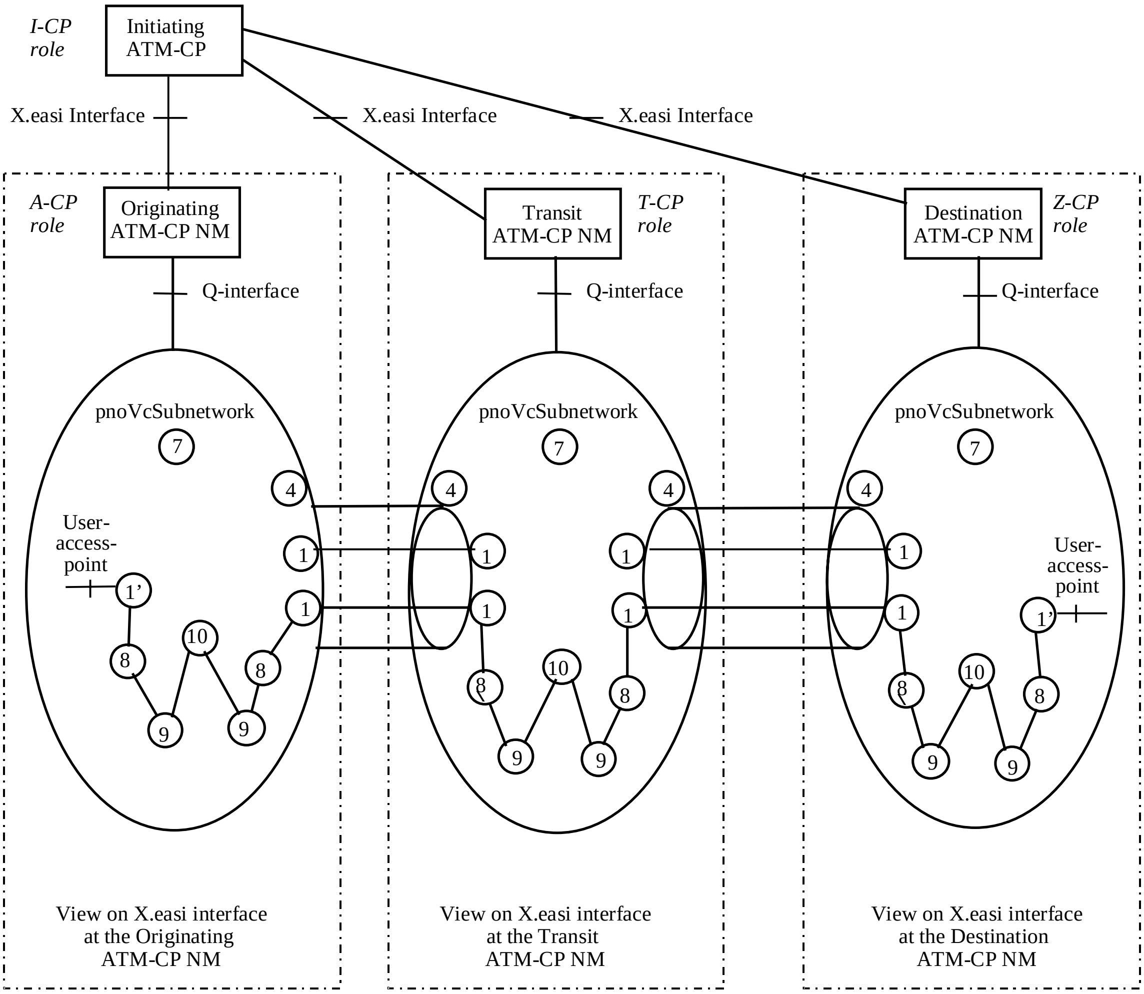
Figure 11: Management view of resources after a User-to-network VP set-up

For figure 11 the same general remarks apply as for figure 10. The difference with figure 10 is that the "network side" of the overall connection terminates at the ATM interconnection gateway (pnoNWAtmAccessPoint) in the Destination CP's subnetwork.

The occupation of the *Inter-Pno Physical Link* between *T-CP* and *Z-CP* is accounted for by pnoVpLinkConnection at the Destination ATM-CP NM and by pnoVpSubnetworkConnection at the Transit ATM-CP NM.

10.3.3 Example of VC User-to-user Connection Set-up

Figure 12 is an example showing the management view after a User-to-user VC connection has been set up.



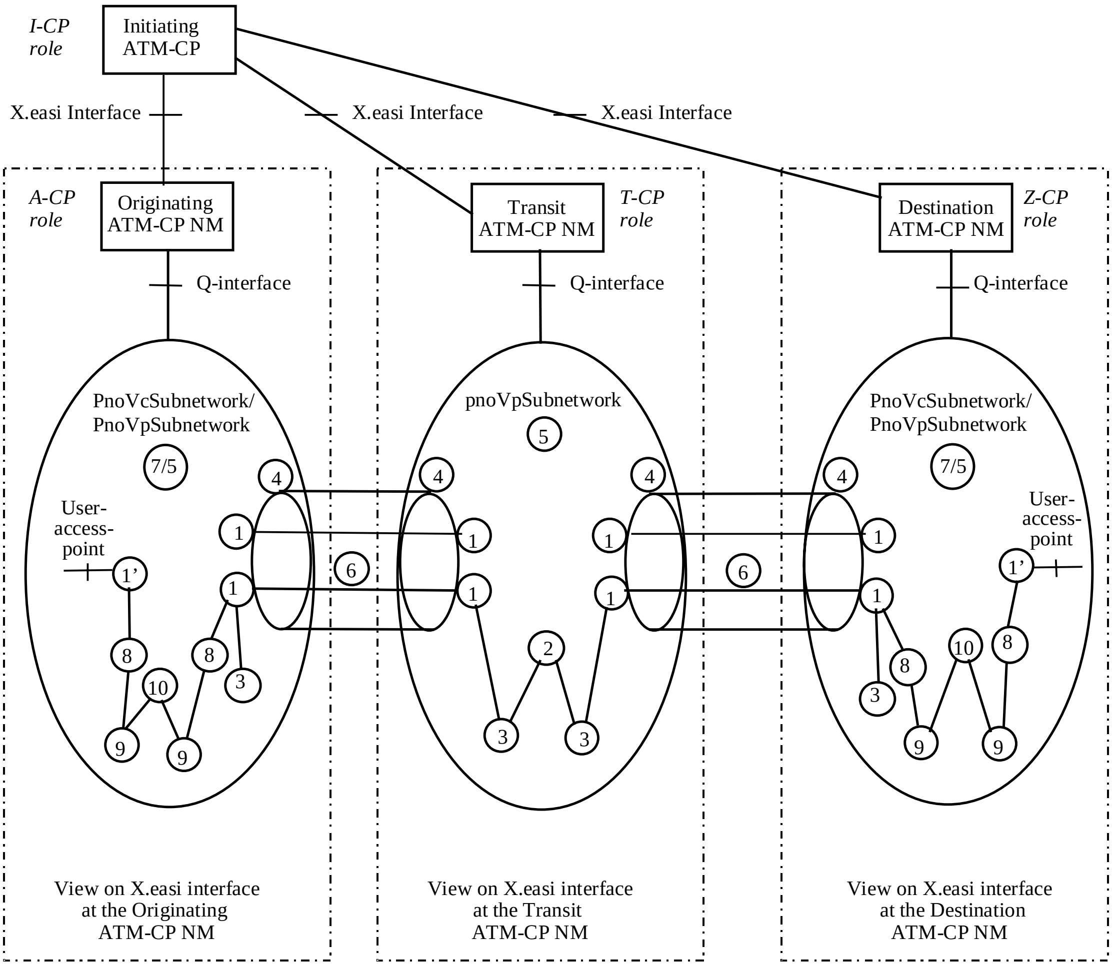
Legend:
1' pnoNWAtmAccessPoint for user access (no association with (4))
1: pnoNWAtmAccessPoint
4: interPnoTopologicalSubnetworkPair
7: pnoVcSubnetwork
8: pnoVPTTP (VP Trail Termination Point)
9: pnoVCCTP (VC Connection Termination Point)
10: pnoVcSubnetworkConnection
NM: Network Management
ATM-CP: ATM Connectivity Provider
I, A, T, Z role: Initiating, Originating, Transit, Destination connectivity provider role

Figure 12: Management view of resources after a User-to-user VC set-up

Figure 12 is essentially the same as for the VP example (figure 10) and shows the management view for the *I-CP* after a VC (User-to-user) connection has been set up. In this particular case, the Vp Link Connections that are used to carry the overall VCC across the links are not made visible over the management interface. The VPTTPs are significant for the X.easi interface because they provide the VPI-values that are used for the Vp Link Connections.

10.3.4 Example of VC User-to-user Connection Set-up using a Network-to-network VPC.

Figure 13 is an example showing the management view after a User-to-user VC connection has been set up.



Legend:

1' pnoNWAtmAccessPoint for user access (no association with (4))

1:	pnoNWAtmAccessPoint	2:	pnoVpSubnetworkConnection
3:	pnoVPCTP (VP Connection Termination Point)	4:	interPnoTopologicalSubnetworkPair
5:	pnoVpSubnetwork	6:	VpLinkConnection
7:	pnoVcSubnetwork	8:	pnoVPTTP (Vp Trail Termination Point)
9:	pnoVCCTP (VC Connection Termination Point)	10:	pnoVcSubnetworkConnection
NM:	Network Management	ATM-CP:	ATM Connectivity Provider

I, A, T, Z role : Initiating, Originating, Transit, Destination connectivity provider role

Figure 13: Management view of resources after a User-to-user VC set-up using a network-to-network VPC

Figure 13 shows the management view for the *I-CP* after a VC (User-to-user) connection has been set up. In this particular case, the Vp Link Connections that are used to carry the overall VCC across the links are also visible over the X.easi interface.

10.3.5 Physical Resources and Object Classes

The attribute values transmitted within the object classes provide the details of parameters required by the *I-CP* in respect of any given VP and VC reservation.

In terms of relating the ATM layer network management object classes of the data model to the physical layer resources identified for the network specification defined in [1], the following is applicable:

The pnoNWAtmAccessPoints object classes, depicted at points labelled (1) in figures 10, 11, 12 and 13 map into the "ATM Gateway (switches)". The interPnoTopologicalSubnetworkPair, depicted at points labelled (4) maps onto the "ATM Transit network, including the NNI.easi interface".

The pnoVpSubnetworkConnection, pnoVPTCP and pnoVpSubnetwork object classes depicted at points (2), (3) and (5) in figures 10, 11, 12 and 13 map onto the individual "ATM networks", in this case for the provision of VP connections,

The pnoVcSubnetworkConnection, pnoVCTCP and pnoVcSubnetwork object classes depicted at points (7), (9) and (10) in figures 10, 11, 12 and 13 map onto the individual "ATM networks" in this case for the provision of VC connections.

However, from figure 13 it can be seen that the relationship between the VC Subnetwork and the VP Subnetwork is not clear. It is assumed they are owned by the same Connectivity Provider as an administrative entity.

The object class pnoVPTTP does not map to a physical resource but reflects the point that the *I-CP* needs to know the VPI-value of the link connections that are used to carry User-to-user VCCs over the inter PNO links.

10.4 Example of operations that can be performed using the data model

An implementation of the data model, supporting the use of an automated X.easi management interface, should facilitate VP and VC configuration and ATM VP alarm reporting. As an example, in the functional area of configuration management (CM), figure 14 shows how messages [6] are exchanged between operators (acting as a manager-agent pair) providing ATM interconnection services and are used for several management functions supporting the following Management Services Components (MSC):

- (PVP, PVC) Establish MSC
- Destination user checking
- Check available cell rate (related to an action to adjacent ATM CPs to "Give Available Links")
- Reserve VP subnetwork connection
- Activate VP subnetwork connection
- Reserve VC subnetwork connection
- Activate VC subnetwork connection
- (PVP, PVC) Modification MSC
- Activate VP connection modifications (i.e. changes to the original reservation)
- Activate VC connection modifications (i.e. changes to the original reservation)
- (PVP, PVC) Release MSC
- Deactivate VP subnetwork connection
- Cancel VP subnetwork connection
- Deactivate VC subnetwork connection
- Cancel VC subnetwork connection

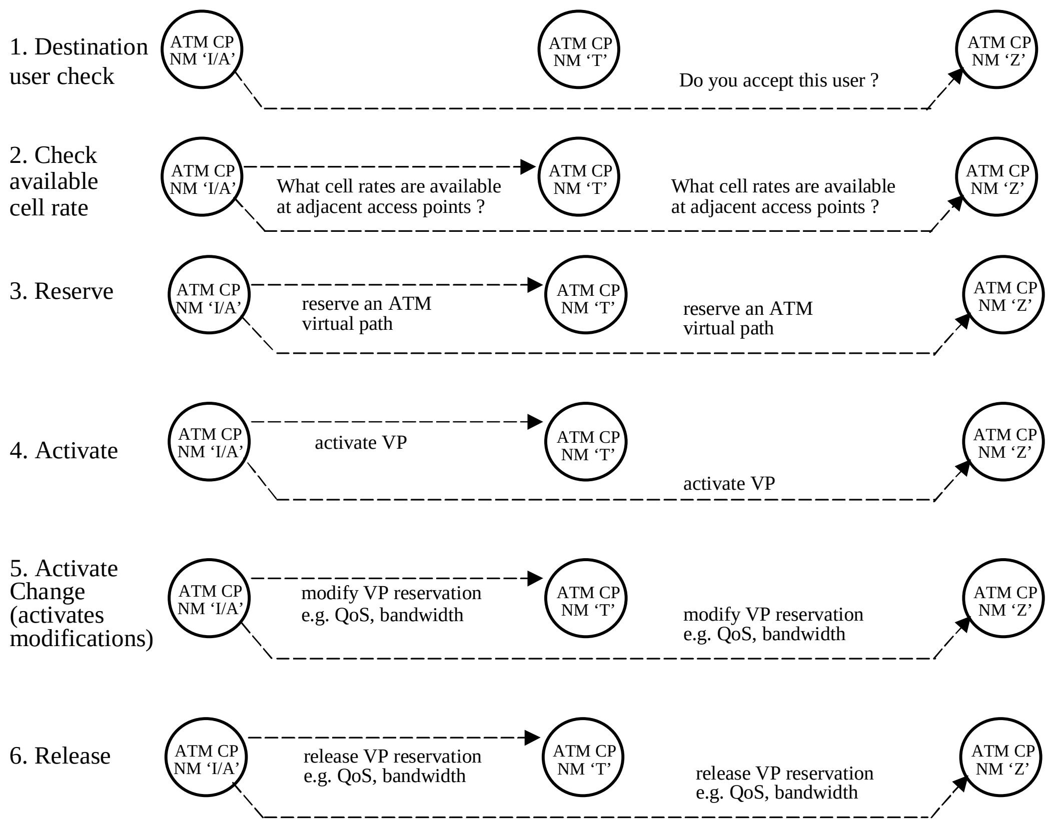


Figure 14: Examples of X.easi messages for management of an ATM VP

Figure 14 illustrates examples of management messages between I/A, T and Z CP's (roles as defined in the Business Model, clause 6) to undertake sequential actions relating to the management of a VP provided using resources belonging to three interconnected ATM CPs. (In this example the *I-CP* and *A-CP* are presumed to be the same organization.)

Figure 14 can easily be adapted for the management of VCs.

Table 8 shows the relationships between the management functions illustrated in figure 14, the CMISE services identified to transfer the management information between ATM CPs and the managed object classes/operations required for the data model. The latter are registered objects and defined in [6] but is not a duplication of the complete list.

Table 8: Summary of MFs, CMISE services, OC's and Operations

Functions	CMISE services	Object classes/Operations
Destination User Checking	M-ACTION	pnoVpSubnetwork/checkUser Action
Check Available Cell Rate	M-ACTION	pnoVpSubnetwork/giveAvailableLinks Action
Reserve VP Subnetwork Connection	M-ACTION	pnoVpSubnetwork/reservePnoVpSubnetworkConnection Action
Activate VP Subnetwork Connection	M-SET	pnoVpSubnetworkConnection/administrativeState Attribute
Activate Change	M-ACTION	pnoVpSubnetworkConnection/activateChange Action
Release VP Subnetwork Connection	M-ACTION	pnoVpSubnetwork/ releasePnoVpSubnetworkConnection Action

An analogous table could be provided for permanent VCCs.

11 Implementation and testing issues

11.1 Overview

Clause 11 considers implementation and testing issues for interconnected ATM services, based on the requirements and constraints of the business policy issues and also on the technologies that are possible. Most of the discussion in subclause 11.2 is concerned with "organizational models" for ATM interconnections assuming the use of the X.easi management interface. Subclauses 11.3 to 11.5 respectively provide brief reviews of Transport Protocols, Interoperability Testing and Interworking between automated and manual process solutions.

11.2 Implementation of the organizational model for operator management interconnections

11.2.1 Overview

Subclause 6.4 described business policy issues in relation to provision and management of interconnected ATM services. Subclause 6.4 also defined the requirement to manage ATM interconnections in accordance with the ETSI Star Model [6] and clarified the policy on the allowable extent of shared information between interconnected operators.

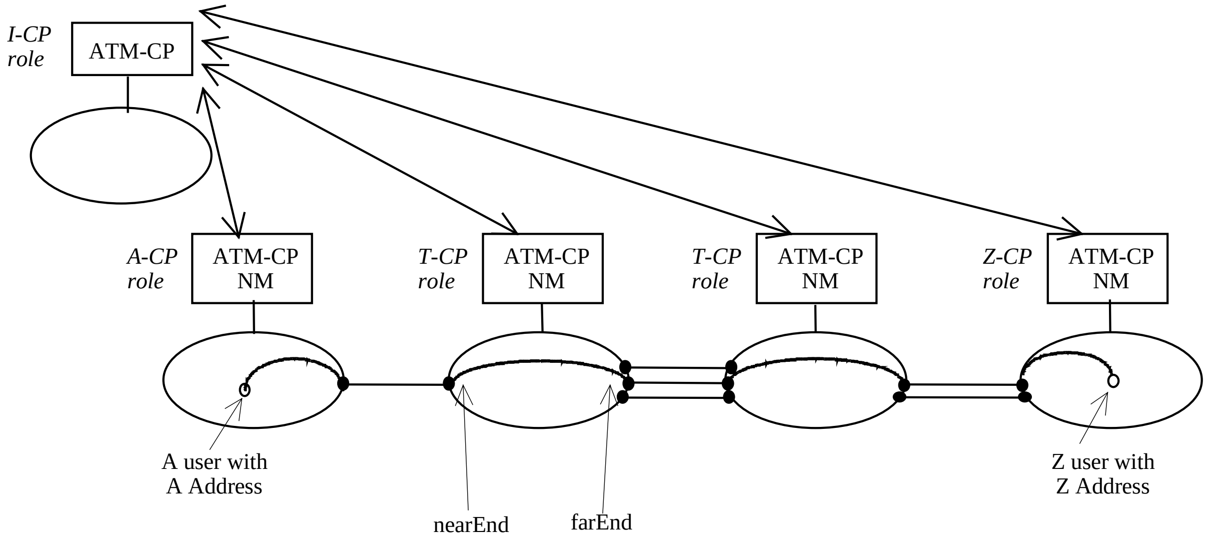
Whilst implementation of interconnected ATM networks and services should be undertaken in alignment with the business model, some differences may be unavoidable at the operational levels for the various ATM interconnect services (introduced in clause 7). An example is provided in subclause 11.2.6 where implementation of part of a subnetwork connection is delegated by a Transit role ATM-CP to a further set of interconnected ATM-CPs.

In subclauses 11.2.2 to 11.2.4, additional detail is provided on the recommended Star organizational model in comparison with the Cascade and Mixture models, which are not recommended for Phase 1 ATM service introduction.

An organizational model for ATM interconnect is essential to ensure that there is no ambiguity about how management tasks over inter-domain connections should be distributed among the operators involved in the connection. Issues included are the way that the connection reservation process is organized (configuration management) and the way operators are required handle the occurrence of faults (fault management). For any implemented interconnection model the management interface (X.easi) must provide the same level of "openness" to every participating operator.

11.2.2 Star Organization

The Star organizational model should be implemented for Phase 1 ATM interconnection service implementation and was introduced in subclause 6.4.2 and figure 6. Figure 6 is developed into figure 15 in order to illustrate the responsibility rules and processes. For figure 15, the Business Model role names are used in place of the equivalent operator names.



Refer to Figure 4 for Legend definitions

Figure 15: Recommended "Star" organizational model

Figure 15 summarizes the recommendation for implementation of interconnection of management systems to support ATM service introduction in Phase 1. The ATM-CP in the *I-CP role* (which may or may not be the same operator as that in the *A-CP role*) has responsibility for management of the overall VP or VC connection. The star model is essentially a "one stop shop" model so far as the user (or customer) is concerned. In the example in figure 15, the *I-CP* role is provided by a facilities based operator but which is not providing network resources for the particular connection shown. Hereafter the "roles" shown in figure 15 are abbreviated to "*I-CP*", "*A-CP*" etc.

In general, implementation has to take account of the following scenario:

> User A has requested operator *I-CP* to set up a connection to user Z.
>
> Towards the "A user", the operator *I-CP* has the responsibility for the overall connection. To manage this particular connection, *I-CP* communicates with operator *A-CP* and with each other involved network operator directly (in this example *T-CP*, *T'-CP* and *Z-CP*).
>
> For connections towards operator *A-CP*, *T-CP* manages and is responsible for the connection inside the *T-CP* domain, *T'* manages and is responsible for the connection inside the *T'-CP* domain and *Z* manages and is responsible for the connection inside the *Z-CP* domain. All operators *A-CP*, *T-CP*, *T'-CP* and *Z-CP* respond to and are responsible to operator *I-CP*, using the X.easi interface, during and after any VP or VC reservation request and until the reservation is released (i.e. the ATM interconnection service is completed).
>
> Responsibility for management of the physical links between operator's subnetwork domains is an open issue. In general, such links may be owned and managed on a bi-lateral basis although capacity may be leased to third parties (i.e. other ATM-CPs). Alarm reports or trouble tickets for failed links should be broadcast on the X.easi interface from the first management system to which the information is available. In the event of an unrecoverable network resource failure, the *I-CP* (in the Star model) always has the responsibility to ensure delivery of customer services and may choose to wait for recovery of the failure or reconfigure the entire ATM service, for example.

11.2.3 Cascade organization

The Cascade organizational model is depicted in figure 16. As this organizational model is not recommended for Phase 1 ATM service introduction, the "roles" may not be fully aligned, from an operational point of view, with those defined in the business model (figure 5). However, for simplicity, the generic roles of *A-CP*, *T-CP, Z-CP* and ATM-CP NM are retained in figure 16 in order to provide a direct comparison with the recommended Star organizational model.

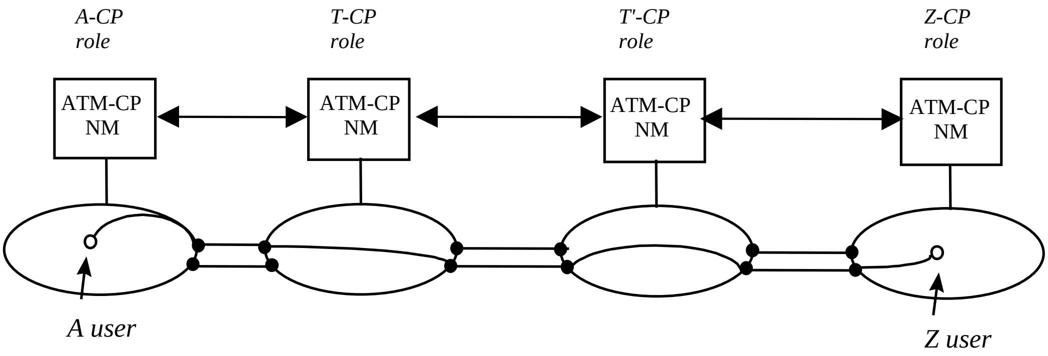


Figure 16: Non-Recommended "Cascade" organizational model

The cascade organization implies that the role of *I-CP* is not appropriate as this model depends only on interconnection of the management systems of adjacent operators acting in respective consumer and provider roles in support of the complete ATM service requirement. Although implementation of the cascade model for Phase 1 is not recommended, should such implementation be undertaken the following requirements are applicable:

> In the example shown in figure 16, the *A user* has requested operator *A-CP* to set up a connection to the *Z user*.
>
> Towards the *A user*, operator *A-CP* has the responsibility for the entire connection.
>
> To manage this particular connection, *A-CP* communicates with network-operator *T-CP* directly, and *T-CP* communicates with *T'-CP* which in turn communicates with *Z-CP* (and vice-versa up and down the management communication chain). In all cases the service requirements must be communicated on a bilateral basis for each inter-PNO part of the connection.
>
> There can be several interconnected "transit" operators *T-CP (e.g. T, T', T'')* in the cascade connection but the principle remains unchanged. That means there is no direct information exchange between *A-CP* and *Z-CP*. In each step of the "cascade", the upstream operator acts in the consumer role to the operator immediately downstream which is acting in the provider role, taking the logical sequence from *A-CP* to *Z-CP* shown in figure 16.

11.2.4 Mixture organization

The "Mixture" organizational model is a variable arrangement of star and cascaded models, in which operator's roles are adjusted according to the requirements for managing any given connection. As the "Mixture" organizational model is not recommended for Phase 1 ATM service introduction, the "roles" may not be fully aligned, from an operational point of view, with those defined in the business model (figure 5). However, for simplicity, the generic roles of *A-CP*, *T-CP*, *Z-CP* and ATM-CP NM are retained in order to provide a direct comparison with the recommended Star organizational model. (The mixture organizational model should be considered for a later phase ATM interconnect service introduction.)

An example of management of a connection, using the Mixture organizational model is shown in figure 17.

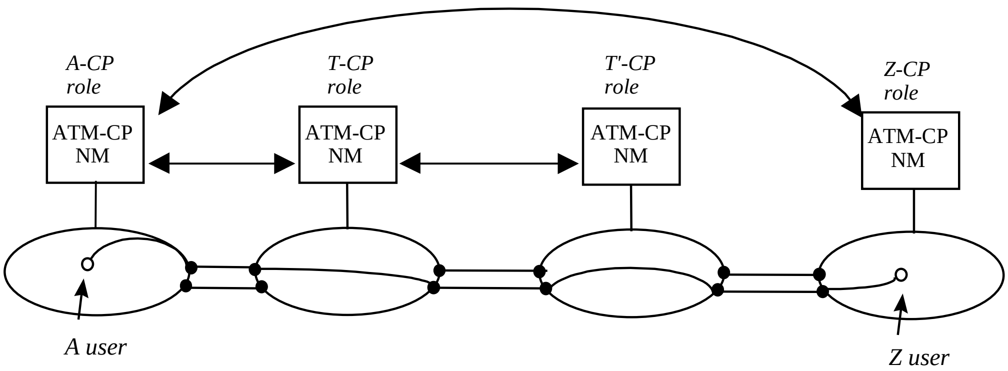


Figure 17: Non-Recommended "Mixture" organizational model

The mixture organizational model implies that the role of *I-CP* is optional. In figure 17, the *I-CP* role is not explicitly shown but may be taken as an example of the situation where the *I-CP* and *A-CP* are the same organization. All the roles shown are providing part of the ATM connectivity resources to support the connection in this example. The value and attraction of implementation of the mixture model is that it combines the benefits of the "one stop shop" approach for the ATM user with a flexible interconnection architecture for interconnected operators wishing to offer rapid ATM service creation and management.

In general, implementation of the mixture model for Phase 1 is not recommended as there is no empirical experience of its use in terms of the automated X.easi management platforms which would almost certainly be required to support it. However, should such implementation be undertaken the following requirements are applicable:

When the A-user has requested the *A-CP* to set up a connection to the Z-user:

- Towards the A-user, the *A-CP* has the responsibility for the entire connection.
- To manage this particular connection, the *A-CP* communicates with the *T-CP* and *Z-CP* directly and the *T-CP* communicates with the *T'-CP*. That means there is no direct information exchange between the *A-CP* and *T'-CP*.
- Towards the *A-CP*, the *T-CP* manages, and is responsible for the connection inside the *T-CP* subnetwork and on the link from the *T'-CP* subnetwork and associated access points.
- Towards the *A-CP*, the *Z-CP* manages, and is responsible for the connection inside the *Z-CP* subnetwork and associated access points.
- Towards the *T-CP*, the *T'-CP* is responsible for the connection inside *T'CP's* subnetwork and associated access points.
- Towards the *T'-CP*, the *Z-CP* is responsible for the connection to the *T'-CP* and associated access points.

In all cases listed above, the responsibilities for the access points may be a shared responsibility between bi-laterally connected operators rather than an individual operator responsibility, but that is a matter for negotiation as part of the interconnect service establish processes (see figure 8).

11.2.5 Advantages and disadvantages of the various organizational models

Having introduced the requirements for the various organizational models identified as recommended or not recommended for Phase 1 ATM service introduction, it is appropriate to provide more detail on the relative advantages and disadvantages of the models. Subclause 11.2.5 aims to provide further insight into the requirements for implementation of the appropriate form of the X.easi management interface.

In the text below, the Star and Cascaded organizational models are compared in detail.

Advantages of the Star model (refer to figure 15 and associated text):

Direct information exchange

The *I-CP* is directly involved with the requesting user and with each individual ATM-CP involved in providing the connection.

Alarm-, Performance- and Accounting messages are directly sent to the *I-CP*.

The ATM-CP who sends the information toward another ATM-CP is fully responsible for the transmitted data and will be identifiable. Consequently, the *I-CP* should be able to directly assign the incoming Performance and Accounting information to the ATM-CP involved.

Compared with the cascade model, the time for any ATM VP (or VC) alarm messages to arrive at the management system of the *I-CP* should be shorter.

Routing

Finding the optimal route for a connection is easier to accomplish for the *I-CP* because the overall topology of the DCN supporting the X.easi system and the related interconnected subnetworks and access points is known.

Security

Specifically in case of implementation of automated interfaces, an ATM-CP should be able to clearly identify the origin of management information, because of the direct association between the OSS systems of the interconnected ATM-CPs. It is possible to have peer entity authentication, data origin authentication, non-repudiation of origin, non-repudiation of delivery and confidentiality.

In addition, ATM-CPs can individually arrange bilateral agreements for additional security steps.

Experience

Since 1995, European experiments (including the ATM Pilot, EURESCOM P408 and P708 and JAMES) on implementation and testing of the Xcoop (equivalent to X.easi) interface, have all been based on the Star organizational model thereby providing considerable experience of its usage and operation.

Disadvantages of the Star model (refer to figure 15 and associated text):

Scalability

A drawback of the Star model is the need for topology management including the need for every operator to be aware of the existence and operational status of every physical link and access point for which it can arrange ATM connections. For a relatively small number of networks this situation is feasible, but it raises some concern about the scalability to large numbers. A reasonable figure for the allowed maximum number of Transit ATM-CP's involved in the configuration of an ATM VP or VC could be two (2) for initial working purposes. (I.e. no more than *I/A-CP + T-CP + T'-CP + Z -CP* supporting the connection.) Refer to annex L for further discussion.

Management connections

For any ATM-CP, management connections have to be made with every other ATM-CP for which an automated X.easi interface is required for efficient operation of the star model. Refer to annex L for further discussion.

Advantages of the Cascaded model (refer to figure 16 and associated text):

(Note that the generic term "operator" is used when describing the Cascaded model)

Scalability

It is expected that this model will be easily scaleable since, if the cascaded organizational model is applied in its conventional form, each operator needs only to be aware of links to neighbouring operator's networks. In this respect the principle of the cascaded model is similar to that of signalling technologies such as SS7, which support global telephony.

Management messages regarding links and access points only need to be sent to the "adjacent" operators.

Management connections

Management connections only have to be made to the adjacent operators' network management systems.

Disadvantages of the Cascaded model (Refer to figure 16 and associated text):

No direct information exchange

The initiator of the overall connection is not directly involved with each individual network operator. Alarm-, Performance- and Accounting messages are not directly sent to the initiator (other than by the next adjacent operator).

The initiator does not have the possibility to directly assign the incoming Performance or Accounting information to each network-operator involved.

Compared with the Star model, the time for the alarm messages to arrive at the initiator could be longer, because for every operator in a chain a connection has to be set up. The risks of lost or corrupted messages multiply as the length of the management chain supporting an ATM connection increases. In general, there is a good probability of taking longer times to create services for users, due to the chains of request and confirmatory messages which would be required, especially in the case of three or more operators involved in the service configuration.

Security

Because there is no direct association between initiator and each individual network operator it is difficult to achieve security services like: peer entity authentication, data origin authentication, non-repudiation of origin, non-repudiation of delivery and confidentiality.

Routing

The initiator, who does not have all topology data, has less possibility to set up an optimal route or to re-route the overall connection. It is not guaranteed that a protecting route [39] is set up via different subnetworks.

Business data

A cascaded approach gives every transit network operator (*T-CP*, *T'-CP* in the example provided by figure 16) full access to all information sent between *A-CP* and *Z-CP*. Therefore, *T-CP* and *T'-CP* get data describing user Z (e.g. usage of band-width, performance data etc.) which is business-relevant data that operators *A-CP* and *Z-CP* and their users may prefer not to make available to *T-CP* and *T'-CP*.

- Information model

It still has to be verified whether the existing X-interface (X.easi) information model defined in [6] is adequate to support the cascaded and mixed models, in particular with regard to performance and accounting management.

To adapt the existing model to the cascaded or mixed models, further work on the specification level is required, which would include the following tasks:

a change of procedures for configuration-, fault-, and performance-management describing the exact order in which the X-interface (X.easi) management functions should be employed (this could be illustrated through SDL diagrams, but would involve considerable development and testing effort).

Advantages and disadvantages of the Mixture organizational model:

The combined advantages and disadvantages of the Star and Cascaded models described above could be expected to be applicable for the situation of the Mixture organizational model, to a first approximation. No further analysis is provided here beyond this observation.

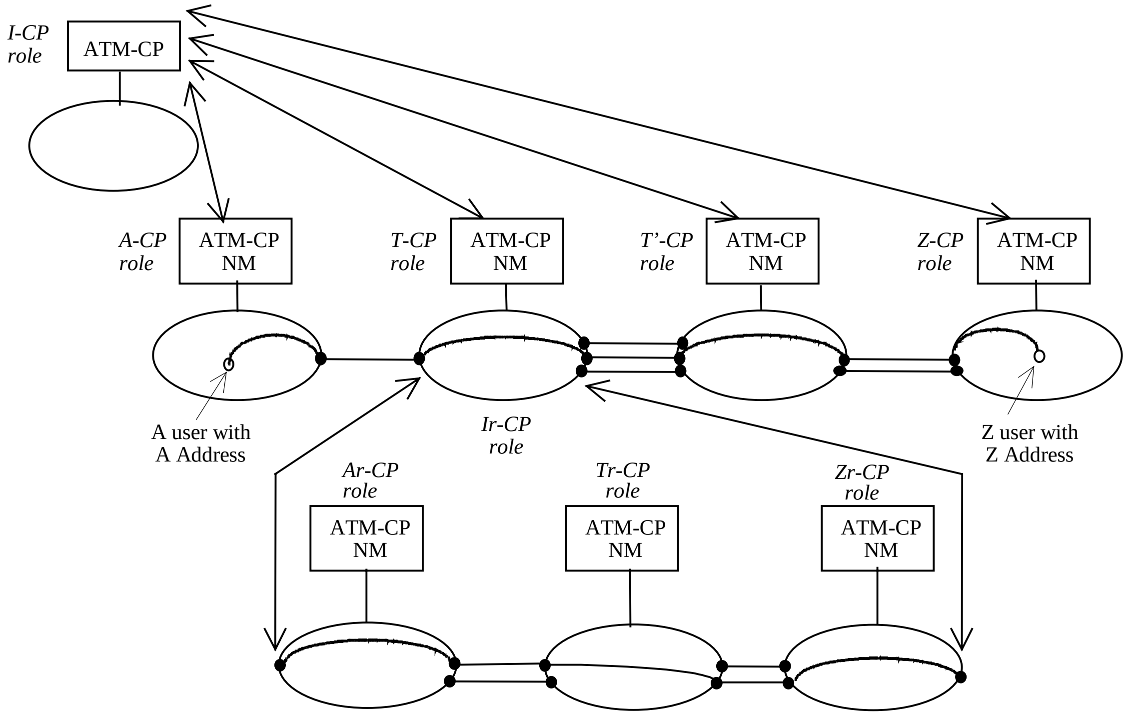
11.2.6 Relationship between the business model and possible organizational models

The following observations may be made on the relationship between the business model (clause 6) and the possible organizational models introduced above:

The business model defines business roles and indicates the choice of a particular organizational model - the Star model - to be recommended for use in operational deployment for Phase 1 implementation. In this respect the chosen organizational model should be considered as an "implementation issue", although the recommended restriction to use of the Star model provides a limit to the required Phase 1 specification definition whilst leaving the possibility to define alternative organizational models open for the Phase 2 specification.

The business model does not preclude recursive implementation or "nesting" of multiple use of the Star model. However, such use is almost indistinguishable from use of the Mixture model described in subclause 11.2.4 (except that the *I-CP* or I-PNO is optional for the Mixture model). The main issue for Phase 1 is scalability because additional ATM-CPs, however organized, would add complexity to the management requirements for ATM interconnect services.

However, if a nested Star model approach is implemented (for any particular ATM service), it would mean that any ATM-CP responsible for a portion (where this could be either the originating, transit or destination connection segment) of the end-to-end connection could delegate the implementation of this connection to several other ATM-CPs. For example, a Transit ATM-CP responsible for a transit subnetwork connection could delegate implementation of the connection to several other ATM-CP's, as depicted in figure 18. In this case the *T-CP* could act in the *Ir-CP* role towards the ATM-CPs acting in the *Ar-CP*, *Tr-CP* and *Zr-CP* roles (where "r" denotes the recursive role as indicated in figure 18).



Legend:
Ir-CP, Ar-CP, Tr-CP and Zr-CP denote recursive roles
Refer to Figure 6 for other Legend definitions

Figure 18: Recursive implementation of the business model

11.2.7 The inter-operator data communications network for automated interfaces

Subclause 11.2.7 considers the options for management communications between operators requiring automated X.easi interfaces to support all or part of Phase 1 service introduction.

Experience in previous European projects for which an Xcoop interface was developed, such as the ATM Pilot, P408, P708, P613, and JAMES, relied on the use of CMIP over X.25 for the exchange of management messages. The X.25 connections between the management platforms of operators in these projects formed the "data communications network" (DCN).

In principle, X.25 connections could form the basis for the DCN supporting the X.easi automated interface for Phase 1 ATM service introduction.

Alternatively, it should be noted that possibilities exist for implementation of automated X.easi interfaces to support ATM service introduction, which are not CMIP based. These may include CORBA or web-based (internet) protocol solutions etc. Any choice, however, will still require considerable software development effort in order to support the full range of inter-operator management functionality required for a comprehensive X.easi automated management interface.

Some observations concerning existing and alternative protocol solutions are provided as follows:

The basic need is to enable secure communication between, perhaps, thousands of partners, which may or may not have contractual relations at any given point in time. The layers of communication, which have been defined in the OSI-model also can be realized using a combination of different, recommended protocols. The main parts of communication would be:

- Transportation. The public Internet is already adequate in some parts of Europe for most management communications, apart from the inadequate security situation. However, if some operators have special communication needs or if the Internet is under-dimensioned, or as back-up, the following solutions (other than CMIP/X.25) can be used.
- Dial-in using ISDN. Availability in Europe is good but the number of simultaneous connections is limited. Support in routers is good.
- Frame relay. Frame relay is a fast growing service and provides a feasible alternative. Support in routers is good.
- ATM. This may be a good solution for high capacity links but vulnerable to the same failures as the managed connections. Support in routers is good.
- Security. IETF trade and AAA working groups are working on a common/compatible solution. This is expected to be adopted, when available. Security requirements must ensure that communication occurs between the intended parties only and prevent the leakage of information to other parties. Companies, which are in contractual relationships, may use shared secret-based security specifications but other companies must use the services of a trusted third party. Different security methods must not influence the priority or handling of connection requests and subsequent messages.

Information representation. The Communication Trade working group has adopted XML for inter-role communication. AAA has not yet defined the preferred model. The information representation in communication is independent from the presentation for realization. That means that the communication interface is the same for manual, semi-automatic and automatic implementation. Only the promised delivery time varies.

In conclusion, the above discussion covers a number of possibilities and options for provision of an inter-operator DCN. The only technology proven to support an automated management interface for the star organizational model is CMIP over X.25. Accordingly, for general deployment of automated management interfaces for a Phase 1 solution, based on the X.easi specification described in the present document, it seems necessary to make the following normative statement:

Where automated X.easi management interfaces are deployed, the preferred solution shall be based on the use of CMIP over an X.25 DCN linking interconnected operators wishing to provide and support Phase 1 ATM service introduction.

11.3 Transport protocols

11.3.1 Recommendation for the Phase 1 specification for transport protocols

The Phase 1 solution for an automated X.easi management interface should be based on the use of Management Function applications developed using GDMO with inter-operator communications accomplished using CMIP-based messages transported on an X.25 DCN.

11.3.2 Alternative solution for Phase 1 or for migration to Phase 2

Possibly for a Phase 1 solution or more probably as a proposed migration to a Phase 2 solution, consideration should be given to the use of CORBA or XML for the creation and interoperability of agent interfaces, both to the network technology and between the management systems of operators supporting ATM interconnection services.

In particular, the use of CORBA based interfaces would be based on the CORBA reference model which consists of the following four components [40]:

Object Request Broker

- which enables managed objects to transparently make and receive requests and responses in a distributed environment and is the foundation for building applications and interoperability between them in hetero- and homogeneous environments.

Object Services

- which is a collection of services that support basic functions for using and implementing objects and is necessary for the construction of any distributed application and is independent of application domains.

Common Facilities

- which is a collection of services that many applications may share but is not necessarily fundamental to the creation of applications which may be suitable for management interface development.

Application Objects

- which are products of a single vendor or in-house development group and are designed, for example, to manage or control interfaces.

In general, the object request broker is the core of a CORBA-based implementation and, simplistically, acts like a telephone exchange in providing the basic mechanism for making and receiving calls. When combined with Object Services, is should ensure the required communication between CORBA-compliant applications.

Beyond use of the four basic CORBA components listed above, use needs to be made of the specification for a General Inter-ORB Protocol (GIOP) for ORB interoperability [40] and therefore potentially related to implementation of interface applications of the X.easi type. The baseline transport specified for GIOP is TCP/IP. The associated mapping of GIOP message transfer to TCP/IP connections is called the Internet Inter-ORB Protocol (IIOP).

Substantially more detailed descriptions, specifications and methodologies for all CORBA-based application implementations is to be found in [40] and should be consulted in the event of bi-lateral agreements to use such methods for interface developments, for Phase 1 or any subsequent phase of ATM interconnect service introduction.

11.4 Interoperability testing (to support ATM interconnection services)

Guidance on interoperability testing for operators wishing to provide ATM interconnection services is provided in the "Operator's Handbook" [3].

11.5 Interworking between automated and manual process solutions

There is very little published operational experience to refer to in this area. The presumptions are:

Use of the Star management organizational model will be supported by some interconnecting operators by deployment of automated interface technology using the basis of specifications proposed in the present document. In subclause 9.1.3 and table 6, it has been stated that a manual (X.easi) interface shall be available in all cases with automation of some management functions as a recommended option. Altogether, there is little known experience of providing ATM interconnection services using varied mixes of automated and manual interfaces for some or all of the management functions involved.

The Operator's Handbook [3] should provide guidance in this area of interworking and a discussion is provided in annex G, which includes a description of some scenarios associated with this topic. For interconnected ATM service introduction in Phase 1, it will be necessary for operators to develop solutions and processes to cope with any situation of mixed use of automated and manual X.easi interfaces.

Refer also to the text in subclause 8.4.3 for basic requirements in the area of manual and automated interface administration.

12 Summary and conclusions

12.1 General conclusions for the Phase 1 NM guidelines

The present document has been prepared as detailed "Guidelines" to support practical use of TS 101 674-2 [2]. The present document and reference [2] relate to TS 101 674-1 [1] which specifies network to network interconnection at the user and control plane levels.

The main part of the present document is based on specifying a solution for all aspects of the management of ATM interconnect services defined in reference [1]. The solution has included development of a set of business model roles and an ATM interconnect services and processes model described in clauses 6, 7, 8 and 9. The non-technological aspects are considered as an essential basis for operators and other involved parties to offer interconnected ATM services to customers. With such aspects in place, use of a network management interface - "X.easi", is specified for configuration and related management functions required to provide and maintain ATM VP and VC services in and across interconnected network domains.

The X.easi interface specification is predicated on the use of CMIP and OSI standards, although the principles could be adapted to other technologies. Implementation of an automated X.easi interface is dependent on a data model and on organizational aspects of network interconnection and service management. These specific topics are described in significant detail in subclauses 10 and 11.

Several annexes are also provided as an integral part of the present document. In brief, these provide detailed discussion of:

- procedures for provisioning of PVP and PVC connections;
- proposals for management identifier schemes;
- proposals for extension of EN 300 820-1 [6] from PVP to PVC level;
- further details on security processes and methodologies for automated interfaces;
- further details on traffic and capacity management processes.

A set of informative annexes is also available which provides further non-essential information and discussion on management aspects for which the main part and annexes provide the basic specification.

12.2 Cross-reference to the Phase 2 NM guidelines

The results reported in the present document are intended to provide detailed guidelines for management of "Phase 1" ATM interconnected services introduction.

A subsequent phase 2 was envisaged, however this will not now be progressed.

Annex A (informative): Phase 1 ATM interconnect management procedures for Provisioning of PVP and PVC Connections and associated Maintain and Repair processes

A.1 Introduction

A.1.1 Preamble

This annex provides an initial proposal for the provisioning (configuration management), and maintenance and repair (fault management) of PVP and PVC connections which require management processes using X.easi interface functions within the ATM interconnect service operation processes.

The processes described in this annex are intended to relate to some of the network management requirements for resources identified in the ETSI EASI specification for the "User and Control Plane" [1]. The network management requirements may use or be mappable to the standard for Configuration Management [6] in its currently available form or in enhanced form (where planned enhancements are expected to provide resilience and performance monitoring functionalities but not change the basic PVP or PVC reservation processes).

The JAMES project also developed the processes described in the present document in SDL diagram format which, in turn, could be translated into OMT. However, this would involve a lot of work which has not been undertaken for the present document.

In this annex, the term "PNO" is used to mean any interconnected operator and is chosen to maintain consistency with the object nomenclature of registered Managed Objects and Attribute names in some of the relevant standards.

A.1.2 Scope and Purpose

A.1.2.1 Scope

This annex provides a set of processes that may be operated in Phase 1 between organizations wishing to deploy ATM interconnect service operation processes. Basically, the present document defines manual processes which need to be performed by operators supporting interconnection of ATM services. However, these processes may be supported by the use of automated X.easi interfaces between PNO's Operations Support Systems (although a requirement will remain to be able to undertake the processes manually if or where necessary).

There are some alternative processes described, and the selection of the appropriate processes depends upon the complexity of the connections which are established, and the extent to which the Operations Support Systems are optionally automated.

The material in this annex is based upon the experiences gained from:

- EURESCOM P407, P612 and P708 projects;
- the JAMES project;
- current practical bilateral processes operated between some European Telecommunications Network Operators (PNOs).

This annex outlines the management processes that may be used across the interfaces between PNOs for:

- ATM Permanent Virtual Path/Circuit Services;
- covering both Provisioning and Repair processes.

It describes the information flows that will be required between PNOs but does not endeavour to mandate within either PNO's organization (even though in the examples some indication of possible approaches is indicated). That information will be found within each PNO's internal documentation.

In terms of investment in automated (X.easi) management interfaces, the expected practical position is for most PNOs is to require automated interfaces for transit traffic. However, it should be noted that most of this annex is restricted to bilateral ordering processes which do not require transit PNO involvement although a description of fault handling involving a transit PNO is provided in subclause A.3.3.2.1.

Automation of interfaces to support other traffic management roles (such as initiating or terminating PNO) may be advantageous, if not necessary. Automation of various management functions, defined for the X.easi interface, may be installed in phases, whilst always maintaining a manual alternative.

The relationship between a PNO's internal process/processes and the proposed ATM interconnect service operation processes is shown in figure A.1.

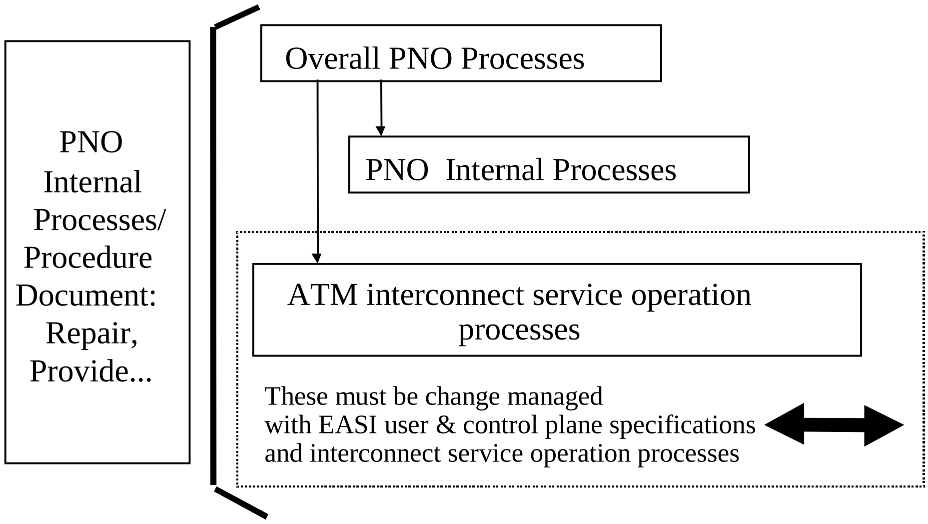


Figure A.1: Relationship between internal PNO Process/Procedures and ATM interconnect service operation processes

Each PNO will need internal documentation describing the processes for managing its ATM based network capabilities, which will cover overall processes tailored to the specific organization of each PNO, and the internal Operations Support Systems used. For the extension to interconnect service operation processes in the inter-operator environment this internal documentation will need to be appropriately updated.

NOTE: Earlier work has presumed that processes will be used solely for international operations. This annex uses the term "inter-operator" as it recognizes that the de-regulation in Europe and elsewhere leads to a situation where a single PNO may operate in several countries, and each country may have several operators.

A.1.2.2 Purpose

This annex provides the basic framework and description of the possible processes which may be used between Telecommunication Network Operators (PNO) requiring use of ATM service interconnect processes. A clear definition of the processes is an essential first step in understanding the business level relationships and information exchange i.e. "what" is to be done. It is an essential precursor to defining detailed automated/semi-automatic/manual interfaces since these define "how" the business level processes are implemented. Indeed, it is important to get agreement on exactly what has to be included in the specification of the ATM interconnect service operation processes and the related functionality of the X.easi management interface, in particular.

The advantage of documenting the processes is that it allows operational and managerial personnel to understand what is being agreed, including implied policies, without them needing to examine the details of the automated/semi-automatic/manual interfaces, which may require considerable technical knowledge and skill.

In developing the annex some alternative operational models (matched orders, one stop shopping, establishment of connections with or without transit operators) are identified. All of these processes can, in principle, be implemented using automated , semi- automated or manual X.easi interfaces. Some processes are complex and labour intensive to implement using a manual interface. PNOs may need to be careful in selecting manual interfaces for some normal operational processes since this may to avoid excessive implementation complexity. The selections made by each PNO are expected to be established and documented on a bilateral basis.

NOTE: It is assumed that all processes need to be operated across manual interfaces for back-up during OSS systems failures. The selection proposed here is purely to avoid excessive operational complexity during normal operational processes.

This annex is intended to be used to validate automated X.easi interfaces by:

- demonstrating that they are sufficiently complete to meet a range of expected operational agreements for the ATM interconnect service;
- identifying the supporting manual processes needed to achieve effective interconnect service operation.

In addition to this annex, PNOs will need to agree Operational Contact and Procedural Templates (OCPT) on a bilateral basis which cover specific issues such as contact points, escalation points, etc.

Within JAMES and other bilateral agreements it was necessary to identify the specific operational units within each PNO which carry out specific operational "roles". This annex identifies some of these roles, which can then be mapped through the completed OCPT Template onto the specific (but different) operational structure of each PNO.

A.2 Provisioning processes

ATM provisioning processes can take the form of:

Bilaterally provided connections involving solely a pair of PNOs. These are relatively simple and are suitable for implementation by manual processes.

Multi-laterally provided connections involving one or more transit operators. Because of the complexity of these processes it will be desirable to have management systems to automate these processes.

The first arrangement is likely to be the most commonly adopted approach initially as it can be readily implemented using manual processes and systems, or by automated/semi-automated systems.

Provisioning covers:

- an overview of the VP/VC reservation processes;
- bilateral (no transit) PVP and PVC Provision procedure;
- one stop shopping Multilateral Provisioning processes;
- regrade provisioning procedure;
- PVP PVC Provisioning order and regrade management escalations;
- detailed descriptions of Provisioning Procedures.

A.2.1 Provisioning - Overview VP/ VC Reservation Procedures

Subclause A.2.1 provides a basic description of the processes required for the provisioning of interconnected Virtual Path Connection (VPC) Bearer and Virtual Circuit Connection (VCC) services.

NOTE: Inter-operator Point to Multi-point Virtual Path Connections, are not included in Phase 1.

A.2.1.1 General

NOTE: In this subclause, taken from JAMES documentation, different terminology is used as compared to [6]. Specifically:

JAMES	EN 300 820-1 [6]
Access Logical Link	access point for a user
Inter-subnetwork Logical Link	interPnoTopological Subnetworkpair plus pair of pnoNWAtmAccessPoints for links between networks
Originating PNO	I-PNO
Destination PNO	Z-PNO

The network processes for setting-up a Virtual Path Connections (VPC) or a Virtual Circuit Connection (VCC) involving more than one PNO, require a number of message exchanges between the corresponding PNO's. These may use manual processes using communication methods, such as fax, or may be automated using TMN Management Systems and interfaces.

Initially, ATM interconnect service operation processes may be supported by a single inter-operator ATM Cross connect or switch (per operator), but large networks will need to:

- introduce more than one network gateway per operator for resilience and capacity reasons;
- introduce the concept of multiple ATM switches or cross connects per operator using a subnetwork concept.

A Subnetwork is therefore managed by a single Subnetwork Operator, having an unique Subnetwork Virtual Path and/or Virtual Circuit Operation Support System (OSS). These concepts are elaborated in subclause A.2.1.2.

A number of basic assumptions have been made in order to simplify the description of the Connection Procedures. They are summarized in subclause A.2.1.3.

Both the static items (Customer's interfaces, Subnetworks and inter-Subnetwork Logical Links) and the dynamic items (VPCs) should be unambiguously identified using identifier scheme(s) described in annex B.

A.2.1.2 Reference Configuration

Subclause A.2.1.2 describes firstly, the Virtual Path Connection reference configuration, and then the Virtual Channel Connection Reference Model which is similar.

Virtual Path Connections

The Reference Configuration for the provisioning of an inter-Subnetwork VPC is shown in figure A.2, which depicts the network elements and their connectivity. Local VPCs, i.e. established between Customer Equipment belonging to the same Subnetwork, are considered outside the scope of the ATM interconnect service operation definitions. The Data Communications Network (DCN) provides interconnection at the network management level and therefore provides the TMN basis for the X.easi interface between PNOs. Figure A.2 is not prescriptive about the functionality or implementation of the DCN. However, automated X.easi interfaces would require TMN management platforms to be able to interwork via the DCN using an agreed protocol (such as CMIP over X.25 or IP or ISDN) and complying to an agreed specification, generally based on OSI standards. Where manual interfaces are implemented, the DCN is likely to be a set of fax machines located at the premises of each interconnecting operator. In this case, the protocol and specification requirements for the interface are less stringent and management processes generally rely on the actions of trained personnel.

The Customer Equipment includes the ATM VPC endpoint. The Originating Customer Equipment is the one owned by the customer which initiates the VPC processes, whilst the Destination Customer Equipment is its counterpart in this point to point VPC.

The possibility of Subnetwork internal congestion during the establishment of a new VPC between two inter-Subnetwork Logical Links must be considered. However resolution of congestion is an internal matter for a PNO.

For a particular VPC, the Originating Subnetwork is defined as the one locally connected the Originating Customer Equipment. Similarly, the destination Subnetwork is defined as the one to which the Destination Customer Equipment is attached. The remainder of the Subnetworks involved in a given VPC are Transit subnetworks.

A maximum limit of two Transit Single Cross Connects is recommended for VPCs in the Phase 1 specification. This is similar to the routing constraints adopted in the ITU-T for conventional International Private leased circuits and some limit is needed in order to:

- ensure that end to end connections have a predictable QoS performance;
- minimize the complexity and volume of management messages to establish available routes.

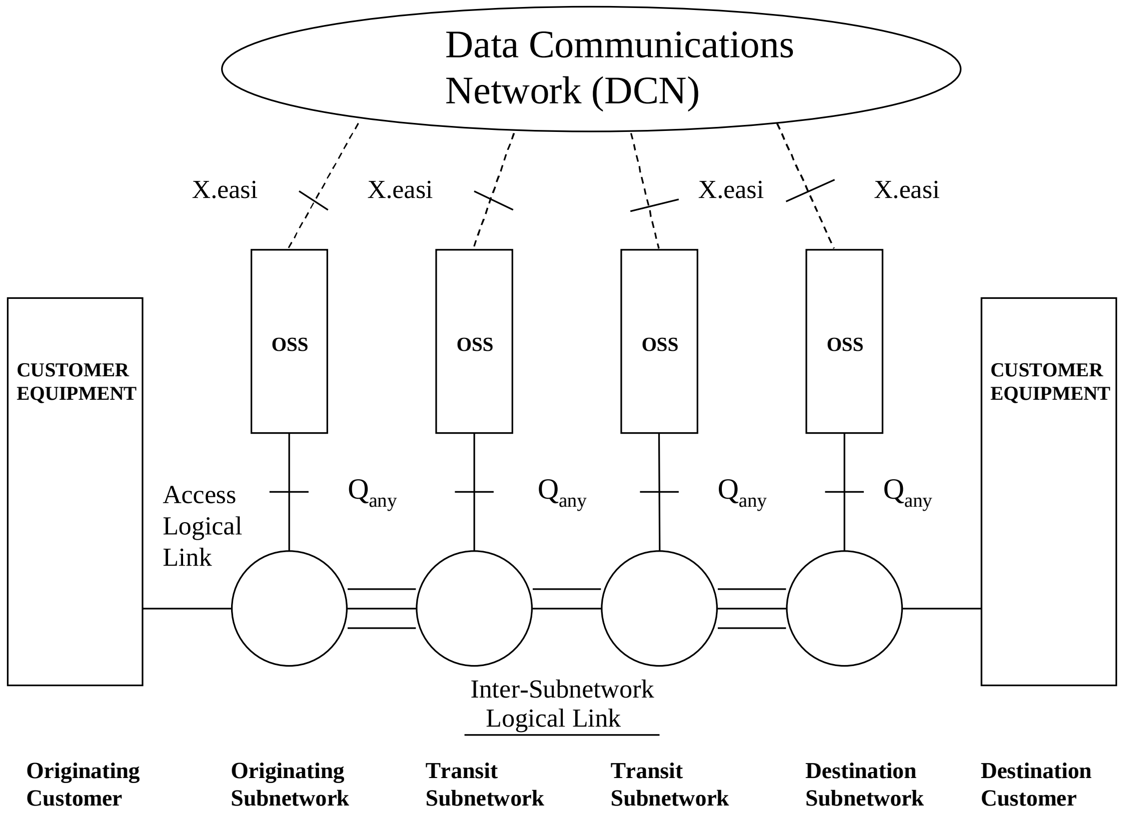


Figure A.2: Reference Configuration

The Subnetworks are interconnected by a set of Inter-Subnetwork Logical Links. The term Logical Link has been used for characterizing an ATM cell transfer capability. A Physical Link such as SDH STM-1 may carry a single VC4 Logical Link or 4 VC3 Logical Links.

The Access Logical Link is the one connecting the Customer Equipment with the corresponding local Subnetwork.

Each Subnetwork has at least one unique OSS with the capability of managing all the VPCs to be established through it. For a given inter-Subnetwork VPC, the Originating OSS is also responsible for the selection of the route and the handling, in a centralized way, of all the network processes related to the establishment, modification and release of this VPC, based on the dialogue with the rest of the Subnetwork OSSs involved in the connection.

Each end user has the capability of requesting several actions concerned with the use of the VP connection. The actions available to each user depend on whether the end user is the originating or the destination one. Therefore, the originating end user should be capable of asking for the release and/or the modification of the VP connection, whereas the destination end user should only be able to ask for the release of the connection (no modification is allowed to the destination user).

Virtual Channel Connection

The reference model for VCC is essentially the same as for VPC with the following changes and enhancements:

- The VCC comprises of a number of concatenated Virtual Channel Sub Network Connections.
- The establishment and routing of VCCs is carried out by an OSS which provides a Virtual Channel operations support system functionality (in conjunction with Virtual Path operations support system functionality).
- The endpoints of the VCC and Logical links will need to identify both the Virtual Path Indicator (VPI) and the Virtual Channel Indicator (VCI) used.
- VCCs will be established across a VP bearer network. Specifically, selection and establishment of the inter-subnetwork links to support a specific VC will be established by the OSS. In [1], it states that VPC will contain either permanent or switched virtual channel connections. This principle should be enforced in the OSS implementation.

A.2.1.3 Main assumptions

For Phase 1, the interconnect processes included in this subclause are based on a set of basic assumptions, which do not preclude further modifications or enhancement to Virtual Path Bearer Services or Virtual Channel Connections , in order to simplify their description.

These main assumptions are:

Point to Point VPCs and VCCs: In Phase 1, only point to point VPCs/VVCs will be supported.

Bi-directional and asymmetric VPCs and VCCs: All the VPCs VCCs established in the interconnected pan-European ATM Network should be logically bi-directional, with the same label (VPI and VCI) for both directions. The bandwidth allocated in each direction may be different (in the case of a unidirectional connection one of them could be null). Thus each VPC/VCC will be described by means of a VPC/VCC data descriptor, and this descriptor will be split into two parts; each of them referring to a distinct direction (forward and backward).

For Phase 1 The bandwidth reservation will be based on terms of peak cell rate.

Individual VPC handling (no grouping of VP will supported): Each VPC should be set up in an individual manner based only on the network load and configuration. The originating OSS will not accept any requirements for routing the requested VPCs derived from the customer grouping requirement (e.g. If a customer requests two VPCs, the originating OSS will select independently the path for each one).

Individual VCC handling (no grouping of VC will supported): Each VCC should be set up individually with connection based only on the network load and configuration. Note a VP will intrinsically allow a set of end to end VCCs to be grouped together under end system control.

Distributed management: There is no requirement for one centralized ATM interconnect service operational network management centre. The management should be distributed among all the OSSs (one for each Subnetwork) in a co-operative way. This assumption implies that each OSS needs to know some topological information of the overall network as which Subnetworks are interconnected and the Logical Links (including bandwidth at the ATM layer) available for the interconnections between two Subnetworks.

Source handling of VPC/VCC routing and parameters modifications: The processes for VPC/VCC establishment are managed by the Subnetwork OSS which originates the connection. This OSS will decide, based on the topological knowledge of the overall network, all the transit Subnetwork identifications required for the connections.

The use of more than two transit subnetworks in a VPC/VCC is permitted when absolutely necessary (for example, a topological reason) and should be recorded in the bilateral agreements.

The VPC/VCC parameter modification will be also be initiated by the originating Subnetwork OSS.

A.2.1.4 General Provisioning Principles

The processes for the establishment, modification or release of VPCs and VCCs are based on the following principles:

To minimize the number of transactions among OSSs in order to reduce the management traffic.

Each OSS will have an updated knowledge of the overall interconnected ATM network physical layer topology at the Inter-Subnetwork connectivity level. This database will comprise:

The existing Subnetworks and their associated Subnetwork Identifiers. No knowledge of the detailed internal composition of such Subnetworks is required.

The detailed list of the Logical Links (with its associated Logical Link Identifiers interconnecting the different Subnetworks. For each Logical Link, the installed ATM transfer capability (cells per second) should be explicitly declared.

Each OSS database should be updated with knowledge of the overall network Topology and available VP bearers/connections, for the support of both VC and VP connections.

The Originating OSS will have an updated knowledge of the activated/reserved VPCs/VCCs originated at its own Subnetwork. This database will contain, as a minimum, per VPC/VCC entry, the following data:

a) Assigned VP/VC connection identifier

b) Customer category, a classification of the customer depending on the operator's tariff policy. This parameter may be used to modify the weighting of the usage dependent parameters, and to set up tariff differential rules. This is, therefore, a local parameter (customer-local OSS related) which will be stored by the PNO in order to classify its customers for charging purposes.

c) Service allowed (permanent, reserved, etc.).

d) Schedule. A list of activation times, dates and duration for a VP/VC connection. This data may include calendar pattern (daily, weekly, etc.), with possible changing cell rate template.

   The cell rate template will include:

   - Bandwidth in the forward (source to destination) direction in ATM layer (peak cell rate).
   - Bandwidth in the backward (destination to source) direction in ATM layer (peak cell rate).

e) Source user identification (as defined in annex B, e.g. E.164 [44] address).

f) Destination user identification (as defined in annex B, e.g. E.164 [44]).

g) Requested Benchmark Service. (SMDS, Frame Relay etc.).

h) Application (File Transfer ...).

i) Path List (Originating Subnetwork Identifier, Transit Subnetwork Identifiers, Destination Subnetwork Identifier, Sequence of inter-Subnetwork Logical Links Identifiers involved in the VPC/VCC).

j) For VPCs the assigned Sequence of the VPIs in each Logical Link (including the Access Logical Link); and for VCCs the assigned Sequence of the in each Logical Link.

k) Parameters used for charging/accounting purposes.

The transit OSSs, if any, will have an updated knowledge of the activated/reserved VPCs/VCCs in transit at its own Subnetwork. This database will contain, as a minimum and per VPC/VCC entry, the following data:

a) Assigned VP/VC connection identifier.

b) Service allowed (permanent, reserved, etc.).

c) Schedule. A list of activation times, dates and duration for a VP/VC connection. This data may include calendar pattern (daily, weekly, etc.), with possible changing cell rate template.

The cell rate template will include:

- Bandwidth in the forward (source to destination) direction in ATM layer (peak cell rate).
- Bandwidth in the backward (destination to source) direction in ATM layer (peak cell rate).

d) Preceding Subnetwork Identifier (Originating or Transit).

e) Next Subnetwork Identifier (Transit or Destination).

f) Inter-Subnetwork Logical Links Identifiers involved in the VPC, from the preceding Subnetwork and to the next Subnetwork.

g) VPIs/VCIs assigned to the VPC/VCC in each of the Logical Links, from the preceding and to the next Subnetwork.

h) Originating PNO identifier. This information, that identifies the origin operator of the connection, is necessary to communicate the fault messages in case of a fault detected in the transit OSS.

The destination OSS will have an updated knowledge of the activated/reserved VPCs terminated at its own Subnetwork. This database will contain, as a minimum and per VPC/VCC entry, the following data:

a) Assigned VP/VC connection identifier.

b) Source user identification.

c) Destination user identification.

d) Service allowed (permanent, reserved, etc.).

e) Schedule. A list of activation times, dates and duration for a VP/VC connection. This data may include calendar pattern (daily, weekly, etc.), with possible changing cell rate template.

The cell rate template will include:

- Bandwidth in the forward (source to destination) direction in ATM layer (peak cell rate).
- Bandwidth in the backward (destination to source) direction in ATM layer (peak cell rate).

f) Originating Subnetwork Identifier .This information, which identifies the origin operator of the connection, is necessary to communicate the fault messages in case of a fault detected in the destination OSS.

g) Preceding transit Subnetwork Identifier (if any).

h) Inter-Subnetwork Logical Link Identifier involved in the VPC/VCC, from the preceding Subnetwork (originating or transit).

i) VPI/VCI assigned to the VPC/VCC in the above mentioned Logical Link and the VPI/VCI assigned to the VPC/VCC in the Access Logical Link (to its local Customer Equipment).

A.2.1.5 Basic provisioning processes

The basic provisioning procedural steps are:

- VPC/VCC Establishment Procedure
- Check Destination Availability
- Check User Compatibility
- Determine Route
- Connection Reservation
- Connection activation

- VPC/VCC Bandwidth Modification Procedure - optional
- VPC/VCC Restoration/ Reconfiguration Procedure - optional
- VPC/VCC Release Procedure

The later subclauses, A.2.2 through to A.2.5, describe at a high level how those procedural steps are used for specific operational approaches. The detailed description of these procedural steps is contained in subclause A.2.5.3.

A.2.1.6 Provisioning Response Targets

From a perspective of satisfactory interconnect service operation processes, the time taken to complete an order should be a maximum of 8 working hours, i.e. 8 working hours from the initial request from PNO A to PNO B at the Service Management level. Provisioning should be performed during the working day, the working day being those hours normally attended by each PNO's operators.

A.2.2 Bilateral (no Transit) PVP and PVC Provisioning Procedures

Two forms of bilateral Provisioning Procedures have been identified:

The Matched Order procedure where the customer orders "half connections" from each of two operators. This approach is difficult to operate for multi-point services or where a specific transit operator is needed to form part of multi-operator provisioned services.

The "One stop Shopping" procedure where the customer approaches one PNO and that PNO acts on behalf of the customer with respect to the other PNOs. This is similar to the approach taken in JAMES and is more suitable for PNOs operating services that also require transit switching or multi-point operation possibly on different routes.

This annex provides process descriptions for both methods and the automated X.easi interfaces should support either method of operation.

A.2.2.1 Bilateral Matched Order Provisioning Procedures

It is assumed for the purpose of this procedure that the customers of the PNOs have access to their respective ATM networks and that sufficient bandwidth exists within those access connections and networks. i.e. adequate network capacity is pre-planned.

A service modification request from VP to VC (or vice versa) will be treated as a "provide and cease".

The preferred method of contact will be the use of X.easi automated interfaces, although telephone, e-mail or fax may be used for backup purposes.

Figure A.3 shows the high level process workflow for the order process.

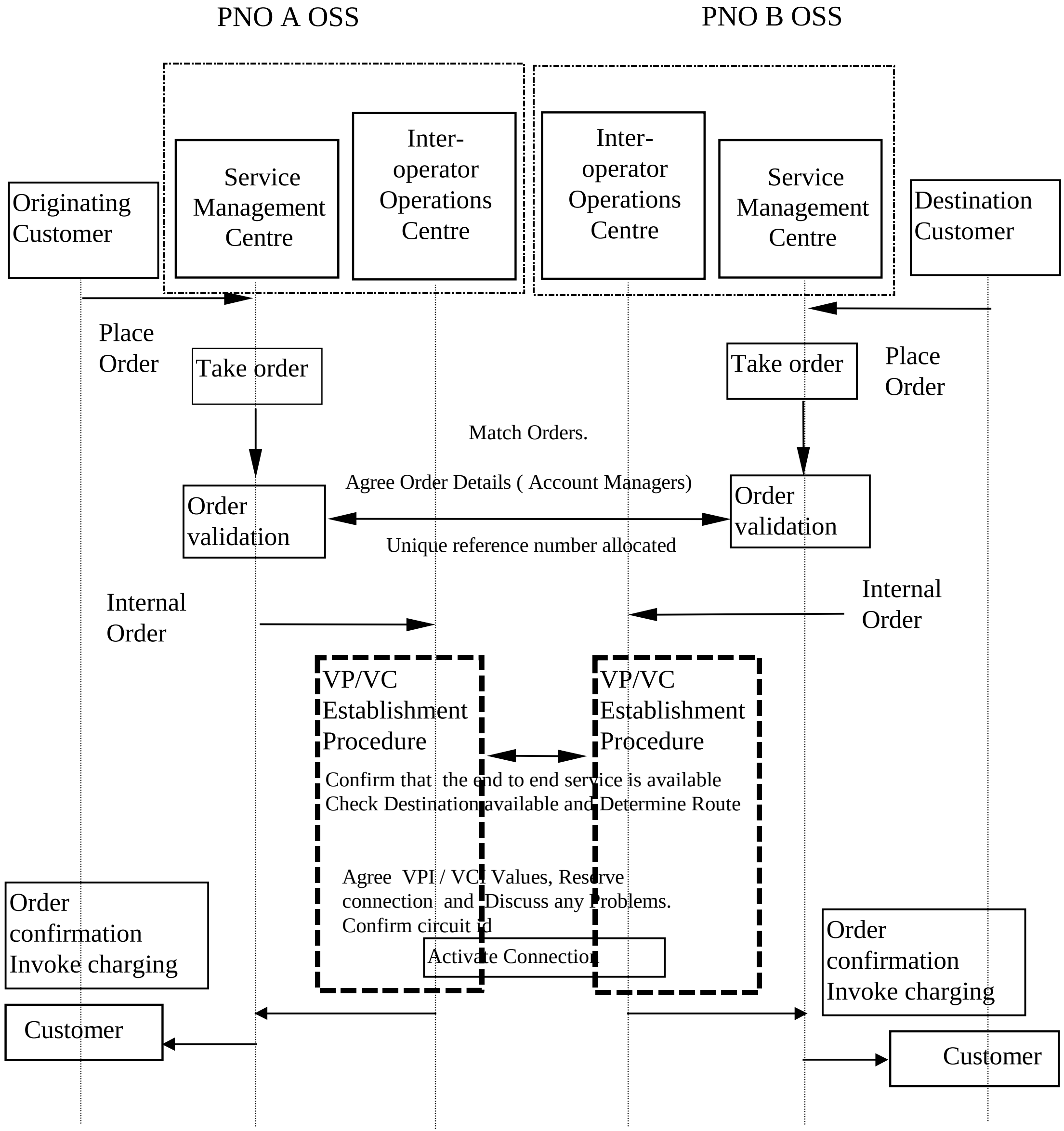


Figure A.3: Bilateral Provisioning Procedure - Matched Orders

The principal critical procedure steps are:

i) The customer order will be placed with each PNO's account team. The PNOs will each confer to obtain a unique order. This unique number will enable both PNO's provisioning systems to identify the orders prior to a common circuit identity being generated. The Service Management Centre (SMC) is responsible for validating the customer's service requirements, matching the orders, and agreeing a single order Reference Number.

ii) Upon agreement with the customer, the PNO's account teams will progress the order. The two PNO's Service Management Centres will then contact each other by telephone and/or fax to confirm that they have received the order.

iii) The two PNOs will each process the order and pass an internal order and authorization to their Inter-Operator/International Operations Centres (IOC).

iv) Upon receipt of the order from their respective SMCs, the two Inter-Operator/International Operations Centres (IOC) will contact their counterparts using the VP/VC Establishment procedure which should use automated X.easi interfaces wherever available for normal operation, or manual processes using phone, e-mail or fax using the form in subclause A.2.6.

The IOCs will agree a PVP/PVC Circuit Identifier and a bearer VPI/VCI allocation.

Connection Identifier

The Connection Identifier and VPI/VCI values to be used will be defined in the engineering plan.

The "end to end" circuit identifier will also need to be agreed at this point and should use one of the forms described in annex B. An example of the currently used form of identifier used is:

"Bearer Link id +VPI/VCI"

This exploits the fact that there is a close coupling in Phase 1 between the Physical Bearer and the ATM Layer for the Inter-subnetwork Logical Link.

Annex B gives a more detailed treatment of the possible choices including the extended ITU-T Recommendation M.1400 standard [13].

v) The two PNO's IOC will then configure the circuits and confirm completion with each other. This should be achieved by using the interface Connection Reservations and Activation processes.

vi) Once confirmation has been received by IOCs, they will inform their respective Service Management Centres via their own internal processes that the order has been completed. The two Service Management Centres will confirm completion of the order with each other and resolve any customer problems that may arise.

If, at any time during this process there is a need to escalate within either company, the management escalation paths contained in subclause A.2.5 should be used.

A.2.2.2 One Stop Shopping Bilateral Provisioning Procedure

The most desirable method of contact will be the use of the X.easi automated interfaces although manual interface processes using telephone, e-mail or fax is the mandated minimum capability.

Figure A.4 shows the high level process workflow for the order process. It differs only in the initial process steps but this lead to considerable timesaving since one PNO acts as a proxy for the customer.

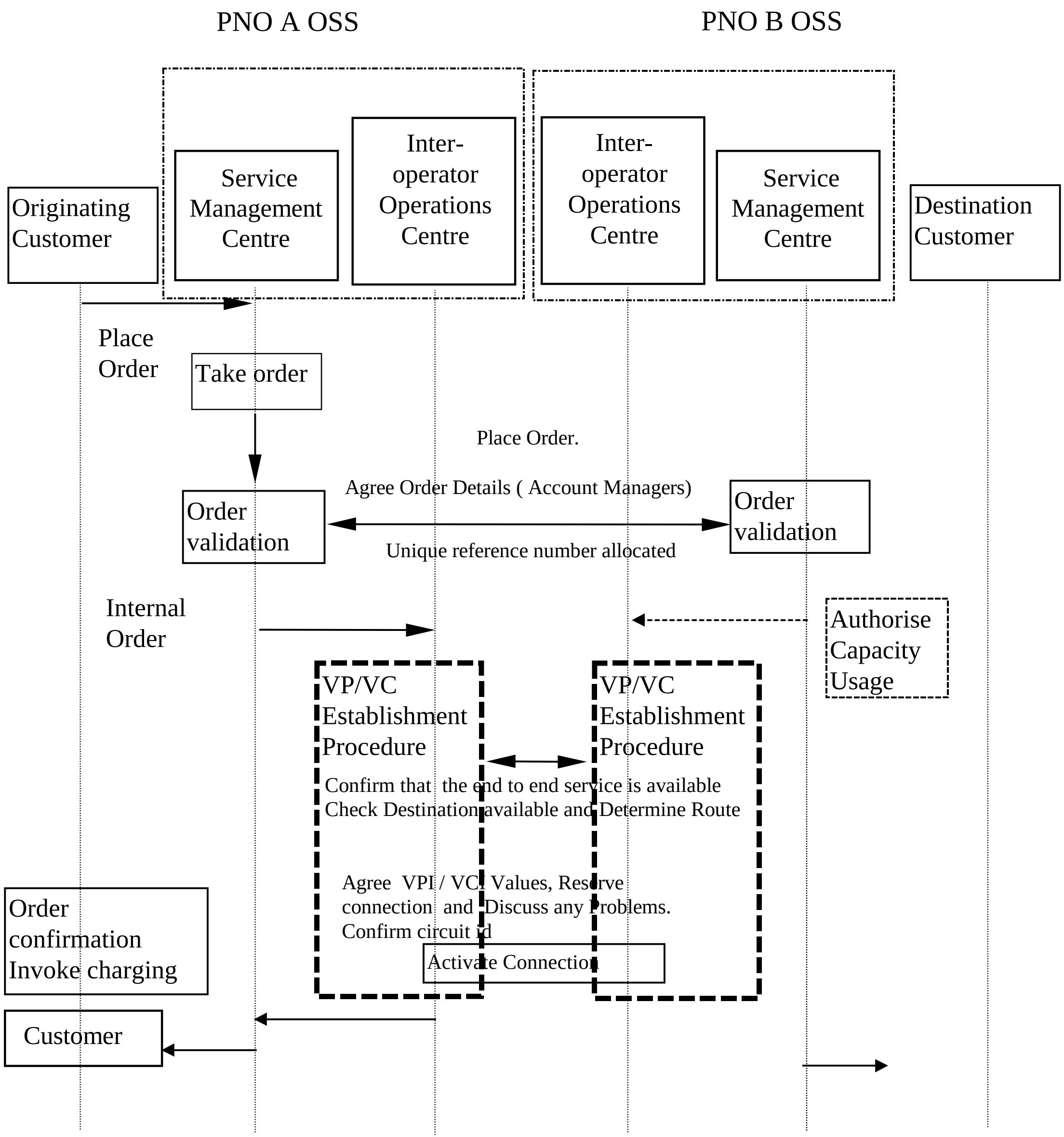


Figure A.4: Bilateral Provisioning Procedure - "One stop Shopping"

The process steps follow the same structure as the previous subclause for matched orders and the same contact information needs to be agreed , recorded and change managed. However PNO B's involvement is simply to authorize capacity usage either for this order, or for sets of orders collectively.

A.2.3 One Stop Shopping Multilateral (Transit) Provisioning Procedure

This is achieved using multiple instances of the One stop shopping Bilateral process with one PNO or a proxy acting as a co-ordinator for establishing the end to end connection. Some examples are shown in the detailed provisioning procedure descriptions in subclause A.2.5.3.

A.2.4 PVP and PVC Regrade Provisioning Procedure

A regrade is defined as a minor change to the attributes of an existing circuit, e.g. a change in bandwidth from 2 Mbits/sec to 4 Mbits/sec or the change in the scheduling of a part-time connection. This should be undertaken in alignment with processes defined by the Modification MSC in [6].

A regrade from VP to VC (or vice versa) will be treated as a "provide and cease" and will therefore follow the SMC order process. This is important because of the customer service and subscription charging implications.

A.2.4.1 Bilateral PVC Regrade Process - Matched orders

Figure A.5 shows the high level process workflow for the PVC regrade process.

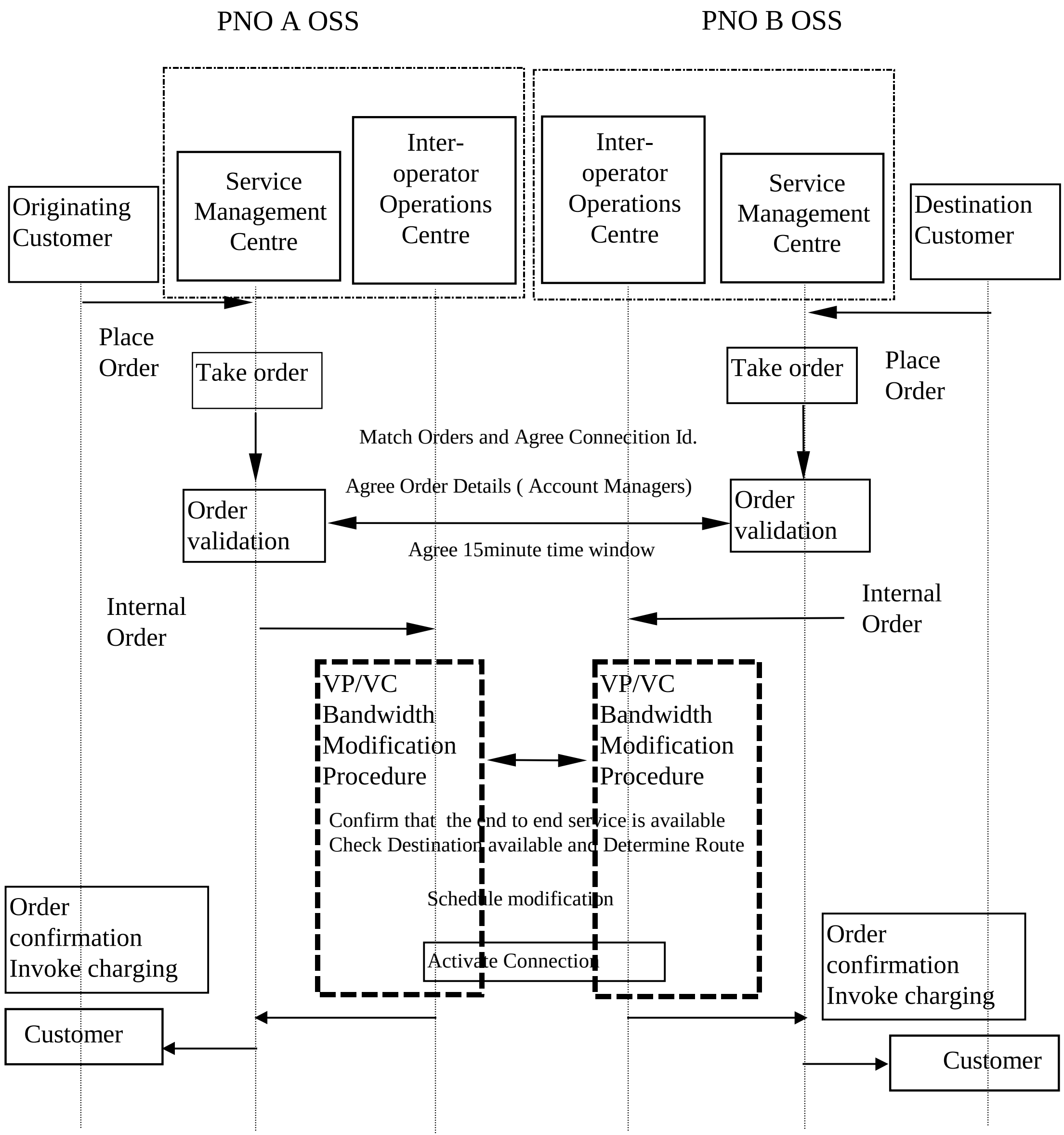


Figure A.5: PVP PVC Regrade Procedure - matched orders

The following critical procedure steps should be noted:

i) The customer request for regrade will be placed with both PNO's account teams. The account teams will ascertain from the customer whether they have a preferred time window for the regrade, or whether they will accept a time convenient to both PNOs. The account teams should endeavour to ensure that this time window is within the normal working day to assist proper supervision of the correct completion of the modification.

Contact details for the respective account teams are recorded in the completed and agreed Operational Contact and Procedural Templates.

ii) Upon agreement with the customer, the respective account teams will progress the order. PNOs will pass the order to their respective SMC. Details of the changes to be made, the circuit identity and the agreed time of the change (if any) must be communicated at this stage.

iii) The PNO SMC's will then contact each other by telephone, fax or e-mail to confirm that they have received the order and progress any issues.

iv) Upon receipt of the order, PNO's IOC will contact each other using the VP/VC Modification Procedure, if using an automated interface.

Where the customer has specified a preferred date and time for the regrade, the PNO IOCs must confirm that they are able to meet the specified time window. Once agreement has been reached, the information should be passed to the respective Service Management Centres using internal processes for onward communication to the customer.

Customer specified time not acceptable to either PNO's IOC. In the event that the customer specified time is not acceptable the PNO's IOC will jointly suggest an alternative time window. The new time should then be communicated to the respective Service Management Centres, who will be responsible for gaining the customers agreement to the suggested time window. Once the new time window is a agreed, the information will be passed from the between the IOCs, who will confirm the new time window is acceptable. When this has been established, the information should be passed to the respective Service Management Centres using internal processes for onward communication to the customer.

Where the customer has specified no preferred time and date the PNO IOC should arrange and agree a time for the regrade. This time window should be within the agreed timeframe following the original customer order. Once agreement has been reached, the information should be passed to the respective Service Management Centres using internal processes for onward communication to the customer. Should the customer not agree to the proposed time window, then the Service Management Centres will communicate this information to IOCs using local processes with a customer suggested time window. The IOC should then agree and confirm this time window using X.easi interfaces, telephone e-mail or fax. This information will then be forwarded to the Service Management Centres who will confirm to the customer that their suggested time window has now been accepted.

v) Once the regrade has been completed, the IOC will confirm with each other that the changes have been made and inform their respective Service Management Centres for onward communication to the customer. During the customer handover period, the Service Management Centres may contact one another in order to resolve any customer problems.

Manual interfaces should use the forms in subclause A.2.6.

At any time during this process there is a need to escalate within either company, the management escalation paths should be used as described in subclause A.2.5.

A.2.4.2 One Stop Shopping Bilateral PVC Regrade Procedure -One stop shopping

This procedure is similar to the bilateral case except the interactions between the SMCs is different since only the originating customer initiates the procedure. The situation is illustrated in figure A.6.

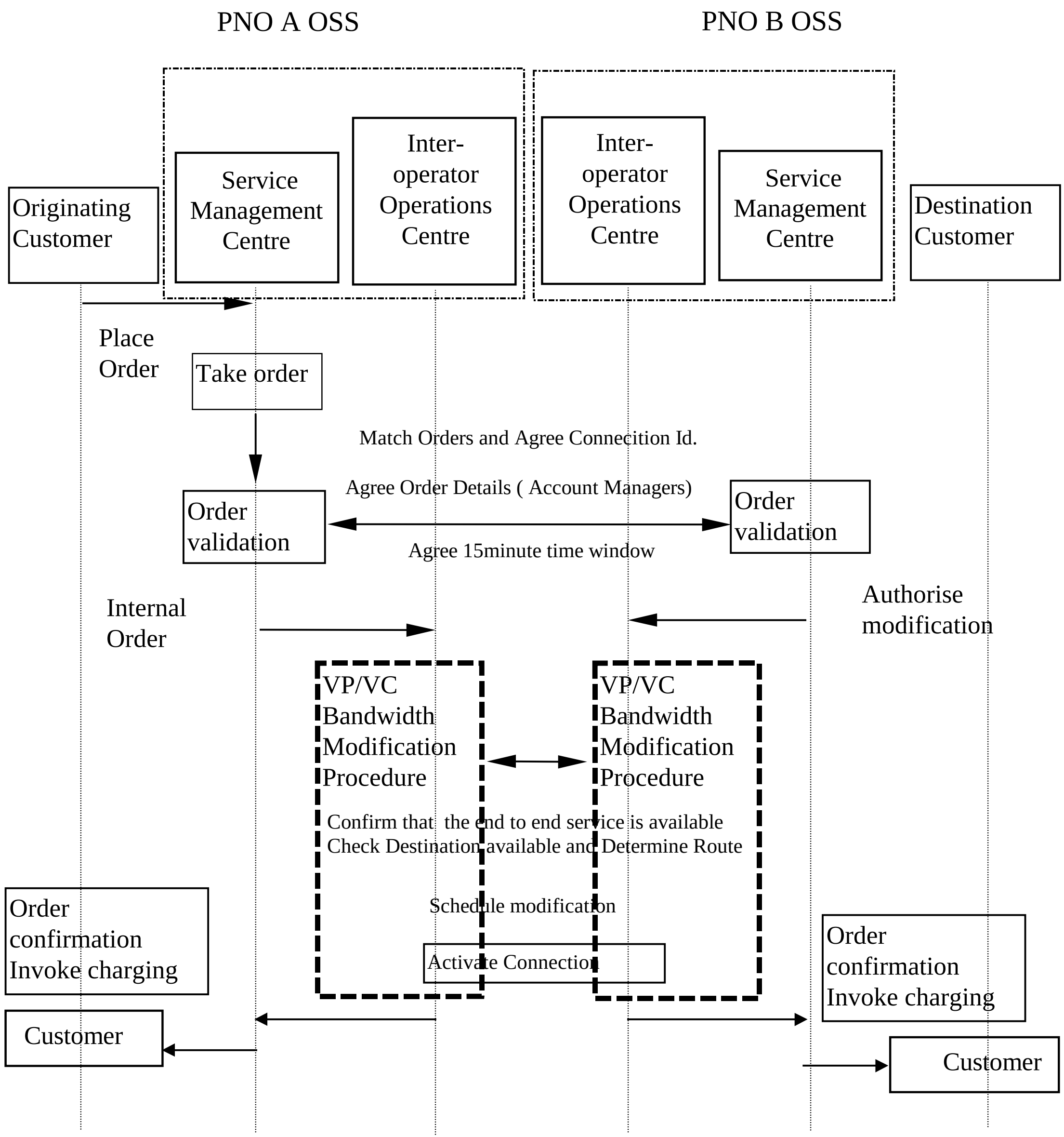


Figure A.6: PVP/PVC Regrade procedure - Bilateral One stop shopping

PNO B's SMC responsibilities are limited to granting of authority to allow the remote modification request this can be done on a per service modification bases, per bilateral pair, or on any other method acceptable to PNO B.

A.2.4.3 Multilateral PVC Regrade Procedure

This is achieved using multiple instances of the One stop shopping Bilateral process with one PNO or a proxy acting as a co-ordinator for establishing the end to end connection. Some examples are shown in the detailed provisioning procedure descriptions in subclause A.2.5.3.

A.2.5 ATM PVC Provision Order and Regrade Management Escalation

A.2.5.1 Service Management Escalation

When events such as a breakdown in communications, lost orders, differing order details, or failure to agree a time window, a four stage escalation process should be used between operators at **a service management level**.

The first level escalation should normally be to the manager for the Service Management Centre. Each escalation should move at least one stage up the internal reporting structure of the PNO.

NOTE: 4th level is the highest level.

PNOs should record in an Operational Contact and Procedural Templates (OCPT) the Service provisioning escalation contact points covering names telephone, fax and e-mail ids.

Where multi-lateral provisioning has been used the organization carrying out the lead role in either one stop shopping or a co-ordinating role should act as the point of escalation for all of the co-operating PNOs. This avoids the need for each organization to hold escalation contact details for all of the co-operating PNOs.

A.2.5.2 Operational Management Escalation

When events such as a breakdown in communications, lost orders, differing order details, or failure to agree a timewindow occur, the following contact points are provided for escalation within the PNOs at an operational level.

NOTE: 4th level is the highest level.

PNOs should record in an Operational Contact and Procedural Templates (OCPT) the operational provisioning escalation contact points covering names telephone , fax and e-mail ids.

A.2.5.3 Provisioning Procedures - Detailed descriptions

A.2.5.3.1 VPC/VCC Establishment Procedure

Apart from some minor additions to the information exchanged about termination's and logical links, the processes described below can be used for both PVP and PVC Connection provision.

The procedure of Establishment of a VPC/VCC has been designed to minimize the number of individual transactions among Subnetworks OSSs, ensuring, at the same time, the VPC/VCC associated data collection, distribution and validation.

After receiving from the local customer the VPC/VCC request (message C_VPC_Request/ C_VCC_Request), the originating Subnetwork PNO will initiate the VPC/VCC Establishment Procedure.

Each C_VPC_Request Request/C_VCC_Request will contain a **request identifier (req_id)** in order to be able to distinguish among several different requests sent by the same customer. It is the responsibility of the customer to follow a predetermined algorithm to assign distinct request identifiers for different C_VPC_Request/C_VCC_Request messages.

This identifier has a local meaning; exclusively related to the customer-local OSS interface during the establishment procedure.

The VPC/VCC Establishment Procedure can be divided into five phases:

- the "Destination availability checking";
- the "Check User Compatibility";
- the "Determine route";
- the "Connection Reservation"; and
- the "Connection Activation" phases.

A.2.5.3.2 DESTINATION AVAILABILITY CHECKING

Upon the reception of the C_VPC_Request/C_VCC_Request, the OSS will assign a unique VP/VC connection id to the new "possible" VPC; establishing, at the same time, the mapping between this VP/VC connection id and the request identifier (req_id).

VP/VC connection id	req_id

For the messages, exchanged among the different OSSs, the *VP/VC connection id* will be used as a unique reference to identify each VPC/VCC.

The originating OSS will issue a N_VPC_Checking/N_VCC_Checking message to the destination OSS, in order to check that the destination user is reachable and wishes to accept this VP/VC connection. This message will contain the VP/VC connection id, the originating Subnetwork Identifier and Customer Identifier, the destination Customer Identifier, the data associated with the duration, start time, etc. of the VPC/VCC, the requested forward and backward bandwidth, the requested service, and the application.

After checking its local resources, the destination OSS will issue a C_VPC_Checking/C_VCC_Checking message to the destination customer. The customer will answer either with a C_VPC_Checking_Confirm(OK)/C_VCC_Checking_Confirm(OK) message in case of acceptance, or with a C_VPC_Checking_Confirm(Not_OK)/C_VCC_Checking_Confirm(Not_OK) message in case of rejection.

In the first case, the destination OSS will issue a N_VPC_Checking_Confirm(OK)/N_VCC_Checking_Confirm(OK) message to the originating OSS, which will proceed to the following phase.

This message should include an ordered list of the subnetworks directly connected to the destination Subnetwork by means of the Logical Links with available cell rate for the requested connection. This list will be used by the originating OSS to assist in the selection of the route (concatenation of PNO's subnetworks).

In the second case, the destination OSS will issue a N_VPC_Checking_Confirm(Not_OK)/N_VCC_Checking_Confirm(Not_OK) message to the originating OSS, giving the cause of the rejection (e.g. destination customer rejection) and the associated VPC/VCC connection id. On receipt of this message, the originating OSS will send the corresponding C_VPC_Request_Confirm(Not_OK)/C_VCC_Request_Confirm(Not_OK) message to the originating customer, and terminate the VPC/VCC establishment procedure.

The C_VPC_Request_Confirm(Not_OK)/C_VCC_Request_Confirm(Not_OK) message to the originating customer will contain the rejection cause and the req_id related to this request, so that the customer will be able to map the rejection to its corresponding request. The req_id will have been obtained by the originating OSS by looking into the VP/VC connection id-req_id table, using as the key the VP/VC connection id received in the N_VPC_Checking_Confirm(Not_OK)/N_VCC_Checking_Confirm(Not_OK) message.

A.2.5.3.3 CHECK USER COMPATIBILITY

Check User Compatibility may be defined as an action is to check if the end user (i.e. the user connected to the network of the Z-PNO) is willing to and is able to accept the proposed VP or VC Connection. The cases described below are based on the use of an automated interface which supports an appropriate standard for VP/VC path configuration [6] but may be replicated by manual procedures and responses in the event of use of a manual interface.

Several different check user causes, which result in user incompatibility may be identified as follows:

- **Bandwidth Not Available:** the end user is not able to support the band width(s) required in the ATM VP or VC schedulers, which need to be specified as part of the path reservation requirements.
- **User Not Available:** it includes the following cases:
    - non-existing end user;
    - end user availability status with the value notAvailable;
    - end user operational state with the value disabled;
    - end user administrative state with the value locked.

All these four cases are internal to each PNO and would not be visible from the X.easi interface. i.e. the I-PNO would only receive the userNotAvailable response over the X.easi interface. In the event that the I-PNO requires additional information consequent on receiving a userNotAvailable response, it may be suggested that investigation by conventional enquiry (e.g. phone call) is undertaken.

- **User Not Compatible:** it includes the following case:
  - with regard to a list of originating users (i.e. users connected to the I-PNO) which the destination user does not want to have any connection.

    Compatibility of the end user will be indicated when the Z-PNO sends a "User OK" response to an I-PNO Check User Compatibility request.

A.2.5.3.4 DETERMINE ROUTE

The following assumptions about the routing method have been made:

Each PNO has a complete knowledge of the topological structure of the whole network, such as subnetworks, number of Logical Links between each pair of adjacent subnetworks and their capacities.

The originating PNO decides the concatenation of PNO's subnetworks to reach the destination.

The PNOs involved in the VP connection establishment have the freedom to choose the Logical Link to reach the next subnetwork on the route.

The OSS has the information to select the appropriate VP to support any required VC Connection.

The objectives of this procedural step are:

Determine route: Determining the different routes between origin and destination subnetworks.

The **result** of the Determine Route algorithm should be **a sorted list of routes** described in terms of subnetworks crossed, between the origin and destination subnetworks.

Route selection: Selecting one route from the list among all the possible alternatives.

After the successful completion of this phase, the originating OSS should have the preferred route through the ATM Network.

A.2.5.3.5 CONNECTION RESERVATION (Allocation of network resources)

The connection reservation phase should try to reserve the resources for the connection on the route previously calculated during the determine route phase.

The originating OSS will select a Logical Link having enough capacity for the required VPC/VCC bandwidth and connecting the originating Subnetwork with the following Subnetwork in the selected route. It will also select the VPI/VCI to be used inside this Logical Link.

Subsequently, the originating Subnetwork OSS will send a message to the following OSSs (transit or destination) in the selected route. This message (N_VPC_Request/N_VCC_Request) will contain the assigned VP/VC Connection Identifier, the data associated with the type of subscription, the originating Subnetwork Identifier, the already selected Logical Link Identifier from the originating Subnetwork to this Subnetwork, its associated VPI/VCI, and the next Subnetwork Identifier.

Assuming this second Subnetwork is a transit one for the VPC/VCC, at the reception of the N_VPC_Request/N_VCC_Request message, the corresponding OSS will investigate both the availability of transmission resources towards the following Subnetwork of the route and the absence of internal congestion inside the Subnetwork. If those resources are enough for the required forward and backward directions, it will reserve a particular Logical Link toward the next Subnetwork, and the corresponding VPI/VCI. Afterwards, it will issue a N_VPC_Request_Confirm/N_VCC_Request_Confirm message to the originating OSS, specifying the Logical Link Identifier and the VPI/VCI proposed in the connection with the next Subnetwork. Both the internal and external resources will be reserved for the duration(s) of this VPC/VCC.

The originating OSS will then proceed with the OSS of the following transit Subnetwork of the selected route, issuing a new N_VPC_Request/N_VCC_Request message that will incorporate again the assigned VP/VC Connection id, the data associated with the type of subscription, the preceding Subnetwork Identifier, the already selected Logical Link Identifier from the preceding Subnetwork and its associated VPI/VCI, and the next Subnetwork Identifier. Again, this OSS will investigate its internal resources and will select, if possible, a suitable Logical Link towards the following Subnetwork, together with the corresponding VPI/VCI. The new parameters (Logical Link Identifier and VPI/VCI) will be communicated to the originating OSS using a N_VPC_Request_Confirm/N_VCC_Request_Confirm message.

Therefore, the reservation of the network resources will be implemented in a serial mode. The originating OSS will send a reservation request to the first transit OSS, waiting for the response from this transit subnetwork. Afterwards, in case of affirmative response, it will send a new reservation request to the next transit subnetwork, and so on.

This process will continue until the originating OSS sends the N_VPC_Request/N_VCC_Request message to the destination OSS. This destination OSS will then investigate the possible internal available resources from the suggested Logical Link input port toward the destination local access port.

If the result is positive, it will issue a C_VPC_Request/C_VCC_Request message to the local customer.

In case of negative answer from the customer, the destination OSS will issue a N_VPC_Request_Confirm(Not_OK) message to the originating OSS.

Afterwards, and in case of positive answer from the customer, the destination OSS will issue a N_VPC_Request_Confirm(OK)/N_VCC_Request_Confirm(OK) to the originating OSS.

Finally, the originating OSS will issue a C_VPC_Request_Confirm(OK)/C_VCC_Request_Confirm(OK) message to the originating customer, and a N_VPC_Reservation(OK)/N_VCC_Reservation(OK) to all the subnetworks to make them aware of the successful completion of the reservation phase.

The C_VPC_Request_Confirm/C_VCC_Request_Confirm message will contain the pair (VP/VC connection id - req_id), in such a way that the customer will be able to relate its request and the VPC/VCC granted. Hence, the customer, from this moment and until the release of the VPC/VCC, will use this identifier (VP/VC connection id) to refer the VPC every time it wants to perform some operation over that VPC/VCC (for instance a modification request).

This successfully completes the "Connection Reservation " phase.

An example

This procedure is illustrated in figure A.7, where the case of an successful end to end VPC/VCC "Connection Reservation" process through two transit Subnetworks is indicated. The figure illustrates the example of a VP Connection to simplify the presentation.

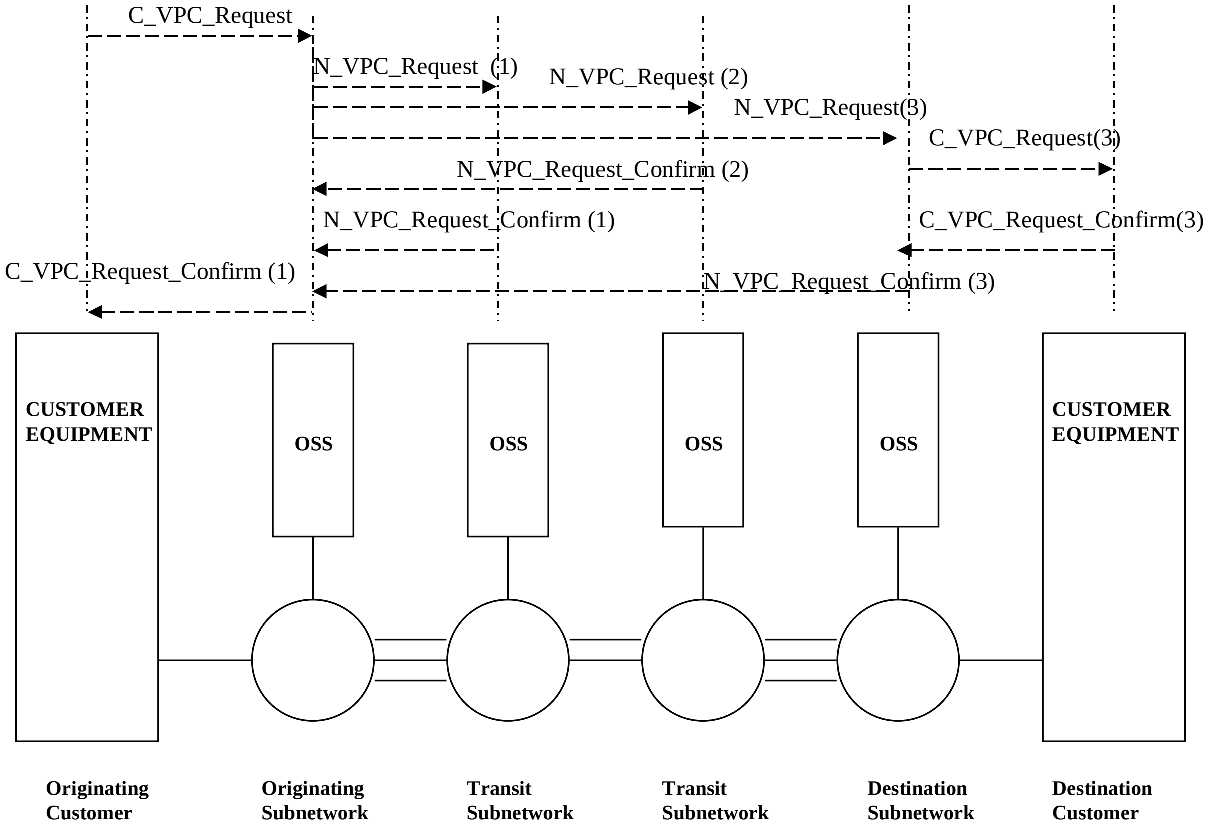


Figure A.7: Connection Reservation Procedure

If a Subnetwork OSS finds that there are not sufficient network resources (internal or external) available in the following Subnetwork, it will issue a N_VPC_Request_Confirm(Not_OK)/N_VCC_Request_Confirm(Not_OK) message to the originating OSS, specifying the rejected VP/VC connection id and the cause(s) of the rejection.

On reception of this message, the originating OSS will send a N_VPC_Request_Confirm(Not_OK)/N_VCC_Request_Confirm(Not_OK) message to each of the OSSs which have already reserved subnetwork connections, indicating the aborted VP/VC Connection id. **(NB: This message is not sent in case of a VPC/VCC without any transit subnetwork)**

Those OSSs receiving this message will cancel the reservation of resources to that particular VPC/VCC indicated in the message. In addition, the destination OSS will send a C_VPC_Checking_Confirm(Not_OK)/C_VCC_Checking_Confirm(Not_OK) message to the destination customer to inform it about the failure of the tentative connection.

The originating OSS will then, if possible, select a alternative route, and it will initiate a new "Connection reservation" phase. If no alternative route is possible, then it will issue a C_VPC_Request_Confirm(Not_OK)/C_VCC_Request_Confirm(Not_OK) message to the originating customer as it has been explained at the destination availability checking subclause, A.2.5.3.2.

A.2.5.4 Connection Activation

At the indicated time(s) by the scheduling in the connection request message, the VPC/VCC will be activated.

It is assumed as a general principle that, if the reservation phase has been successful, the activation will take place correctly as well. Hence, if NO abnormal event occurs between the end of the reservation phase and the activation triggering time, NO message will be sent at this latter time.

If a failure occurs during the interval between the connection reservation and activation , the VPC/VCC Restoration/Reconfiguration Procedure, described in subclause A.2.5.6 will be invoked.

A.2.5.5 VPC/VCC Bandwidth Modification Procedure

Several assumptions about the bandwidth modification procedure have to be taken into account:

The VPC/VCC bandwidth modification procedure should be only allowed for the case of reserved occasional mode with constant peak cell rate (a cell rate template with no variation has been provided at registration time).

The Bandwidth Modification is allowed if it does not produce any impact on the VPC/VCC routing.

The VPC/VCC bandwidth modification procedure is initiated by the originating customer in order to get an increase or decrease in the bandwidth of the VPC/VCC previously established (or reserved).

In the case of a bandwidth reduction, it is unlikely that there will be problems on the network side, the only required actions by the OSSs will be the adjustment of the UPC/NPC functions and the tables of the allocated resources.

In the case of an increase of the bandwidth, the result of the request may be either accepted or rejected.

Due to the fact that during some phases of the modification procedure "old" (Not modified yet) and "new" (Already modified) bandwidths along the distinct Logical Links could eventually co-exist, the customer must be willing to accept a possible degradation of the service temporarily.

The originating customer will issue a C_VPC_Modify_Request/C_VCC_Modify_Request message to its local OSS, (including the time parameter at which the modification is requested). At the reception of this message, this OSS will investigate the possibility of the modification of the bandwidth in the same Logical Link previously allocated, together with the absence of internal congestion problems.

If no problems are found, it will issue a C_VPC_Modify_Request/C_VCC_Modify_Request message in parallel to every transit and destination OSS.

In case of acceptance, a N_VPC_Modify_Confirm(OK)/N_VCC_Modify_Confirm(OK) message will be sent by the involved transit and destination OSSs in the backward direction and a N_VPC_Modify_Confirm(Not_OK)/N_VCC_Modify_Confirm(Not_OK) message in case of rejection. In the former case, the involved OSS will reserve the resources required for the new bandwidth, without changing the current VPC/VCC parameters.

On reception of the N_VPC_Modify_Request/N_VCC_Modify_Request message, the destination OSS will, after checking its local resources, make a request to the destination customer by means of a C_VPC_Modify_Request/C_VCC_Modify_Request message, that will in turn answer either:

- with a C_VPC_Modifiy_Confirm(OK)/C_VCC_Modifiy_Confirm(OK);
- or a C_VPC_Modify_Confirm(Not_OK)/C_VcC_Modify_Confirm(Not_OK) message.

The destination OSS will issue accordingly the N_VPC_Modify_Confirm(OK)/N_VCC_Modify_Confirm(OK) or the N_VPC_Modify_Confirm(Not_OK)/N_VCC_Modify_Confirm(Not_OK) message to the originating OSS.

In case of general acceptance, the originating OSS will issue a C_VPC_Modify_Confirm(OK) message to the originating customer and a N_VPC_Modify_Complete(OK) message to all the other involved OSSs (transit and destination subnetworks). At the reception of the N_VPC_Modify_Complete(OK), the destination OSS will send a C_VPC_Modify_Complete(OK) to the destination customer.

In the case of reception of a N_VPC_Modify_Confirm(Not_OK) message, the originating OSS will send a N_VPC_Modify_Complete(Not_OK) message to each one of the transit and destination OSSs. It will also send a C_VPC_Modify_Confirm(Not_OK) message to the originating customer. The destination OSS will also send a C_VPC_Modifiy_Complete(Not_OK) to the destination customer upon the reception of the N_VPC_Modify_Complete(Not_OK).

A.2.5.6 VPC/VCC Restoration/Reconfiguration Procedure

This procedure is optional. Each operator should indicate in their bilateral agreements whether they support this option. There is some interaction between the alarm processes and the fault and maintenance trouble ticketing processes described in subclause A.3.6.1.

A Restoration/Reconfiguration Procedure will take place as a consequence of a fault condition in the VPC/VCC. This fault condition may occur in one of the Access Logical Links, in one of the inter-Subnetwork Logical Links, or internally to one of the originating, transit or destination Subnetworks.

The OSS detecting a fault condition occurring in its Subnetwork or in its attached Logical Links, will issue a N_VPC_Fault/N_VCC_Fault message identified by means of a fault_id to the originating OSS, indicating all the affected VP/VC connection id's, the cause of the VPC/VCC interruption, the date/hour of such interruption, and the estimated duration of the fault situation. On reception of this message, the originating OSS will issue a C_VPC_Fault/C_VCC_Fault message for each fault VPC/VCC to the originating customer including the received fault duration estimation and the cause of failure.

The fault identifier (fault_id) will be used for identification purposes to distinguish several different faults and the affected VPCs/VCCs. The OSS detecting the fault situation must assign distinct fault identifiers for different N_VPC_Fault/N_VCC_Fault messages following a predetermined algorithm.

It its assumed that, immediately after the detection of the fault condition, the responsible OSS will start the required actions in order to solve the failure. As a result of such actions, two outcomes are possible:

(i) The failure only affects to an internal Logical Link inside a Subnetwork. In this case the affected Subnetwork is responsible of the restoration. Two possibilities exist:

  (a) The restoration inside the subnetwork is successful. In this case the subnetwork will issue a N_VPC_Fault_Recovery/N_VCC_Fault_Recovery message to the originating OSS indicating the fault_id and the time at which the restoration took place. In this case this message has only information purposes to the originating OSS. The originating OSS will accordingly send a C_VPC_Fault_Recovery/C_VCC_Fault_Recovery message to the originating customer.

  (b) The restoration inside the subnetwork is not successful. In this case the subnetwork should issue a N_VPC_Fault_Non_Recovery/N_VCC_Fault_Non_Recovery message to the originating OSS indicating the fault_id.

(ii) The failure affects an inter-subnetwork Logical Link between two different subnetworks. In this case another two different possibilities exist:

  (a) The failure is corrected without the intervention of the originating OSS. In this case the OSSs of the affected subnetworks are capable of correcting the failure. One of these subnetworks (the one who chose the Logical Link now in failure), will send a N_VPC_Fault_Recovery/N_VCC_Fault_Recovery message to the originating OSS indicating the fault_id and the time at which the restoration took place. In this case this message has only information purposes to the originating OSS. The originating OSS will accordingly send a C_VPC_Fault_Recovery/C_VCC_Fault_Recovery message to the originating customer.

  (b) The OSSs of the two affected subnetworks are not capable of correcting the failure. One of these subnetworks (the one who chose the Logical Link now in failure), will send a N_VPC_Fault_Non_Recovery/N_VCC_Fault_Non_Recovery message to the originating OSS indicating the fault_id and the Logical Link identification affected with the failure.

In case of unsuccessful failure restoration the originating OSS could initiate the actions related to the reconfiguration.

If reconfiguration is selected, the originating OSS will not send a C_VPC_Fault_Recovery/C_VCC_Fault_Recovery message to the originating customer until the reconfiguration procedure has successfully finished. This OSS will send a C_VPC_Release(Cause: Fault_Non_Recovery)/C_VCC_Release(Cause: Fault_Non_Recovery) message in case of unsuccessful completion of the reconfiguration actions and will initiate the release procedure (see subclause A.2.5.7).

If the non reconfiguration option is chosen, the release procedure will be initiated on decision from the originating OSS.

When the originating OSS receives a N_VPC_Fault_Non_Recovery/N_VCC_Fault_Non_Recovery message and a reconfiguration process has been started, the following actions are performed:

Searches for possible routes between the source and the destination using any user specified criteria.

Select a route (if any) between the source and destination. In case of no routes found, a C_VPC_Release(Cause: Fault_Non_Recovery)/C_VCC_Release(Cause: Fault_Non_Recovery) message is sent to the originating customer. The originating OSS should start the release procedure when it is judged necessary.

If a route has been found, the OSS should reserve in its local subnetwork the necessary resources.

This reservation process is repeated sequentially with all subnetworks involved in the connection until either a negative response is received or the destination subnetwork is reached.

If a negative response is received, it should be necessary to cancel the previously made reservations. In this case a C_VPC_Release(Cause: Fault_Non_Recovery) message is sent to the originating customer. The originating OSS should start the release procedure.

If the destination subnetwork is reached a C_VPC_Fault_Recovery message is sent to the originating customer. In this case the originating OSS should proceed to activate the new connection, and release the one in failure.

A.2.5.7 VPC/VCC Release Procedure

The VPC/VCC Release procedure may be initiated due to four possible reasons:

(i) Explicit request of the originating customer. The originating customer, using a C_VPC_Release/C_VCC_Release message to the local OSS, indicates the end of the subscription time.

(ii) Explicit request of the destination customer. The destination customer sends a C_VPC_Release/C_VCC_Release message to the destination OSS.

(iii) Implicit request of the originating customer. At subscription time, the originating customer had reserved a subscription duration that has expired.

(iv) Fault condition with unsuccessful Reconfiguration or reconfiguration not chosen. This case has been already covered in the previous point.

Case (I), see figure A.8: after the reception of the C_VPC_Release/C_VCC_Release message, the originating OSS, will answer to the customer with a C_VPC_Release_Confirm/C_VCC_Release_Confirm. In parallel, the originating OSS will issue a N_VPC_Release/N_VCC_Release message to all the affected OSSs. The transit OSS will release all the network resources allocated (activated or reserved) to this VPC/VCC. The destination OSS will, additionally, send a C_VPC_Release/C_VCC_Release message to the destination customer, including the cause of the release.

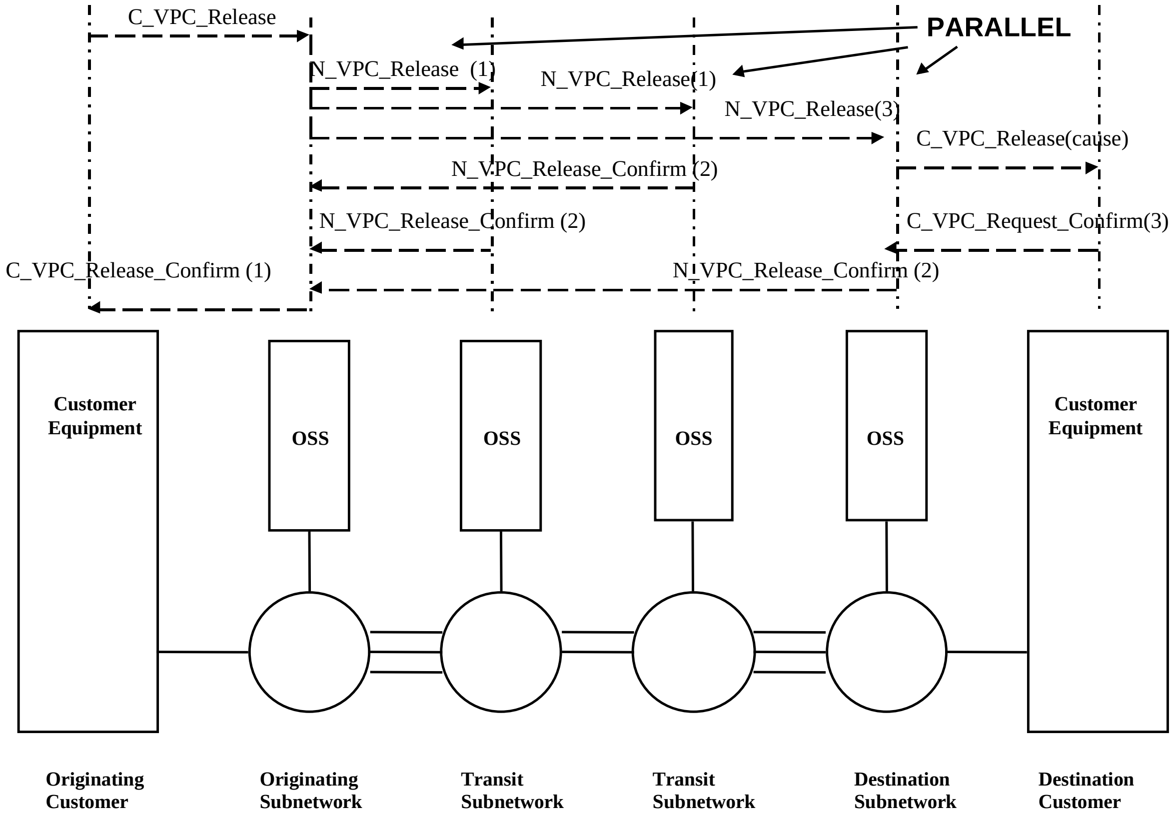


Figure A.8: Release (Explicit Request from the Originating User)

Case (ii), see figure A.9: the destination OSS, at the reception of the C_VPC_Release/C_VCC_Release message, will answer to the destination customer with a C_VPC_Release_Confirm/C_VCC_Release_Confirm. This OSS will also issue a N_VPC_Dest_Release/N_VCC_Dest_Release message to the originating OSS. The originating OSS will issue a C_VPC_Release/C_VCC_Release message to the originating customer, and a N_VPC_Release message to the transit and destination OSSs. All the OSSs involved in the connection will release the network resources allocated to the VPC/VCC, answering with a C_VPC_Release/C_VCC_Release.

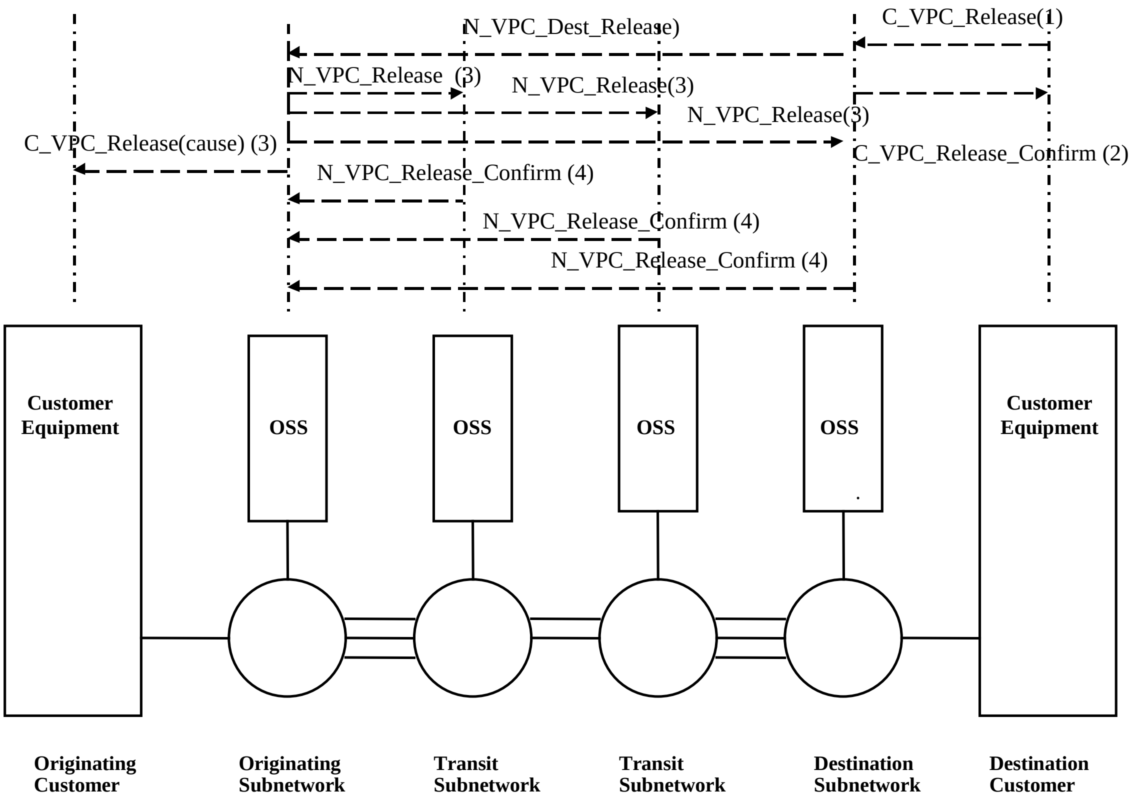


Figure A.9: Release (Explicit Request from the Destination Customer)

Case (iii), see figure A.10: the originating OSS starts the release procedure (because the subscription duration has expired). The originating OSS will issue a C_VPC_Release/C_VCC_Release message to the originating customer. This OSS will also issue, in parallel, a N_VPC_Release/N_VCC_Release message to all the affected OSS. The transit OSS will release all the network resources allocated (activated or reserved) to this VPC/VCC. The destination OSS will, additionally, send a C_VPC_Release/C_VCC_Release message to the destination customer including the cause of the release.

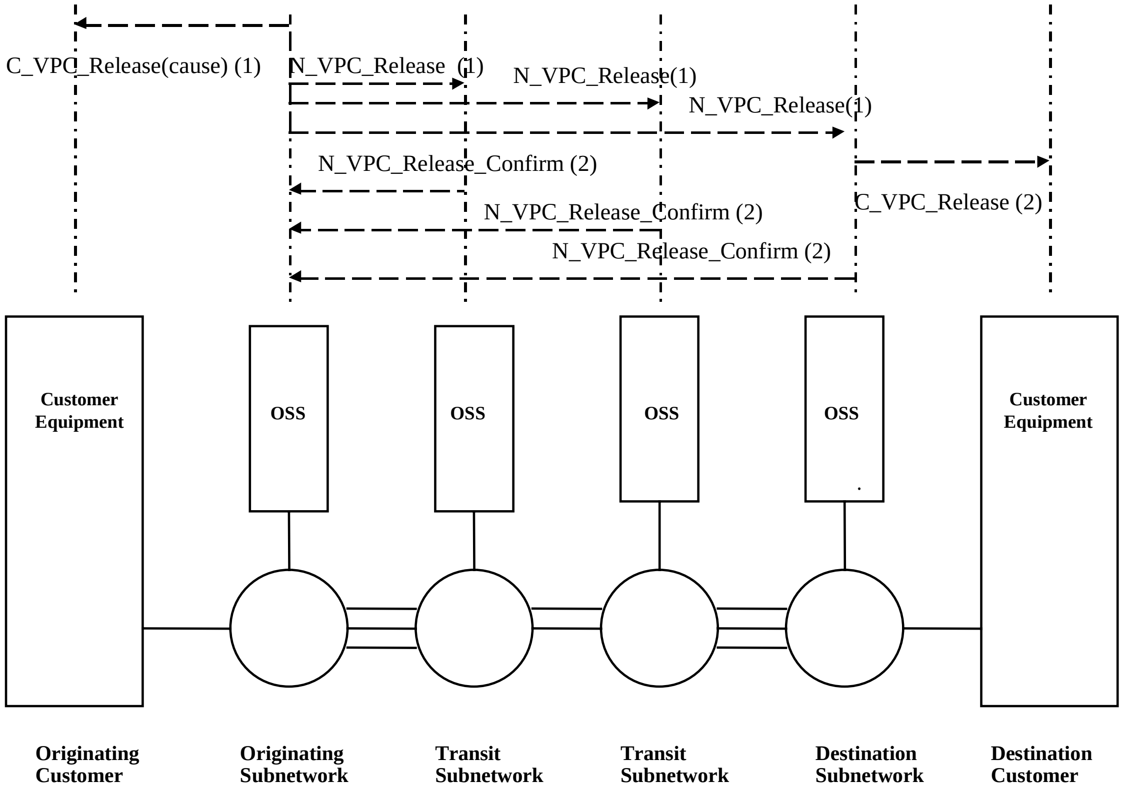


Figure A.10: Release (Implicit Request from the Originating Subnetwork)

Case (iv), see figure A.11, the originating OSS starts the release procedure (because of a non recoverable failure). The originating OSS will issue a C_VPC_Release/C_VCC_Release(Cause: Fault_Non_Recovery) message to the originating customer. This OSS will also issue, in parallel, a N_VPC_Release/N_VCC_Release message to all the affected OSSs. The transit OSS will release all the network resources allocated (activated or reserved) to this VPC/VCC. The destination OSS will, additionally, send a C_VPC_Release/C_VCC_Release message to the destination customer including the cause of the release.

In all cases, at the end of the release procedure, the VP/VC connection id will be no longer valid *and may be recycled*.

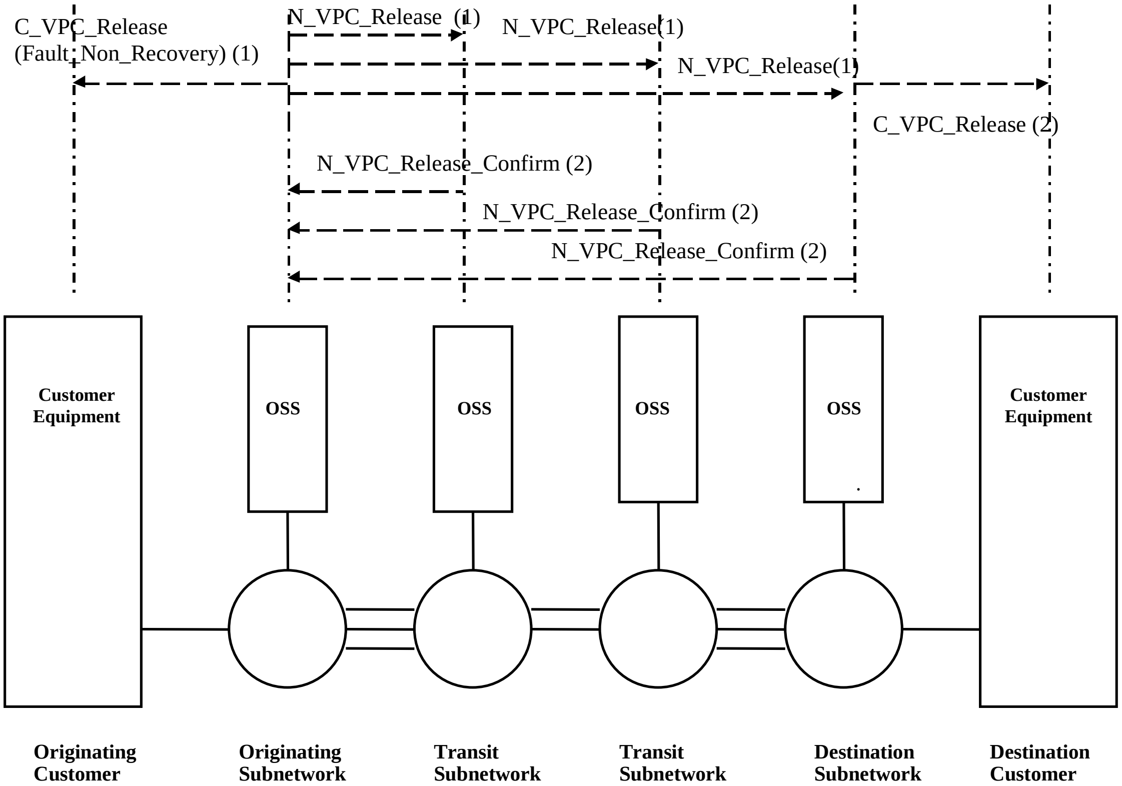


Figure A.11: Release (Implicit Request due to a non Recoverable Failure)

A.2.5.8 Inter-Subnetwork Routing Criteria

The routing of the VPCs/VCCs established through several Subnetworks is based on the following criteria:

In the Pan-European ATM Network it has been suggested that a maximum of two transit Subnetworks should be involved in a VPC/VCC. However the previously specified network processes have been defined without any restriction in the number of transit Subnetworks.

The VPC/VCC routing for establishment and reconfiguration is based on the source handling assumptions mentioned in subclause A.2.5.3.1. This implies that the OSSs of the transit subnetworks cannot modify the route proposed by the originating OSS.

The originating OSS will choose the route taking into account economical criteria basically. Normally it means to minimize the number of transit Subnetworks, but particular agreements among the operators of the Subnetworks could modify this "shortest path" criterion.

A.2.6 ATM Provision Request Information Forms

The following forms are taken from JAMES Forms annex G EAP 1 through 4 + scheduling forms EAP 6 through 9. It is proposed that when using a manual X.easi interface, for ATM interconnect service operation processes, that these forms should be used. They also provide the essential requirements for the information to be exchanged over automated or semi-automated interfaces. Many of the identifiers and parameters need to align with the recommendations in annex B.

Provide/Cease/Regrade/Rearrange		
Order Reference Number *To be agreed by account teams*		
Customer AddressPNO A	*Changed for re-arrangement (Yes/No)*	
Customer AddressPNO B	*Changed for re-arrangement (Yes/No)*	
Time and Date Order Details Agreed *To be agreed by account teams*		
Circuit Identifier		*Time and date complete*
Gateway VPI/VCI		*Time and date complete*
Agreed regrade time *For regrades only*		*Time and date complete*
End to end commissioning complete		*Time and date complete*
Correspondent Confirmation of Configuration Signed Time/Date Problem Details		
PNO A Confirmation of Configuration Signed Time/Date Problem Details		
Filing Reference		

A.2.7 Capacity Management Processes

Refer to text in the main part of the present document

A.3 Fault Localization and Repair

Fault localization and repair processes need to take account of the topology of the ATM PVP/PVC. Possibilities include a bilaterally provided circuit, or a multi-laterally provided circuits which involves the use of transit connections.

A.3.1 Maintain and restore processes

The following subclauses describe how it may be possible to implement the repair process using the exchange of alarm reports or trouble tickets. Alarm report provide and indication of the technical state of a resource and are generally suited to assist repairs at that operations level. Trouble tickets record information about the progress of the repair processes, escalations, and the contact point in the PNOs. They are suitable for both the service management and operational network management levels.

A.3.1.1 Overview of Fault Management

Sources JAMES O&AM 4.1 through 4.3.

There are basically, two types of fault, transmission and the equipment types.

Faults caused by troubles at the ATM Layer are accommodated in the optional "VPC Restoration/Reconfiguration Procedure" discussed in subclause A.2.5.6.

A.3.1.2 Transmission failure

The transmission failures are considered at the Physical Layer. Each ATM operator is expected to manage internally this type of faults. Such a problem must be automatically transmitted to the appropriate internal operational staff for correction.

Optionally the internal trouble tickets recording the presence of these faults may be notified immediately to other PNO's whose connections are affected by these faults. The trouble ticket information contents are described in subclause A.3.6.1.

However, should the fault be present in excess of 90 minutes during "working hours", a message should be sent to all the others PNO having VP concerned by the failure, to notify the estimated duration of the break. This could be in the form of a trouble ticket open notification where automated Trouble Ticket interfaces are used [28].

This is to allow to the other ATM operators to update their routing plans and advise their local customer.

A message of restoration will be send when the transmission facility is available again.

A.3.1.3 Equipment failure

Each ATM operator is expected to repair the equipment failures in the shortest possible time.

If the default has an effect on the subnetwork operation for more than 30 minutes, a message will be sent to all the other PNOs having VPs affected by the failure, to notify the estimated duration of the break. During working hours, this message should be sent out within 30 minutes, otherwise as soon as possible the next morning.

This is to allow to the other ATM operators to update their routing plans and advise there local customer.

A message of restoration will be sent when the subnetwork is available again.

A.3.1.4 Planned interruption of service

In case of a planned interruption, information about the interruption should be distributed to all PNOs who support the affected Connection Identifier.

This should be in the form of a Trouble Ticket. The information that should be made available is described in subclause A.3.6.1.

A.3.1.5 General Repair Principles

The fault localization and repair process is based upon the following principles and agreements:

i) Customers will report faults to their own PNOs customer reporting points referred to PNO A's Service Management Centres (SMC), who will contact one another, as appropriate, to ensure the effective service management of the customer.

ii) Operationally, the PNO A's Inter-operator Operations Centre (IOC) and the other PNO's (Correspondent) IOC will be the single points of contact for the repair of ATM services between PNOs.

iii) The "end to end" circuit identifier will be that generated during the provision process.

iv) For customer reported faults, both operators will prove the fault off their network before contacting the other operator for co-operation.

v) The preferred method of contact will be automated electronic exchange of trouble ticket information, whilst noting that a manual exchange is the mandated minimum capability.

A.3.1.6 Repair response targets

i) Both PNOs operate a 24 hour maintenance unit in support of the service.

ii) ATM Correspondent Services require an end to end Time to Restore of 12 Hours. To cope with practical cases where diagnosis is needed by both PNOs, each PNO should have an internal target of 5 hours for the Time To Restore customer service. This is based upon the assumption that initial diagnostics can prove a fault onto the correspondent network within 1 hour. This then requires each Correspondent Operator to restore service within their own network within 4 hours.

Customer demand is likely to require considerable shortening of these times in Phase 2.

A.3.2 Overview of M & R Procedure Phases

The repair process is divided into three main phases.

Fault Reception

As a single point of contact all faults which affect a PNO's customer service will be reported, to the PNO Service Management Centre. The faults will be logged and tracked in the PNOs local Trouble tracking/ticketing systems. The fault reports can originate from:

- a customer;
- another PNOs SMC or OSS;
- the Inter-operator Operations Unit (IOU);
- the Element Manager Alarms;
- correlate and diagnose.

Once the faults have been reported and logged the PNO IOU will carry out low level fault diagnostics to determine the reason and possible solutions to the fault. This may require co-operation with other internal units within the PNO. Once the reasons for the fault are known the IOU will ALWAYS inform the customer and other PNOs IOUs, if applicable.

Information given will include:

- a fault identity;
- the affected resource/connection identity;
- the cause;
- the start and estimated duration of the fault;
- restore.

Once the diagnostics have proved where the fault lies action is taken to rectify the fault. This may involve tasking other PNO operational unit or the equipment supplier.

Reconfigure

If a fault cannot be resolved within a reasonable period of time then the VPC/VCC can be reconfigured to provide service.

Release

If it is not possible to reconfigure a VPC/VC for whatever reason the VPC/VCC will be released.

A.3.3 Bilateral Fault Reporting

A.3.3.1 Bilateral

The following process steps should be followed:

A.3.3.1.1 Customer or Other PNO Reported Fault

Figure A.12 shows the high level processes used to handle faults reported by a customer or another PNO. The other PNO could be the originating or destination PNO depending on who is designated as the controlling end. Normally the Originating PNO will be designated as the controlling end and hence be PNO "I".

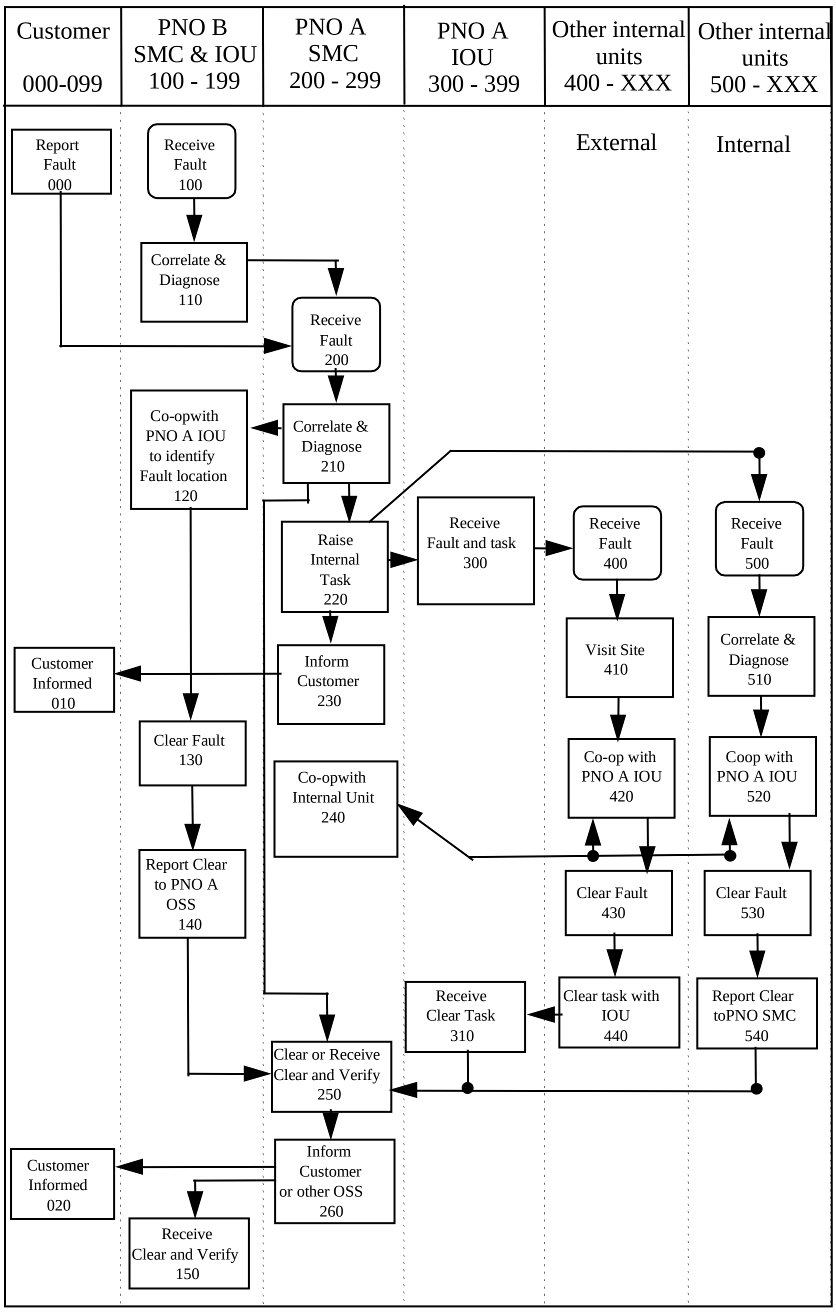


Figure A.12: Customer Reported Fault or Other PNO

i) Customers will report their faults to their normal fault reporting points (SMCs) using business as usual processes.

ii) Should the Correspondent Service Management Centres wish to inform their opposite numbers of the fault report or request updates at any time, they will use the contact numbers which are recorded in the completed OCPT.

iii) Upon receipt of a fault relating to an International VP/VC terminating in the either PNO's network, both operators will endeavour to locate and fix the fault using existing processes and processes. Both PNOs will prove the fault to be off their own network before contacting the other operator for co-operation.

iv) Should the fault prove to be from within the PNO network where the fault was reported, that operator will inform the other correspondent PNOs of the fault localization.

v) PNO A will contact the Correspondent Inter-operator Operations Centre (IOC) quoting the circuit identity, the nature of the fault, and a fault reference number. A follow up may also be sent for confirmation or to provide some additional information. PNO A's IOU will then update the PNO B's IOU and its own SMC every 30 minutes until the fault has been cleared.

PNOs should carry out proactive fault reporting, updating other PNOs who co-operate in providing the affected Connection.

vi) Should the fault prove onto the International link or the Correspondent Network, then the PNO A's IOU or the Correspondent's IOC will be contacted quoting the agreed circuit identifier. An internal target of ONE hour for initial diagnostics is needed for proving the fault on to the correspondent network.

vii) Once the PNOs have accepted a fault as being in their network or the international link, they will supply a trouble ticket reference number. A follow up communication may also be sent for confirmation or to provide some additional information.

viii) Upon acceptance of a fault, PNO A IOU will enter the fault description on to a local trouble ticketing system which will normally automatically generate a reference number. This number will be quoted to the Correspondent IOU upon acceptance of the fault. PNO A will then update the other PNO's IOU and its own SMC every 30 minutes on progress until the fault has been cleared.

ix) Once the fault has been cleared, the IOU of PNO resolving the fault will inform the Correspondent IOC of the clear and given a brief description of the nature of the fault and the corrective action taken. The customer will then be informed using business as usual processes using the appropriate SMCs.

A.3.3.2 Network Reported Fault and Pro-active Reporting

Figure A.13 shows the high level processes for handling network reported faults and the pro-active reporting which is required to support the repair. (This figure and the associated proposed processes are based on experience in the JAMES project and also with one operator's existing processes.)

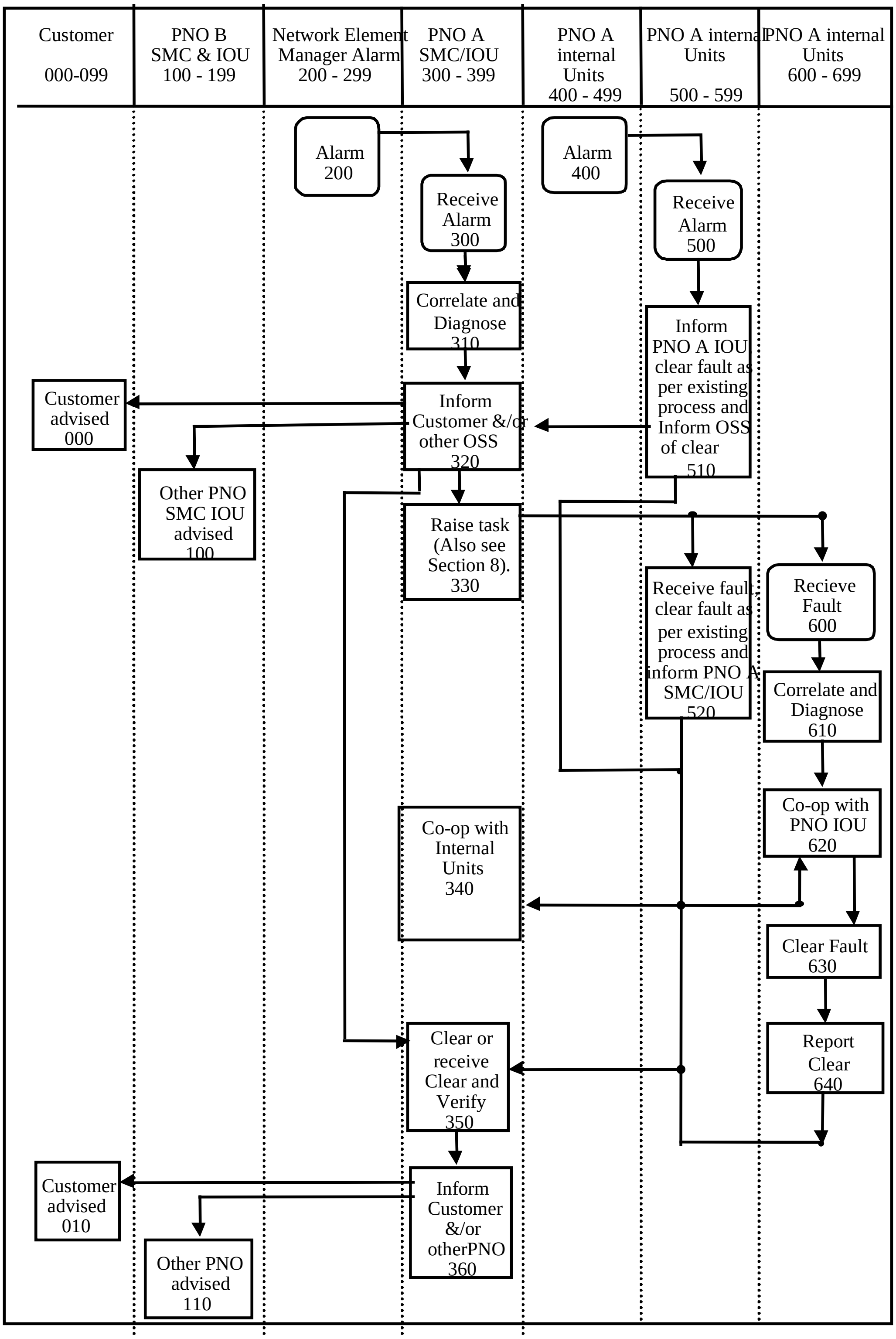


Figure A.13: Network Reported faults and proactive reporting

Both PNO's IOUs will both actively monitor their own networks for alarms and clear any faults that occur within there own subnetwork.

Should a fault or alarm occur on a PNO's Network that is known to affect service to customers terminated on a correspondent PNO network, then those PNOs should be informed of that fault and the circuits affected.

The reporting PNO A's IOU will contact the Correspondent IOC quoting the circuit identity, the nature of the fault, and a fault reference number. A follow up may also be sent. PNO A IOU will then update the correspondent PNO's IOC and their SMC every 30 minutes until the fault has been cleared.

A.3.3.2.1 Fault Reported By Transit PNO

Figure A.14 shows the approach to be adopted in repairing faults in circuits which have a transit PNO.

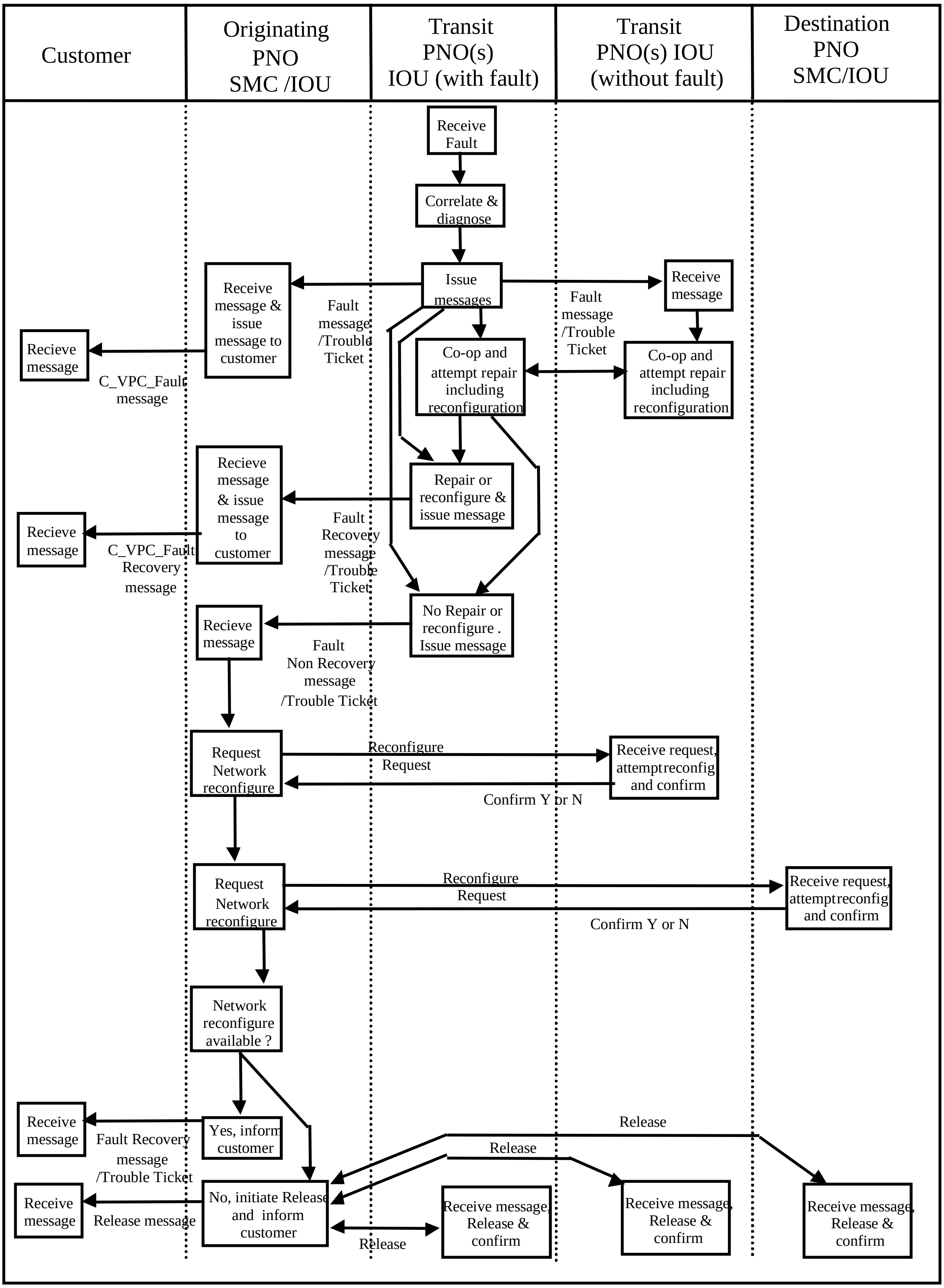


Figure A.14: Fault Reported By Transit PNO

The key procedural policy is that the Originating PNO acts as the controlling end to co-ordinate the repair procedure.

Communication between the PNO can be by either alarm reports or Trouble Tickets.

The procedure above also shows the use of reconfiguration to recovery from a fault. This is optional in Phase 1 and may not be supported by all PNOs.

A.3.4 Planned Engineering Works

There is a need to understand the internal time windows for planned works within both interconnected operators so an acceptable agreement can be reached both for internal planned works and those where co-operation between the operators is required. Planned (and indeed non-planned) engineering works are one of the reasons for requiring a Trouble Ticketing function for the X.easi management interface. Refer also to subclause 9.3 of the present document.

For example the agreed planned work time window for ATM within the UK is Sunday 0400 - 0630 local time. Agreement on customer outage for breaks in service greater that 10 seconds is required. The customer requires a minimum of 14 calendar days notification.

Typically customer can insist upon a minimum of 72 hours for emergency planned work.

The following critical process steps are required:

i) Upon notification of an internal network planned work, both the PNOs will ascertain if any international circuits are affected. The PNO's SMC/ IOU will encourage those customers affected to gain agreement from the distant end prior to agreeing the planned work. Once agreement has been reached, the respective IOU Maintenance Centre will telephone and/or fax the other operator and inform them as a matter of courtesy, not for agreement, as this should have already been obtained from the distant end customer.

ii) Upon receipt of a planned work notification, PNOs will inform those customers affected using internal business as usual processes.

iii) For emergency situations, the originating PNO will inform affected at the earliest opportunity.

iv) For planned work on the link or International Gateway when there is a need for co-operation between the PNO's, then this is treated as an emergency planned work and will be arranged between PNO's IOUs. A time is arranged which is convenient to both companies and the customers.

Contacts point for planned work escalations should be entered in the completed OCPT.

A.3.5 ATM Fault Localization, Repair and Planned Work Management Escalations

A.3.5.1 Service Management Escalations

In the event of a breakdown in communications, failed repair targets etc., contact points are provided for escalation within PNO the Service Management Centre (SMC) **at the service management level.**

The first level escalation should normally be the manager for the Service Management Centre. Each escalation should move at least one stage up the internal reporting structure of the PNO.

NOTE: 4th level is the highest level.

PNOs should record in a OCPT the Maintenance and Restoration escalation contact points covering names telephone , fax and e-mail ids.

Where multilateral provisioning has been used the organization carrying out the lead role in either one stop shopping or a co-ordinating role should act as the point of escalation for all of the co-operating PNOs. This avoids the need for each organization to hold escalation contact details for all of the co-operating PNOs.

A.3.5.2 Operational Management Escalation

Should events such as a breakdown in communications, failed repair targets etc. contact points are provided for escalation PNO IOUs **at an operational level.**

The first level escalation should normally be the manager for the Inter-operator Operations Unit (IOU). Each escalation should move at least one stage up the internal reporting structure of the PNO.

NOTE: 4th level is the highest level.

PNOs should record in a OCPT the Service provisioning escalation contact points covering names telephone, fax and Email ids.

Where multilateral provisioning has been used the organization carrying out the lead role in either one stop shopping or a co-ordinating role should act as the point of escalation for all of the co-operating PNOs This avoids the need for each organization to hold escalation contact details for all of the co-operating PNOs.

A.3.5.3 Testing Facilities

To aid fault localization, the following test facilities should be provided:

i) Virtual loops will be placed at the respective international gateway switches. These will allow PNOs to transmit on VPI/VCI 0, 30 and receive on 0, 31. Similarly the PNO switch will be looped to allow Correspondent Operator's to transmit on VPI/VCI 0, 28 and receive on 0, 29.

ii) Virtual loops will also be placed within the operators network, Location XX for PNO A and XXXX for the Correspondent Operator. The loopback values will allow PNO A to transmit on VPI/VCI 0, 26 and receive on 0, 27. Correspondent Operators will transmit on VPI/VCI 0, 24 and receive on 0, 25.

iii) Each PNO will be able to use the loops for whatever purpose they choose, e.g. racetrack, test call loops etc. the circuits will be set up as CBR.

iv) Each PNO will place a router in their network to allow the other operator to "Ping".

The IP address of the router in the PNO networks is recorded in the Operational Contact and Procedures Template.

A.3.6 Fault Management Information Forms

These are derived and adapted from JAMES O&AM form 5 James Fault management annex B and other correspondent operational forms.

Note that the complete specification of the Fault management function of the X.easi interface should include ATM VP/VC alarm reporting as well as Trouble Ticket reporting.

The following two subclauses will need to be rationalized as they contain the original JAMES Proposals and the updated proposals.

A.3.6.1 Trouble ticket information for Fault and Maintenance

Trouble [ ] **/ Maintenance** [ ] **nat.Ref. No:**	
Originating PNO of the trouble ticket: PNO: ____________________ Fax: ____________________ Tel: ____________________	**Creation date:** date: ____________________ time (UTC): ____________________ Name: ____________________
Fault detection/Start of Maintenance activity: date: ____________________ time (UTC): ____________________	**Closing time/End of Maintenance activity:** date: ____________________ time (UTC): ____________________
Ticket status (only for trouble tickets): [ ] OPEN [ ] CLOSED	**Expected duration for the maintenance activity** time (hours:minutes:seconds): ____________________
VP/VC connection identifier: ____________________	**Malfunction description:** *(Only when the originating PNO of the trouble ticket cannot specify a fault class identifier)* ____________________ ____________________ ____________________ ____________________
Fault class identifier/Network resource involved (#2,#3): [ ] F#1 (int. VP/VC Connection) [ ] F#2 (int. Physical Link) [ ] F#3 (int. ATM Gateway) [ ] F#4 (nat. ATM subnetwork) PNO 1: ____________[ ] OK [ ] NOK [ ] CLEARED PNO 2: ____________[ ] OK [ ] NOK [ ] CLEARED PNO 3: ____________[ ] OK [ ] NOK [ ] CLEARED PNO 4: ____________[ ] OK [ ] NOK [ ] CLEARED PNO 5: ____________[ ] OK [ ] NOK [ ] CLEARED PNO 6: ____________[ ] OK [ ] NOK [ ] CLEARED	**Location or int. transport link:** *(Only for fault classes: F#1, F#2 and F#3).* ____________________ Fault end of each PNO: Date:__________ Time:__________ Date:__________ Time:__________ Date:__________ Time:__________ Date:__________ Time:__________ Date:__________ Time:__________ Date:__________ Time:__________
Comments and further information	

A.3.6.2 Trouble and Maintenance ticket information

It is the aim to create one ticket for both purposes, a trouble ticket for fault handling, as well as a maintenance ticket for planned outages.

The fields included in the ticket are defined as following:

Trouble [ ]/Maintenance [ ]:

Usage of the ticket form. If the ticket is used as a trouble ticket, then the trouble field should be marked.

Due to this field it is possible to use the same form for both purposes.

nat. Ref. No:

The originating PNO of the ticket should give its Carrier Code, which identifies the trouble or maintenance activities in the JAMES network.

Due to this reference number, each PNO can locate the same fault/maintenance activity.

The national reference number gives a relationship between the trouble or maintenance activity in the JAMES network and the national used data bases.

Originating PNO of the trouble ticket:

Name, fax and phone number of the PNO which opens the ticket.

Creation date:

Date and time, when the ticket is created. The field name identifies the representative of the ATM staff.

Fault detection/Start of maintenance activity:

The time when the malfunction has been detected (usage as trouble ticket) or the date and time when the maintenance activity will be started (usage as maintenance ticket). It will be filled out by the originating PNO of the ticket.

Closing time/End of maintenance activity:

The time when the trouble ticket has been closed or the date and time when the maintenance activity will be finished (usage as maintenance ticket). It will be filled out by the originating PNO of the ticket.

Ticket status:

This field is only important for the usage as trouble ticket. For maintenance activities the ticket will be used as an information for the involved PNOs. Due to this fact it is not necessary to send two times the information for a maintenance activity.

The ticket status is set to OPEN, when a fault is detected. It is set to CLOSED when the fault is cleared and, when applicable, a confirmation of the recovery of the service was received from the user.

This field has been filled out by the originator of the trouble ticket.

Expected duration for the maintenance activity:

This field will be mainly used for maintenance activities. It should give the information how long the maintenance activity will probably last during the time window given at the top of the ticket (start and end of maintenance activity).

The time should be inserted in the form "hours:minutes:seconds".

VP/VC connection identifier:

A number of 12 digits assigned by the originating OSS of the VP Connection affected by the fault. It is the same value of the VP/VC connection identifier used in the forms exchanged by fax or automated scheduler system between the PNOs during the establishment phase of the connection.

Malfunction description:

A description of the detected malfunction.

Fault class identifier/Network resource involved:

While usage as trouble ticket, this field specifies the fault class and the fault status in each involved PNO.

while usage as maintenance ticket, this field specifies the network resource involved in the planned outage, i.e. the international physical link or the international ATM Gateway.

Location or int. transport link:

It describes the location of the fault, e.g. "Network side", "User side" or the link designation.

During a fault of the international transport link, the bearer should be inserted in this field, according to the ITU-T Recommendation M.1400 [13].

Fault end of each PNO:

Each PNO should give the date and time, when the trouble was solved in its own entity. This time could be different to the closing time of the trouble ticket.

Comments and further information:

This field gives the technicians the chance to write important information, necessary for the trouble shooting activities.

A.3.6.3 Trouble Ticket for planned interruption of service

The following was the original JAMES Trouble Ticket proposals for planned interruption of service.

Ticket Status:	If you plan an interruption, you must mark "Open". If you have finished an interruption, you must mark "Closed".
Country Code:	e.g. Austria "43" => 043
PNO Code:	Code that is used for JAMES. (e.g. Austria "APTT" => XAPTT)
Creation Date:	Date and time when the ticket was created. (e.g. 96/12/17 10:30 UTC)
Ticket Source:	Office where the ticket was created (operational centre). (e.g. OSS: B-ISDN-NMOC)
Phone:	Telephone - Number of the operational centre. (e.g. Austria => + 43 1 79744 3240)
Fax:	Fax- Number of the operational centre. (e.g. Austria => + 43 1 79744 3232)
e-mail:	E-mail address of the operational centre.
Ticket Owner:	Name of the person who created the present ticket.
Ticket Type:	for Maintenance, If it is regular planned work, the announcement should be sent **more than 7 days** to the other PNOs !! "Urgent" should be marked, if there are less then 7 days left for the planned interruption. (This situation should be avoided !!)
Ticket Scope:	Line: Which line (from-to) has an interruption? (One line consists of one or more links)

	Link:	Which link (line, from-to, number of the link) has an interruption?
	Switch:	Which switch (site) has an interruption?
	etc.:	any other causes

Type of Connection: Type of connection that is planned to interrupt.

Total capacity which is lost.

Alternatives: Maybe there is a possibility to reroute the connection.

If it is possible you should name the total capacity of these alternatives.

If the Ticket Status is "**open**":

Start of Interruption: Date and time when the interruption will start.

End of Interruption: Date and time when the interruption will end.

If the Ticket Status is "**closed**":

Start of Interruption: Date and time when the interruption has precisely started.

End of Interruption: Date and time when the interruption has precisely ended.

Annex B (informative): Phase 1 Proposals for X.easi management Identifier Schemes

B.1 Introduction

B.1.1 Overview

This annex provides an initial proposal for a model of the entities which need to be identified across the X.easi interface and describes the specific identifier schemes that may be used to unambiguously identify instances of each type of entity, and some of their attributes. In some cases these are also referred to in the industry as "designations". It also provides a high level logical model to show the naming relationships amongst these entities which is essential to ensure that a complete and unambiguous scheme has been produced.

The models provided in this annex are based on a list of Requirements (subclause B.1.2) which have been identified as being essential for defining a scheme for network management identifiers and addressing, where pertinent for ATM interconnect service introduction and operation. In all cases the information provided relates to network management of resources identified in the ETSI EASI specification for the "User and Control Plane" [1].

In this annex, the term "PNO" is used to mean any interconnected operator and is chosen to maintain consistency with the object nomenclature of registered Managed Objects and Attribute names in some of the relevant standards.

B.1.2 Requirements for X.easi Management Identifier Schemes

The following list of Requirements for X.easi management identifier schemes has been established. Proposals for solutions relating to these requirements are to be found in this annex:

For management of ATM interconnect services, there is a requirement to be able to uniquely identify the addresses of all operators and associated entities using an addressing scheme which does not rely solely on the operator's Country Code.

To exchange information in a standardized way with both the static items (including Customer's interface, Subnetworks and inter-Subnetwork Links) and the dynamic items (including VPCs and VCCs) identified uniquely and unambiguously.

To be aware that ITU-T Recommendation M.1400 [13] provides the basic foundations for administering codes which uniquely identify the operating company.

To note that for Phase 1, operators are restricted to designate exactly one VP subnetwork and one VC subnetwork.

> **The identity of the customers (numbering plan) should be dissociated from the identification scheme needed in the ATM management network in order to address the various network elements (ATM switches, connections, etc.).**

In an interconnected pan European ATM network there will be the need for VPC and VCC identification in order to complete the storage in the management network of the information related to a virtual connection between two ATM network users.

Identifier schemes must be applicable to ATM VP logical links which have to be allocated by management to suitable physical transport resources. For example, in the case of SDH, the ATM VPs will have to be inserted in an available logical link (Virtual Container). Network management has to correlate objects belonging to the physical resources.

Due to the fact that two subnetworks can simultaneously allocate the VPI's of the Logical Links which interconnect them, a VPI "collision" could occur. In order to minimize the probability of the simultaneous allocation of the same VPI to two different VPC's by two subnetworks directly interconnected, use of an appropriate algorithm is required:

> A list of OSI identifiers needs to be defined locally by each PNO and communicated to other PNOs to support interconnected ATM service introduction.

B.1.3 Entities for which identifiers are proposed

The entities listed in the bullets below have been derived from experiences described in the JAMES project. For the JAMES project, a simple assumption was used that the Country Code = the Operator (e.g. 44 = BT). This is totally unsatisfactory for an operational situation in the multi-operator environment (e.g. 44 means all licenced operators based in the UK). There is therefore a requirement to be able to uniquely identify the addresses of all operators and associated entities (as listed in the bullets below) using an addressing scheme which does not rely solely on the operator's Country Code.

The entities for which identifiers are proposed are:

- PNO
- Subnetwork
- Customer
- End to End Virtual Path Connection (across several subnetworks)
- End to End Virtual Circuit Connection (across several subnetworks)
- Internetwork ATM logical link - both Virtual Path and Virtual Circuit level
- pno Virtual Path Subnetwork Connection (pnoVpSubnetworkConnection) identifier (for connections within one subnetwork)
- pno Virtual Circuit Subnetwork Connection (pnoVcSubnetworkConnection identifier (for connections within one subnetwork)
- pno Virtual Path Connection Termination Point (pnoVpCTP)
- pno Virtual Path Connection Termination Point (pnoVcCTP)
- Virtual Path Trail Termination Point (VPTTP)
- VP Link Connection
- Inter subnetwork Physical link - pnoNWpnoAtmAccessPoint, interPnoTopologicalSubnetworkPair
- Operations Support (OS) systems
- OSI applications

The definitions and relationships between the managed object classes which correspond to the list of entities in the bullets above is described in annex C, clause C.4 and figure C.2 in particular. This is mainly based on definitions in [6]. VP Link Connection is an additional object class which may be defined as the entity which connects two subnetworks where the VP identifier is terminated or translated. It represents the part of the overall connection that runs over an Inter-PNO Physical Link.

The list of entities is indicative and may be added to or deleted from during implementation of the X.easi specification.

B.1.4 Purpose of the management identifier schemes

There is a need to exchange information in a standardized way and the possible evolutionary steps, both the static items (Customer's interface, Subnetworks and inter-Subnetwork Links) and the dynamic items (VPCs) should be unambiguously identified.

This annex should be used to guide the procedures and algorithms used for generating unambiguous entity identifiers for use with the X.easi interface management systems and operational procedures.

Identifiers are needed to populate attributes within instances of managed object classes that are referenced by OS applications though relationships called Name Bindings; these must be unambiguous to ensure correct operation of the applications. There may be a need to provide the identifiers with "user-friendly" names which are different from formal name-bindings. The reason is that in some cases these identifiers are also used by human end users and must therefore be man-readable, and integrate with the current operational procedures used for international network management.

B.2 Administrative Identifiers

B.2.1 PNO Identifiers

ITU-T Recommendation M.1400 [13] provides the basic foundations for administering codes which uniquely identify the operating company. In reference 22 of [13] it identifies the ITU-T Operational Bulletin as the definitive source of Carrier Codes which are updated periodically.

These can be obtained electronically from the ITU-T web site: www.itu.int.

Examples of these Carrier Codes are shown in table B.1:

Table B.1: PNO Identifiers based upon ITU-T Recommendation M.1400 Carrier Codes

ISO Country CODE	PNO NAME	PNO Identifier =Carrier Code
FRA	France Telecom	FT
AUT	PTA	AUPTT
BEL	Belgacom	BGACOM
GBR	British Telecom	BTPLC
DEU	Deutsche Telekom	DTAG
CHE	Swisscom	CHEPTT
IRL	Telecom Eireann	EIREAN
PRT	Portugal Telecom	PT
ITA	Telecom Italia	TI
FIN	Telecom Finland	TFIN
ESP	Telefonica	TFCAES
NOR	Telenor	TELNOR
SWE	Telia AB	TELIA
FIN	Finnet	FINNET
LUX	PTT Luxembourg	EPT
GRC	OTE	OTE
NLD	PTT Telecom Netherlands	TCOMNL
DNK	Telecom Denmark	TD

There is considerable advantage to having an internationally recognized PNO identifier since it can be used within other identifiers to allow individual operators to generate independent unique or unambiguous identifiers without needing to operate a central registry collectively with other operators. Communication of identifiers is simply a matter of bilateral agreement and publication.

However, an example of the limitations which can be found is that there are currently only three PNOs, based in the UK, with ITU-T carrier codes although any company can register with ITU-T for such an identifier. Clearly, the maintenance of lists of carrier codes in a rapidly-developing market is an addressing-related issue which requires a workable solution.

Some technical issues may arise in terms of the use of ITU-T carrier codes for identifiers and increasing numbers of such identifiers in the developing multi-operator market, e.g.: The maximum length of a carrier code in the ITU-T scheme is 6 characters and this may need to be added to a country code. Such a combination of codes may be used to create a unique PNO identity but the extended length may cause difficulty in the use of M.1400 [13] . This requires some checking with ITU-T SG 4.

B.2.2 Subnetwork Identification

For Phase 1 Operators are restricted to designate exactly one VP subnetwork and one VC subnetwork. However the following proposal for an identifier structure has been chosen to make the extension to additional subnetworks a possible enhancement for later ATM service introduction phases.

These subnetwork identifiers will be needed to construct the attributes in the following table. For network management, the attributes belonging to the related Managed Objects should point at subnetworks and therefore the subnetwork identifier is needed:

Managed Object	Attribute
InterPnoTopologicalSubnetworkPair (Describes the link between subnetworks)	SubNetworkPairId (describes which subnetworks are linked)
pnoNWAccessPoint	AssociatedSubNetworkPairId (Describes for which pair the accesspoint is a part of)
PnoVpSubnetworkConnection (Describes the Vp connection within one subnetwork)	InitiatingPnoSubnetworkId (Describes which operator has set up the connection)

The recommendation is to construct the SubnetworkId, in an "ITU-T Recommendation M.1400 [13] style" as follows:

PNO identifier Carrier code. E.g. ITU-T carrier code + country code	Char "-"	Local name Max. 15 characters	Char "-"	Sub network type M.1400 [13] Function Code e.g. VPA or VCA

The local name is selected by each PNO and may be different for the VP and VC subnetworks. The concatenation shown above can be used to create unique identifiers for PNOs and their subnetwork types.

Sub Network Pair Ids can then be constructed as follows:

PNO A SubnetworkId	Character (e.g. "-")	PNO B SubnetworkId

This is similar to the convention used in Project JAMES and related EURESCOM Projects.

B.2.3 Alternative Sub network identification scheme

In the JAMES project, an alternative Subnetwork Identifier scheme was proposed based upon the use of knowledge of the structure of the national significant number. It is probably unworkable in a operational environment because it assumes that PNO can control parts of the national number space. Given the new regulatory demands in Europe it is advisable not to depend on getting the mutual agreement of national number regulators in Phase 1 timescales.

For this alternative scheme, the identification of each network element will need a hierarchical structure in which the sub network identifier is the first part. The necessity of a geographical indication and the simplicity of the identifier should be the primary considerations. Since nationally, each operator will be assigned E.164 [44] numbering space identified by the leading digit(s) of the National Significant Number, it is possible to use such a part of the E.164 [44] number for subnetworks identification. In this case the subnetwork identifier structure is presented in figure B.1.

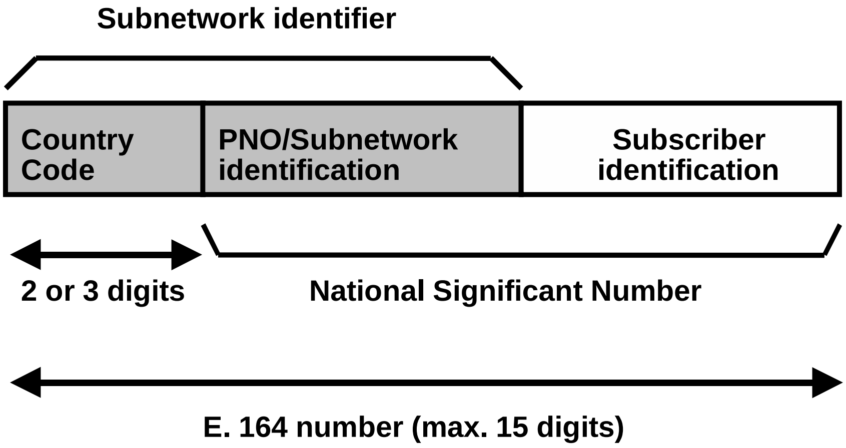


Figure B.1: E.164 Sub network identifier structure

As the composition of the leading part of the National Significant Number is a national matter, the use of this to identify ATM subnetworks is left for further study.

In general, the scheme described above does not seem to be adequate for the multi-operator environment, due to PNO's lack of control of the national numbering space. Accordingly, the scheme described in subclause B.2.2 is recommended as the basis of the subnetwork identification scheme. The scheme recommended in subclause B.2.2 would require all PNOs offering ATM interconnect services to register for an identifier with the ITU-T and to combine such an identifier with their country code at the top of the addressing hierarchy.

B.3 End Point identification

B.3.1 Preamble

The identity of the end points (numbering plan) should be dissociated from the identification scheme needed in the ATM management network to address the various network elements (ATM switches, connections, etc.). In this way it is possible to provide flexibility both to the users and to the network architecture. The proposed numbering plan and the identification scheme are summarized in this subclause.

B.3.2 Customers numbering plan and management network identification scheme

In the dialogue between the ATM network users and the Operation System (OS) it will be necessary to use numbering information such as the destination user number and the originating user number as well. A range of solutions will need to be adopted which accommodates the use of appropriate international standards.

It is proposed that Customer Numbers are formed as follows:

Initiating PnoSubnetwork Identifier As is proposed in subclause B.2.2	initiatingVpConnectionId	
	Name/Address Type	Customer identifier

Some points of clarification concerning connections to the customer are as follows:

> In management, the overall VP connection (end to end, across several subnetworks) is uniquely described by the pair: "InitiatingPnoSubnetworkId, InitiatingVpConnectionId
>
> This should be linked to the customer identity.
>
> InitiatingPnoSubnetworkId: Describes which operator has set up the connection.
>
> InitiatingVpConnectionId: Refers to the overall connection

It is proposed that the name/address type should include:

Name/address Type	Identifier value	Comment
E.164 [44] Address [44]	E.164 [44] -	the character "-" is used as a terminator max. no of characters 8 (including terminator)
E.191 [43] Address	E.191 [43] -	"
M.1400 [13]	M.1400 [13] -	"
AESA (note)	AESA-	"
Proprietary	LOCAL-	"

NOTE: *Use of the ATM Forum End System Addresses (AESA) appears to be required in order to precisely define the physical location of the end of the connection.*

A combination of E.164 [44] and E.191 [43] addresses and M.1400 [13] identifiers is required in order to define connection between the end-customers.

These identifications will be needed to construct the following attributes:

Managed Object	Attribute
pnoVpSubnetworkConnection	initiatingPnoSubnetworkId
	Initiating VpConnectionId
Managed Object	Attribute
pnoVcSubnetworkConnection	initiatingPnoSubnetworkId
	Initiating VcConnectionId

B.3.3 E.164 overview and E.191

In addition to E.164 [44] based numbering, the recommendations in [44] should be utilized where appropriate. This provides guidance, principles and requirements for addressing reference points located at customers' premises, servers allowing communications between terminals, applications and persons in B-ISDN networks. B-ISDN numbering and addressing is based on E.164 [44] . Additional numbering and addressing requirements not covered in E.164 [44] are described in E.191 [43] and should be considered as a modification to the E.164 [44] description in this and the following subclause.

Each PNO will be responsible for assigning the E.164 [44] number to its customers and also make these numbers public for all interconnected ATM Network users. In figure B.2 the E.164 [44] Customer identifier structure is presented.

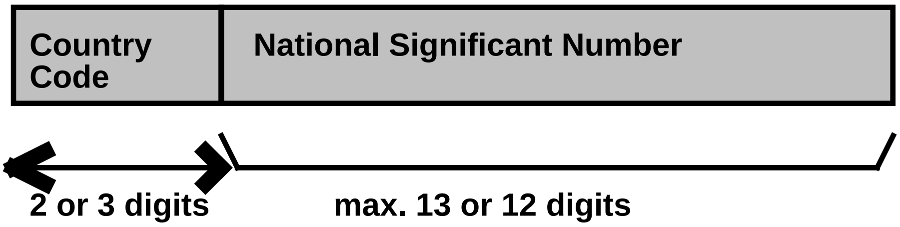


Figure B.2: Customer identifier structure

The composition of the National Significant Number is a national matter. The implication of this customer identifier structure is that ATM service addressing would look very similar to telephony addressing. Some further study is also required to establish whether there is duplication in the use of the country code between the unique subnetwork identifiers (discussed in subclause B.2.2) and the customer identifier.

It should be noted that for interconnected ATM service introduction in the near future, Number Portability will be a regulatory requirement for E.164 [44] telephony connections. Hence the initiating PNO has to carry out some checks on the number before being able to ascertain which PNO is servicing that E.164 [44] number or whether it has been ported to another PNO.

NOTE: The EU has directed that Number Portability shall be introduced before the end of the year 2000 for voice services. The E.164 [44] scheme above does not yet address number portability issues. The networking issues for Number Portability have been studied in the ETSI Number Portability Task Force and EURESCOM is studying the consequential implications for OS systems. (Refer to P908 documents.)

B.3.4 E.164/(E.191) based Customer Numbering

In the following discussion, the convention "OSS" is used to identify both Virtual Path and Virtual Circuit Operation Support Systems, since the convention may be applied to both.

E.164 [44] guarantees both backward compatibility and consistency for customers and network operators and there is sufficient flexibility within E.164 [44] to allow the introduction of new numbers to meet future requirements.

The OSS has to operate in order to establish ATM virtual path and circuit connections (VPC and VCC). For this purpose there is the need to identify objects inside the management network. It is important to note that such an identification scheme is pertaining to the OSS and in principle it is completely separated from the numbering plan of the ATM network users.

The ATM network user has to provide to the OSS information in order to establish a specific VPC or VCC. The destination user's E.164 [44] number, together with other additional parameters (schedule, etc.) will be used during the reservation phase for this purpose. Management information provided between the OSS and the user will provide the user with a virtual path identifier (VPI) to be used for that specific VPC as well as a VCI identifier when referencing a VCC. The VPI and or VCI value will be associated with the specific VPC and/or VCC at the ATM network user premises.

The E.164 [44] number has to provide the OSS all information needed for routing purposes and for the VPC and VCC set-up. The management flow communication between the OSS and the VPCC (Virtual Path Cross Connect) will identify the cross connects related to that specific VPC; Similarly communication between the OSS and the VCCC (Virtual Circuit Cross Connect will identify the cross connects related to that specific VCC. Cross-connect may be replaced by switch, if appropriate.

If the VPC/VCC is limited to one subnetwork it is solely the responsibility of a single OSS to collect the information necessary to establish the VPC/VCC. If more than one subnetwork is involved in the VPC/VCC there will be the need to identify the subnetworks (originating, transit and destination), the inter-PNO ATM logical links and the VPC/VCC itself involved in a standardized way which is described in subclause B.5.

B.3.5 M.1400 based Customer identification

The ITU-T Recommendation M.1400 [13], defines a general identifier, or named designator, for any kind of international physical link (analogue, digital, switched, leased, etc.). It has been recently extended to identify SDH end to end Virtual Containers and ATM end to end Virtual Paths and Virtual Circuits. In figure B.3, the form of layer 1 details of such a designator is presented [13]. (For the avoidance of doubt, note that the layer 2 specification described in [13] provides identifiers for carrier codes.)

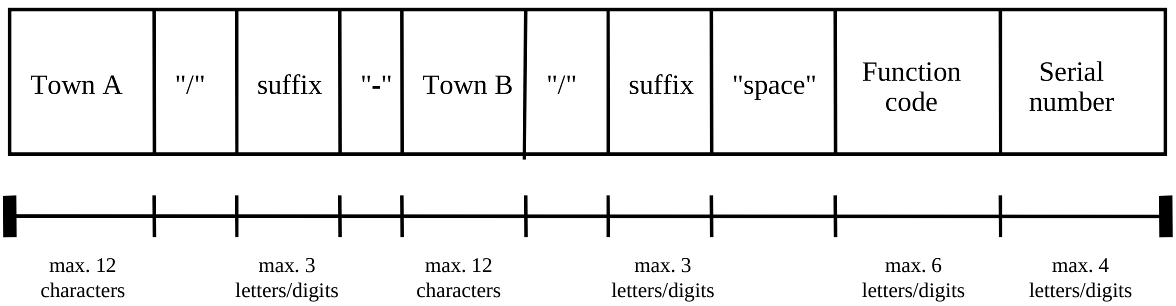


Figure B.3: M.1400 [13] Recommendation designators' general structure

The theoretical maximum length is 44 characters.

In the M.1400 [13] structure Town A and Town B represent the internationally unambiguous names of the towns which form the ends of the connection. Together with the suffix fields they unambiguously identify the international switches and the traffic relations of the connection route. The Function Code field defines the type of the route and the Serial Number distinguishes the specific route within the same traffic relation and same Function code. The Serial Numbers for Virtual Containers, ATM VP and VC, and the physical bearers are assigned independently.

For permanent connections - such as PVP and PVC - it is common operational practice for end to end circuit designation to be based upon these standards. Implicit in the M.1400 [13] designation is some information about the termination points and their location. Also implicit are the serving PNOs in the suffix field. The first town/PNO in the connection designation is usually the controlling end and is equivalent to the initiating (I) or access (A) PNO [6] for most practical ATM service provisioning. These designations are also used for transit PNOs which, from the M.1400 [13] designation (Town/suffix), can identify that neither initiating or terminating end is in within their domain and therefore confirm that the connection is a transit connection.

B.3.6 Local Schemes Customer identification

The purpose of the customer identification is simply to identify the end to end circuit and which PNO is controlling the establishment and release of the connection (i.e. the I-PNO role defined in [6]). It is possible that local designations can be used such as internal circuit or termination designations. It not recommended that this approach is used without explicit bilateral agreement.

B.4 End to end Identifiers

End to end identifiers and associated numbering schemes for VPs and VCs were described in subclause B.3, on the basis of using GDMO terms and descriptions. More generically, VPC and VCC identification should be defined unambiguously using the conventions shown in figures B.4 and B.5. In all cases there is a requirement for any pan European ATM network to assign unique VPC and VCC identifications in order to complete the storage in the management network of the information related to a virtual connection between two ATM network users. Irrespective of technological solution, the methodology described in subclause B.4 should be followed.

Originating Subnetwork Identifier	VPC Subfield

Figure B.4: VPC identifier

Originating Subnetwork Identifier	VCC Subfield

Figure B.5: VCC identifier

B.5 Inter-subnetwork and physical link Identifiers and algorithms

B.5.1 Transmission Link and access points Identification

The ATM VP logical links will have to be allocated by management to suitable physical transport resources, for instance in the case of SDH, the ATM VPs will be inserted in an available logical link (Virtual Container). Network management has to correlate objects belonging to the physical resources. An example of the range and scope of the requirements for addressing and identification of all entities associated with the provision of ATM over SDH services is given in subclause B.12.

B.5.1.1 Transmission Links

ITU-T Recommendation M.1400 [13] provides a suitable scheme for physical links supporting the transmission bearers such as SDH STM-1 and E3 links, as mandated in [1].

Transmission Link type	M.1400 [13] Function Code
SDH STM -1	As described in M.1400 [13]
E3	As described in M.1400 [13]

The terminology used in [6] has a slightly different view of the modelling for the physical interconnection having the concept of an access point pnoNWAtmAccessPoint which is assigned by each PNO for each physical link termination on a subnetwork. Conceptually, the ATM Access Point would be located in the Gateways as defined for the user and control plane in [1].

B.5.1.2 M.1400 ATM Connections

Figure B.6 shows the relationship between the physical models defined in [13] and [6].

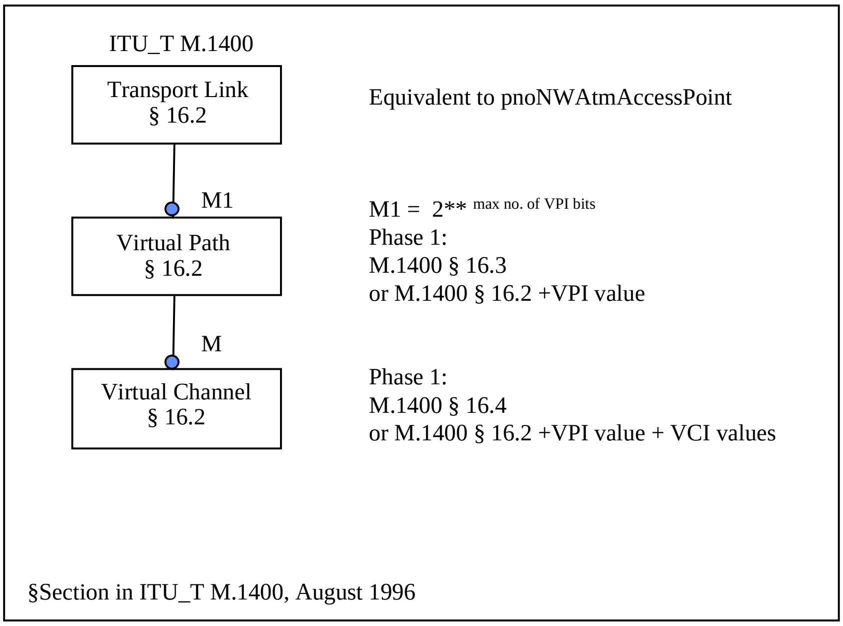


Figure B.6: Relationship between ITU-T Recommendation M.1400 ATM entities and EN 300 820-1 Physical entities

The M.1400 [13] view is that a transport link can support a number of VPs some of which may support VCs. (The modelling depicted in figure B.6 may require adaptation to the layer definitions in ITU-T Recommendation G.805 [55] which describes the functional architecture of transport networks in a technology independent way.)

Preferred VP/VC Identifier Scheme

In the updated M.1400 [13], Function code identifiers have been allocated for transmission links and VP and VC:

Type	M.1400 [13] Function Codes
Virtual Path	VPA
Virtual Circuit	VCA

This allows the serial numbers for Transmission Links VPs and VCs to be allocated independently.

Alternative VP/VC Identifier Scheme

In practice, early implementations have taken a simpler approach which is to assume a one to one binding between the transmission links and the VP and the VC.

This allows:

- the VP to be modelled as a transport link M.1400 [13] designation + VPI code;
- the VC to be modelled as a transport link M.1400 [13] designation +VPI +VCI.

For pragmatic reasons associated with the support of existing operations support systems this is a reasonable approach for Phase 1. (It should, however, be replaced in later phases of ATM service introduction by the Standards based approach described above.)

ITU-T Recommendation M.1400 support in EN 300 820-1

To resolve the differences in the modelling approaches it is necessary to balance two factors:

- Operational practice for identifying International leased circuits is based upon the use of M.1400 [13] Designations for International Networks.
- The ETSI standard for PVP Configuration [6] uses a slightly different concept for modelling the physical links between PNOs based upon interPnoTopologicalSubnetworkPairs which tie together the endpoints of physical links denoted by the pnoNWAtmAccessPoint. This is not exactly the same as the M.1400 [13] method which uses an identifier based on a pair of towns and a unique Function Code/Serial Number identifier per physical link.

In order to resolve these differences, a specific interpretation has to be placed upon the use of the InterPNOSubnetwork Topological Pair Managed Object defined in [6]. Essentially this amounts to merging the concept of a link and a connection termination point into a single location and PNO identifier.

B.5.2 Proposed X.easi convention for use of the InterPNOSubnetwork TopologicalPair Managed Object

In [6] it is assumed that the (logical) link is identified by the SubNetworkPairId of each PNO. In operational systems this is not feasible as the endpoint is normally a local identifier linked to the physical location of the terminating rack and circuit card. In practice these change and it is impractical to keep these details up to date across PNO domain boundaries.

In [6] the link (the bundle of "wires" or "optical fibres", etc) is identified by the "SubNetworkPairId" which is not the endpoint identifier, but simply the Identifier of the link. The attributes "aEndPoint" and "zEndPoint" contain the Identifier's of the subnetworks that are interconnected. The set of individual "wires etc" are described in attribute "ListofAtmAccessPointPairResources" which actually contains each pair of ATM Accesspoints that are interconnected. (Together with the bi-directional Bandwidth and QoS.) The definition of link is in accordance with [22].

Changes in links may be reported over the X.easi interface if they are relevant (assuming implementation of CM to [6]). That means not only a change in bandwidth or in QoS but also in AccesspointId, because the AccesspointId is used in the connection reservation request and the Initiator should know about requirements for such changes.

The current operational practice (for international leased circuits) is to use M.1400 [13] identifiers which uniquely identify the interconnecting links and not the endpoints. Although operationally untested, [6] should offer the possibility to uniquely identify the interconnecting links with "SubNetworkPairId". M.1400 [13] designations support links between International Gateways and conceptual termination points are created for these gateways - i.e. virtual town codes for the gateways. Semantically, the M.1400 [13] designations embed details of these termination points and a unique serial number to bind them together.

It is proposed therefore to align the unique identifier requirement by pragmatic use of the following conventions for the attributes of this managed object:

aEndpoint	Carrier code as per ITU-T Operational Bulletin
zEndpoint	Carrier code as per ITU-T Operational Bulletin

SubnetworkPairId	The scheme proposed in subclause B.2.2 should be used e.g. BTIMondial3VPA- FTIEtoile28VPA"
	minimum field length 39 characters including "-"

within each listOfATMAccessPointPairResources:

ApnoATMAccessPointId	Use the accessPointId of the AccessPoint at the A side if it proves fit for purpose after implementation and testing or use the M.1400 [13] code for Virtual Path as described above Typically 34 characters (maximum 44). The M.1400 [13] code should probably be used for manual implementations of the X.easi interface
ZpnoATMAccessPointId	Use the accessPointId of the AccessPoint at the Z side if it proves fit for purpose after implementation and testing or use the M.1400 [13] code for Virtual Path as described above Typically 34 characters (maximum 44). The M.1400 [13] code should probably be used for manual implementations of the X.easi interface.

The use of M.1400 [13] would lead to redundancy in stored information but is necessary to ensure effective integration with current operational systems and operational practice and avoids the need to change [6] for a relatively minor reason. It also allows relatively simple retrieval of attribute information in a way that is intuitive to human operators.

B.5.3 Inter subnetworks ATM logical links identification

The material in this subclause should be carefully reviewed and tested in X.easi interface implementations before deployment. The proposal is as follows:

Besides the physical links, each ATM VP logical link between two subnetworks of an interconnected Pan-European ATM network will have to be identified unambiguously for OSS purposes. That can be realized by a further identifier or by the previous identification means.

The M.1400 [13] designator in conjunction with the VPI provides a method to build a suitable inter -subnetworks VP identifier, considering that one-to-one correspondence between an ATM cross-connect port and physical link exists. This kind of identification method could be used for Phase 1 of service introduction for a Pan-European ATM network since it permits simplification of the global identification task.

For later phases of ATM service introduction, the necessity to de-couple information belonging to potentially different network management systems should be evaluated since SDH management is, in principle, separated from ATM management.

Even if it should not be applied in for Phase 1 service introduction, it seems useful to propose a specific identifier with a scope limited to the ATM network management. That will make it unnecessary for the ATM management centre to know and use M.1400 [13] identifier values really assigned by the physical (e.g. SDH) network management. Figure B.7 presents a proposal of structure for this identifier which contains information on the subnetworks connected by the link and other information needed for the unambiguous identification of the link itself.

Subnetwork A	**Subnetwork B**	**Link**
identifier	identifier	identifier

Figure B.7: Inter-subnetwork links Identifier

The Subnetwork identifier fields should follow the structure described in subclause B.2.2.

The link identifier is mainly a sequence number used as pointer to a data area that includes all the parameters concerning the ATM logical link (i.e. Originator and destination User identification, VP Connection Identifier, VPI value, etc.). It should be defined on the basis of bilateral agreement and information should be given to the other operators. The length of such fields is for further study.

B.5.4 Virtual Path Identifier (VPI) assignment algorithm

This is the identifier to use in the ATM header for the cell to be transmitted on the VP. The same VPI will be assigned for both directions (forward and backward).

Due to the fact that two sub networks can simultaneously allocate the VPI's of the Logical Links which interconnect them, a VPI "collision" could occur. In order to minimize the probability of the simultaneous allocation of the same VPI to two different VPC's by two sub networks directly interconnected the following algorithm is advised:

> Every sub network allocates VPI values according to a pre-set scheme (i.e. top down or bottom up from their possible list) and then for the very occasional duplication of VPI values both connection attempts should fail. Each subnetwork starts allocating VPIs from the top or bottom according to the relative position of its subnetwork identifier with the subnetwork identifier of the subnetwork at the far end of the transmission link. The subnetwork whose subnetwork identifier is lower will allocate from the lower to the higher VPI and the subnetwork whose subnetwork identifier higher is will allocate from the higher to the lower VPI.

B.5.5 Virtual Circuit Identifier (VCI) assignment algorithm

This area remains for further study and description of a solution. At first appraisal, a scheme following the same pattern as for the VPI assignment algorithm should be satisfactory.

B.6 Subnetwork Connection and Termination Point Identifiers

B.6.1 Virtual path subnetwork connection identification

The identifier for a Virtual path subnetwork connection used in the following managed object and attributes.

Managed Object	Attribute
pnoVpSubnetwork	SubnetworkConnectionId

The assignment of these identifiers is local to the OSS of the PNO and the only requirement is that it is unambiguous within each OSS.

EURESCOM P708 [38] made a proposal for the attribute as follows:

"In order to guarantee a unique name for a pnoVpSubnetworkConnection object created as a result of the Reserve Request, the value for its naming Attribute (SubnetworkConnectionId attribute inherited from the SubnetworkConnection MOC) must be set to the concatenation of the values of the initiatingPnoId and initiatingVpConnectionId in the ASN.1 syntax of the reservePnoVpSubnetworkConnection Action received from the Manager.".

This proposal may be accepted as an enhancement for [6] and should be adopted for implementation of the X.easi interface unless an alternative proposal is endorsed for the standard.

B.6.2 Virtual Circuit subnetwork connection identification

The identifier for a Virtual Circuit subnetwork connection is used in the following managed object and attributes.

Managed Object	Attribute
pnoVcSubnetwork	SubnetworkConnectionId

The assignment of these identifiers is local to the OSS of the PNO and the only requirement is that it is unambiguous within each OSS. The information provided in subclause B.6.1 should be considered for adoption at the VC level.

B.6.3 Virtual Path Connection Termination Point (pnoVPCTP) identification

This Termination Point logically binds the end of a pnoVpSubnetworkConnection to a physical access point called pnoNWAtmAccessPoint. The identifier for a pnoVPCTP is used in the following managed object and attributes.

Managed Object	Attribute
pnoVPCTP	vpCTPId

The use of the I.751 [18] identifiers is recommended to be considered for enhancement to the CM standard [6]. There may be a requirement to add an attribute in the pnoVPCTP which contains the associated M.1400 [13] Designation for the VP.

B.6.4 Virtual circuit Connection Termination Point pnoVCCTP identification

This Termination Point logically binds the end of a pnoVcSubnetworkConnection to a pnoVP termination point called pnoVPCTP. The identifier for a pnoVPCTP is used in the following managed object and attributes.

Managed Object	Attribute
pnoVCCTP	vcCTPId

The use of the I.751 [18] identifiers is recommended to be considered for enhancement to the CM standard in [6]. This could mean that the name binding is logically equivalent to naming the termination point as "Transmission bearer Identifier" + "VPI" "+"VCI".

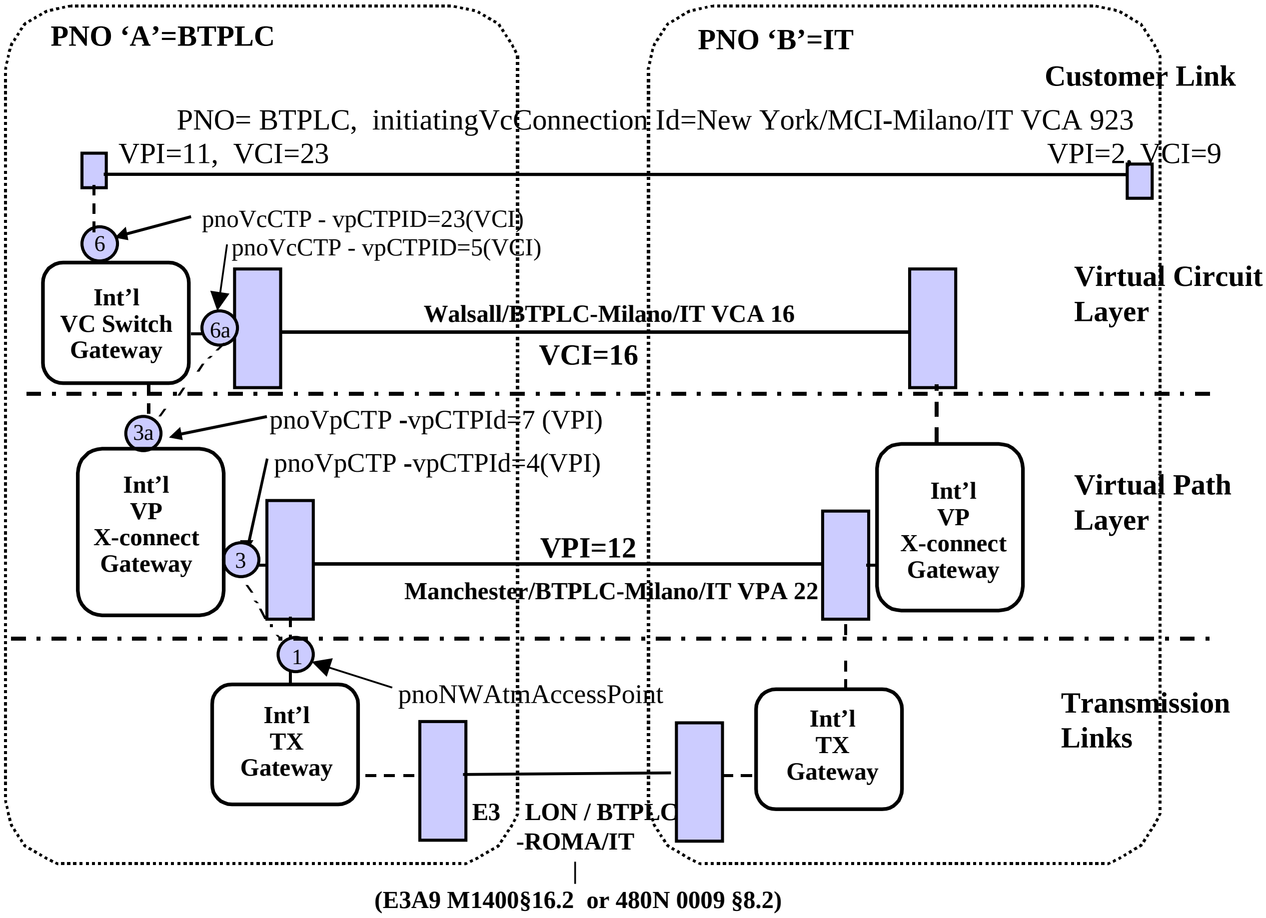
This may be too restrictive for long term operational use and either the attribute may need to be changed to support M.1400 [13] VC Designations or there may be a requirement to add an attribute in the pnoVPCTP which contains the associated M.1400 [13] Designation for the VC.

B.7 VP Trail, VP Trail Termination Point and VP Link Connection Identifiers

No proposal is available in M.1400 [13] for identifiers of Trails, VP Trail Termination Points and VP Link Connections. Assignments of identifiers for these are therefore for further study. The minimum requirement is clearly that assignment of identifiers is unique for any given connection and unambiguous within the OSSs of the operators providing the connection.

B.8 An example

Figure B.8 shows a specific example of the identifiers in use for Permanent Virtual Circuits. (PVC).



Legend (referring to numbers in the figure:
1 inter-operator gateway connection point corresponding to pnoNWAtmAccessPoint
3, 3a inter-operator (or international) VP cross connect termination point corresponding to pnoVpCTP
6, 6a inter-operator (or international) VC cross connect termination point corresponding to pnoVcCTP

Figure B.8: Example of mapping between M.1400 [13] Designations and EN 300 820-1 [6] entities

This example is entirely fictitious as it has not been possible to check carrier codes in the operational bulletin. The example does not imply that any specific company will or will not participate in ATM interconnect processes or that the processes described are complete and accurate. I.e. the description is for discussion and illustrative purposes only.

The example shows a Customer connection between New York and Milan - for example between the New York Stock Exchange and the Milan Bourse. The New York end is assumed to be served by MCI. The circuit is a transit circuit via BT. The Initiating PNO is BT. The VC connection is established between the UK and Italy using a VC connection between international Gateway VC switches in Walsall/UK and Milano/Italy. The VC used between these switches has a separate M.1400 [13] VC designation.

The VC switches in Walsall and Milan utilize international Gateway VP crossconnects to establish a VP on which the PVC can be established. The VP between the international cross connects used for this connection is also given an M.1400 [13] designation. In the example the UK VP switch is located in Manchester.

The VP between the International VP cross connects uses transmission links between London/UK and Roma/Italia. The international Transmission link also has a M.1400 [13] designation - in this case for an E3 Transmission Link.

Figure B.8 also shows the mapping of the EN 300 820-1 [6] objects and attributes onto these entities. Specifically the pnoNWAtmAccessPoint, shown as "1" maps to the end point of the transmission link into the VP switch. The transmission link is equivalent to the Inter-PNO Physical Link (IPPL) in [6], which needs to be mapped to M.1400 [13] identifiers for operational purposes.

The pnoVpCTP corresponds to the termination on the VP International cross connect shown as "3" and this is logically equivalent (1:1 mapping) to the termination on the VC switch "3a". The pnoVcCTP, which is associated with this, is shown as "6a" and this is logically equivalent to the pnoVcCTP shown as "6".

B.9 Operations Support Systems Identifiers for OSI-based implementation

B.9.1 General OSI naming concepts and models

Clause B.9 is very much concerned with implementational issues and the practical development of automated functions of the X.easi management interface. Such development will need pre-operational and operational testing, which comes within the scope of the requirements defined in the Operator's Handbook [3]. Figure B.9, taken from the NMF C++ API, gives guidance on the relationships amongst OSI entities.

When using the naming service, it is assumed that each combination of a managed object and the agent it resides in, is unambiguously represented in a manager application. That is, given the Distinguished Name (DN) of a managed object, a manager can unambiguously identify at least one agent that supports that managed object. This does not preclude the "same" managed object (i.e. a single DN) from residing in multiple agents, nor does it preclude a manager from communicating with this managed object via different agents. If a manager wishes to communicate with this managed object via different agents, it must instantiate multiple managed object handles (internal software references) for this managed object with the same DN (MO Name), but then assign a different agent handle (internal software references) to each managed object handle. Operations on that managed object handle will then be sent to the managed object via the agent specified in that managed object handle. Figure B.9 shows an example of such a situation, where two agents support the "same" managed object. (Note that implementation would require some form of "record locking" in this case.)

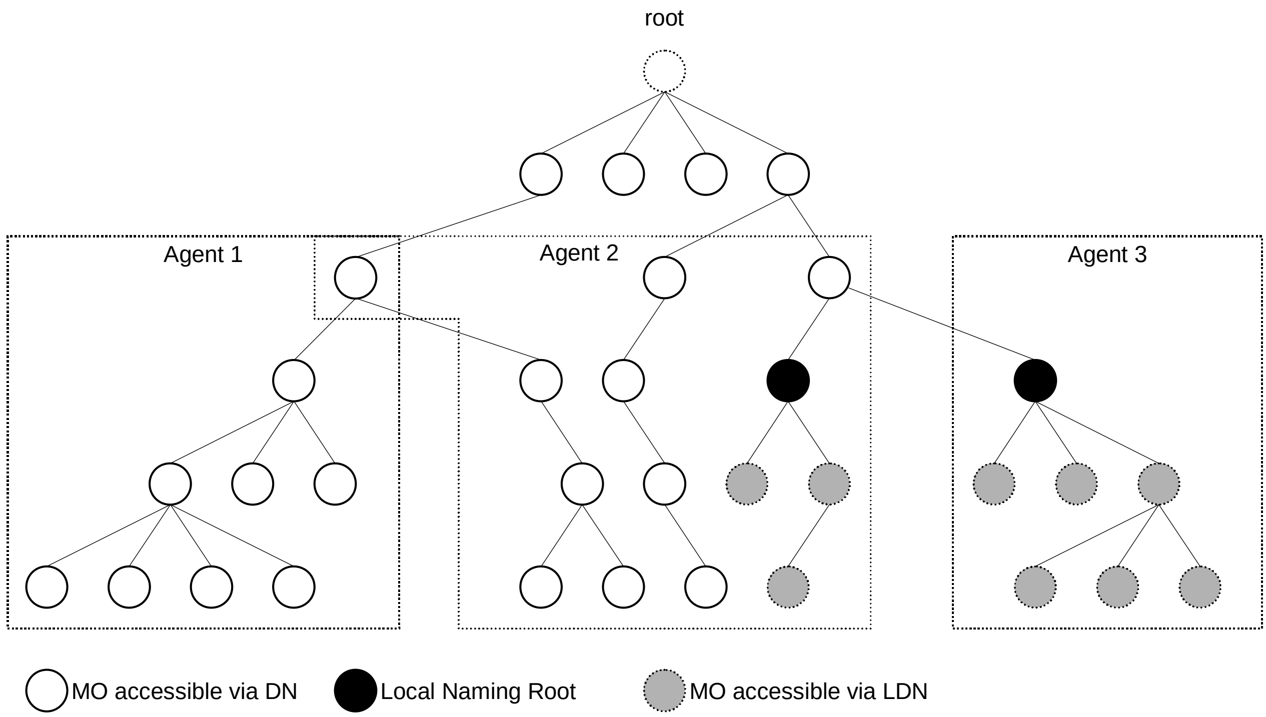


Figure B.9: Multiple Agents Supporting Same Managed Object

The relationships between managed object names, agents, and other entities is not obvious from reading the appropriate standards. Figure B.10 shows an entity-relationship diagram for the key elements used by the NMF API and is generally useful for understanding what needs to be identifier and specified for the OSS applications API.

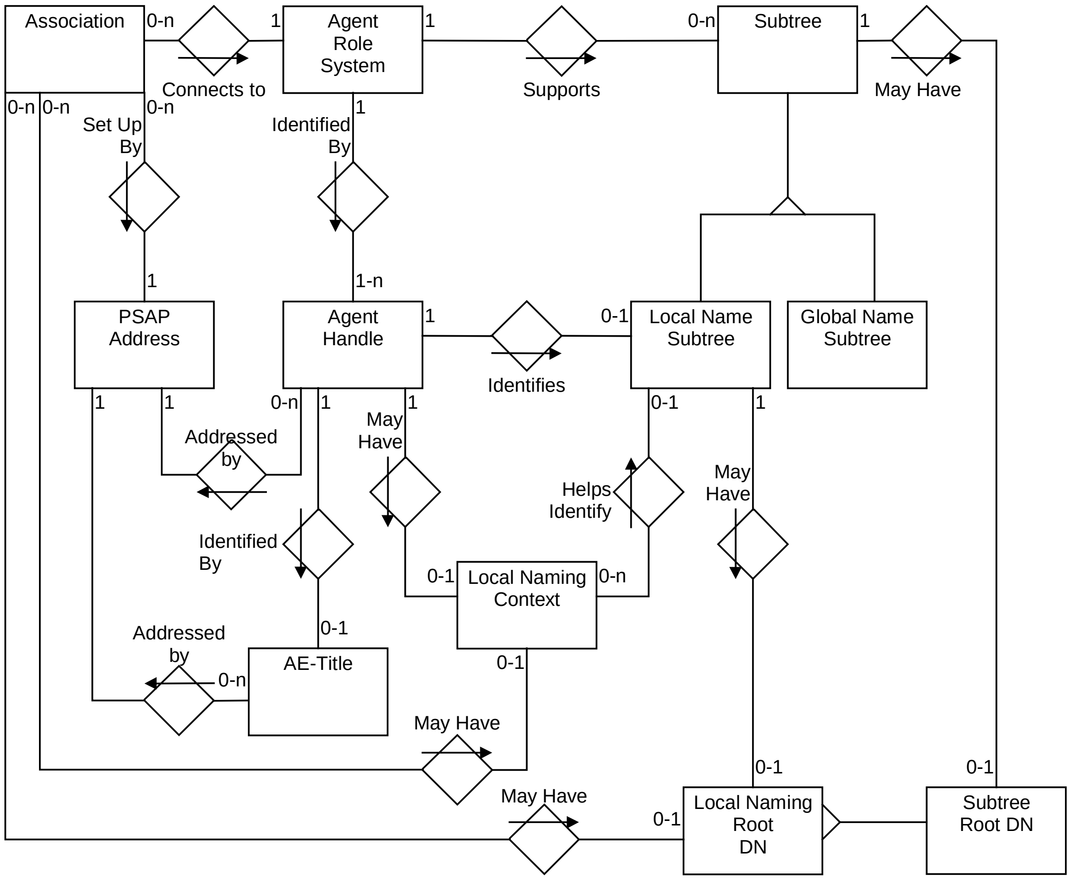


Figure B.10: Relationship amongst OSI Management Systems entities

(In figure B.10, "Handles" are a local implementation concern and do not need to be specified amongst PNOs involved in X.easi implementation.)

Figure B.10 also shows the following relationships, with the cardinality of the relationship provided by the numbers by each entity.

Each association connects a single agent role system (OSI term, "AE invocation") to a single manager role system. An agent role system (OSI term, "AE Application Entity") may, in principle, be connected by any number of associations at a time. (This latter point adds complexity, and for Phase 1 implementation, single associations between pair to pair agent and manager roles should be specified.)

(ii) Each system that operates in the agent role supports zero or more subtrees of the global naming tree. Each subtree is supported by a single agent role system (except for the case described above where several agents support the same managed object instance). An agent that supports zero subtrees is not very interesting except for when an agent simply has not yet had any managed objects created in it yet.

(iii) Each subtree may have at most one Distinguished Name (DN) for its root and each DN identifies a single subtree.

(iv) The concept of an agent handle to identify each agent role system may be introduced. Each agent role system is then identified by one or more agent handles, and each agent handle then identifies a single agent system. For every invocation a handle is created, for this scheme.

(v) Since an agent system may support several associations, each with the same or different PSAP addresses (i.e. different for the case that there are different AE's), an agent handle contains exactly one PSAP address, although the same PSAP address may be used by multiple agent handles, and a PSAP addresses a single agent handle. The concept may be introduced, of an agent handle to recognize that an agent system may support several associations, each with the same or different PSAP addresses.

(vi) An association is established (set up) by PSAP address. At any point in time, a particular PSAP address may be used for zero or more associations.

(vii) Each agent handle may have at most one Application Entity Title (AE-Title), although the same AE-Title may be used by multiple agent handles. Also, each AE-Title identifies a single agent handle. (An agent handle is the internal software reference to an AE-invocation.)

(viii) Each AE-Title is addressed by a single PSAP in a 1:1 naming relationship. The mapping of AE-Title to PSAP address can be retrieved from a directory function or look-up table.

(ix) A subtree may be either a global name tree or a local name subtree. A global name subtree consists of managed objects that may only be accessed by a DN. A local name subtree consists of those managed objects that may be accessed by an LDN, and possibly a DN. Note that a global name is related to a specific global root. It is proposed to recommend use of the same global root for every interconnecting operator wishing to implement an automated X.easi interface.

(x) Occasionally, an agent needs to support multiple associations with the same PSAP address, but support different local name subtrees. In such cases, the agent and manager(s) must have agreed on some information to be exchanged or inferred that can be used to identify which subtree to support over which association. (This may be a local agent implementation issue or may be associated with implementation agreements between operators.) We call that information *local naming context*. Local naming context is any static or dynamic information an application uses to establish and distinguish multiple associations set up with the same PSAP address but using different local name subtrees. An agent handle may have at most one local naming context and a local naming context goes with a single agent handle.

(xi) An agent handle is uniquely identified by a combination of a PSAP address (which always exists), an AE-Title (if it exists), and a Local Naming Context (if it exists). If neither an AE-Title nor a Local Naming Context exists, then the PSAP address must by itself uniquely identify the agent handle.

(xii) When an association is established, at most one local naming context may be selected; the same local naming context may be used over any number of associations.

(xiii) An agent handle and local naming context (if any) identifies at most one local name subtree. A local name subtree may by identified by any number of agent handles and any number of local naming contexts.

(xiv) A local name subtree may have at most one DN for the local naming root and a local naming root is for a single local name subtree. The DN for a managed object in a local name subtree can be produced by prefixing the LDN with the local naming root DN. If the local naming subtree root does not have a DN.

(xv) Accordingly, all of the managed objects in that subtree can only be accessed with LDNs.

(xvi) One of the key constraints is that an association may have at most one local naming root DN. A local naming root may be used over any number of associations, either at the same time, or at different times.

B.9.2 OSI Systems Identifiers

The following list of OSI systems identifiers, for interface application development, needs to be defined locally by each PNO and communicated to other PNOs to support interconnected ATM service introduction. The selection of their values is a local matter for a PNO but should be related to M.1400 [13] identifiers where possible.

Manager Role:

Manager_Title (calling-AP-Title)

Manager_Qualifier (calling-AE-qualifier)

Manager_NetworkAddress * (NSAP address)

Manager_TransportSelector *

Manager_SessionSelector *

Manager_PresentationSelector *

Agent Role:

Agent_Title (called-AP-Title)

Agent_Qualifier (called-AE-qualifier)

Agent_NetworkAddress * (NSAP address)

Agent_TransportSelector *

Agent_SessionSelector *

Agent_PresentationSelector *

Notes concerning the above list:

The AE-Title, which addresses the AE, is the concatenation of AP-Title and AE-qualifier

PSAP address = NSAP address+ + TransportSelector + SessionSelector + PresentationSelector

* this means: it is not a parameter in the association, but needs to be known by operators using an automated X.easi interface. The AE Title should be mapped to the PSAP address either by some directory service or by an internal table.

Parameters which can be used when making an association, (when using the X.easi interface), should be available from the Operator's Handbook (P813 Deliverable 3) [3].

B.10 Summary and Issues

This annex has identified a number of requirements and issues which need definition or resolution in order to be in a position to fully specify the ATM interconnect service operation processes and the X.easi management interface. These are specifically:

> It is noted that project JAMES did not use the international standard ITU-T Recommendation M.1400 [13] for addressing and entity identification. The JAMES solution is clearly not adequate for ATM interconnect services in an operational situation relating to the multi-operator environment.
>
> It seems essential to use M.1400 [13] identifiers, with adaptations or extensions if necessary, for identifying the entities required to support interconnected ATM services. Customer connections require identification based on an appropriate combination of M.1400 [13], E.164 [44] and possibly AESA addressing components.
>
> For each of the entities listed in subclause B.1.1, there is a clear requirement for having a standardized method of identifying each entity, which should be related to established international standards as closely as possible.
>
> In subclause B.9, a software design issue of mapping OSI to M.1400 [13] identifiers was discussed.
>
> An improvement in descriptions could be achieved by separating the identifier and addressing Requirements (for the entities specified) from the proposed solutions or specifications for the management identifier schemes required to support the ATM service interconnect operation processes.

B.11 Example of ATM over SDH functional architecture

Figure B.11 replicates an example taken from ITU-T Recommendation G.805 [55] for the case of the functional architecture required for ATM supported on SDH. Additionally, a "scope" box and Management Interactions linkage arrow have been added to illustrate the scope and extent of the X.easi interface specification provided in the present document.

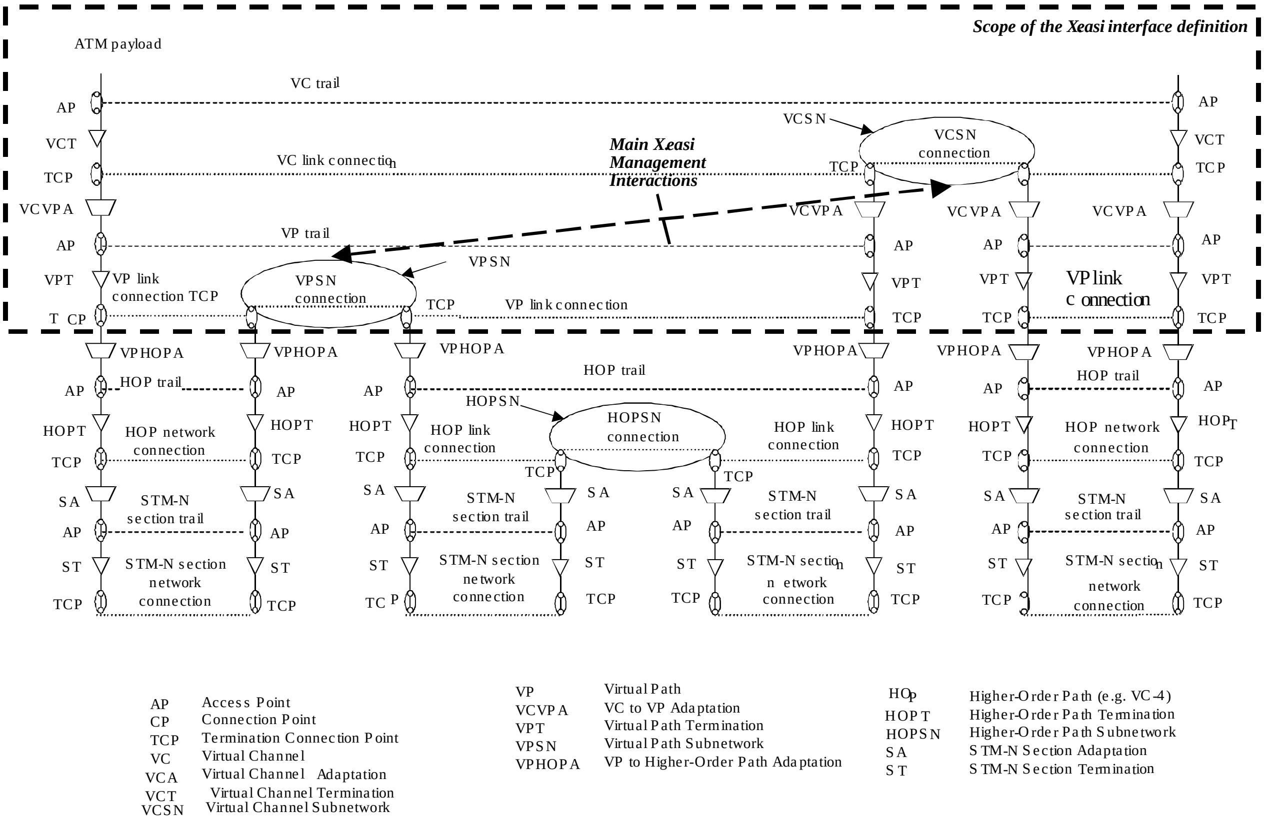


Figure B.11: Functional architecture illustrating addressing and identity requirements

The example in figure B.11 is included to illustrate the extent and complexity of the addressing and identity requirements for various entities associated with one particular form of ATM service provision and shows these in relation to respective VP and VC trails and connections.

Note that the X.easi interface "view" only sees one side of any connection whereas figure B.11 shows the full series of network connections and therefore illustrates the depth of complexity of both the network connections and the management needed to provide ATM based services using it.

Additionally, it should be noted that all the entities, trails and related resources will need to have unique identification, which in turn, will have to be transferred across PNO boundaries in cases where ATM interconnect services are required.

Annex C (informative): A detailed discussion of the data model for PVP and PVC connections

C.1 Introduction

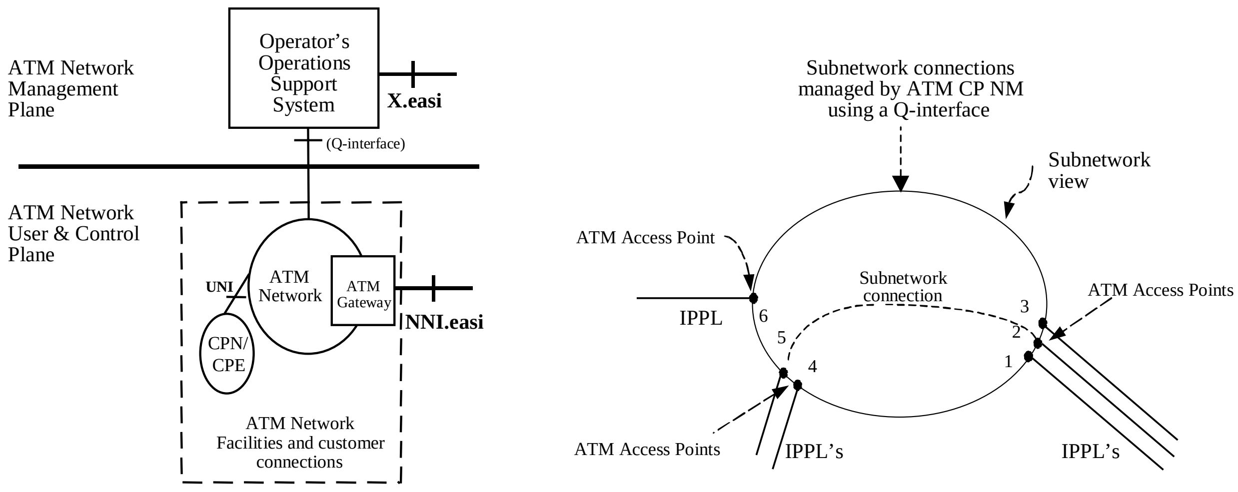
This annex provides a detailed discussion of the data model for PVPs and PVCs, as applicable to the implementation of automated X.easi interfaces to support management of ATM services. In particular, proposals are presented in this annex for extensions to the PVC level derived and developed from existing standards [6], [10] and should be considered for presentation as new standards in support of management of PVC-based services.

In general, this annex should be considered as an addition to, or enhancement of, the "Data Model" in clause 10 of the main part (which relates only to the established management of PVPs).

C.2 General Modelling requirements

Modelling requirements need to consider that in the ATM Reference Model there are 3 planes: "user-plane", "control plane" and "management plane". For each plane, a layered approach is used which should include descriptions for the physical layer, ATM layer and ATM adaptation layer respectively.

Figure C.1, derived from figures 4 and 7 (in the main part), summarizes the physical layer and ATM layer connections:



Physical view of connections and interconnections from one operator towards another operator.
For Legend, refer to equivalents in Figure 4.

Logical view of connections set up across one subnetwork for interconnection with another subnetwork using IPPLs
For Legend, refer to equivalents in Figure 7

Figure C.1: Physical layer and ATM layer connections to support an ATM VP

Interconnection at the physical and ATM layers for the U&C plane is defined by the requirements in [1] whereas management of ATM VPs and VCs, in the NM plane, should follow the requirements in [6] and in this annex. The ATM Access Points and IPPLs, shown in the Logical view in figure C.1, are associated with the ATM layer Gateways and physical transport bearer links (e.g. SDH links) which interconnect operator's subnetworks.

The ATM and physical layers for the NM and U&C planes include the following:

- **ATM layer, network management plane:**

the set of VP (or VC) subnetworks, that are used to carry out the user-to-user PVP (or PVCs) connections.

The IPPL links that provide the inter-carrier connectivity.

- **ATM layer, user and control plane:**

  the set of ATM links (i.e. Transmission Paths) that provide the inter-carrier connectivity.

  (The "ATM Link" is formally defined in [54].)

- **Physical Layer:**

  The SDH, PDH etc. and switching systems which provide the resources for creating the ATM links (defined as the resources that provide the inter-carrier connectivity and that are required to support ATM PVP (or PVC) services).

C.3 Connection Types and Resources

In subclause C.3, the necessary resources in relation to the layers and their management identified in subclause C.2 above, are listed and described. From this a description of the object model is given.

C.3.1 Connection Types

To provide interconnected ATM services, the following connection types are of significance for the specification of the functionality of the X.easi management interface:

- user-to-user VCC;
- user-to-user VPC;
- user-to-network VPC;
- network-to-user VPC;
- network-to-network VPC.

(A connection that terminates in a network should do so at an ATM interconnection gateway.)

These are overall connections. They involve the networks and NNIs of more than one ATM CP and they are formed by resources like subnetwork connections across the networks of the individual ATM CPs and/or link connections across the NNI.easi interface. **It is important to note that the managed resources describe the situation at an individual ATM CP. There are no managed resources identified that describe the overall connections.**

C.3.2 Resources

The managed resources identified for user-to-user VPC services are:

- *Virtual Path Subnetwork*, which provides the ability of an ATM CP to establish (reserve) and release VPCs;
- *AccessPoints*, to or from a subnetwork which can be either ATM interconnection gateways or UNIs;
- *Virtual Path Connection Termination Points*, which are the termination points for a VPC;
- *Virtual Path Subnetwork Connections*, the VP reservations made across a CP's subnetwork. They can terminate at ATM interconnection gateways and/or at UNIs;
- *Inter-Pno Physical Links*; the NNI.easi interface [1], the links between the ATM interconnection gateways that belong to different CPs.

For the other types of VPCs an additional managed resource is identified:

- *Virtual Path Link Connections*, which are VP reservations made from one subnetwork to another, across the NNI.easi interface.

The additional managed resources identified for user-to-user PVC services are:

- *Virtual Channel Subnetwork* which provides the ability of a CP to establish (reserve) and release VCCs.
- *Virtual Channel Connection Termination Points,* which are the termination points for a VCC;
- *Virtual Channel Subnetwork Connections,* the VC reservations made across a CP's subnetwork . They can terminate at ATM interconnection gateways and/or at UNIs.

For the X.easi management interface the following observations are also applicable:

- a *Virtual Path Subnetwork Connection* need not show the Virtual Channels it contains. This does not always apply to a *Virtual Path Link Connection;*
- a *Virtual Channel Subnetwork Connection* need not show the Virtual Path Connections it is contained in. However, for the NNI.easi interface the VPI-value needs to be known to the ICP.

For User-to-user overall connections (PVP and PVC), the parts of the overall connection going across the *Inter-Pno Physical Link* need not to be seen because, by both accepting the request for a *Subnetwork Connection*, the ATM CPs on both sides of the link will take the occupation of the link into account.

For overall connections that terminate at an ATM interconnection gateway the ATM CP at the other side of the *Inter-Pno Physical Link* needs to be informed about the occupation of the link by a *Virtual Path Link Connection* request.

The resources are modelled by object classes. These object classes are mainly derived from generic classes of the ETSI GOM Model [22] and ITU-T Recommendation M.3100 [21].

The generic models recommend the use of layered network modelling. Trails are served connections at a lower layer and serving connections at a higher layer. In a model which has both VCCs and VPCs, trails can be modelled to relate these two layers of connections. In this context, VCCs can be seen as being served by VPTrails, which are terminated by Trail Termination Points. However, from the observations i) and ii) above it can concluded that for X.easi this concept is only relevant for the part of User-to-user VCCs going over *the Inter-Pno Physical Link.*

A *Virtual Path Link Connection* provides a *VP Trail* which is terminated by *Virtual Trail Termination Points.*

According to [22], only the VPTTP needs to be modelled, leading to a requirement for introduction of the following entity:

- VP Trail Termination Point (VPTTP).

C.4 Object Model

PVP services have been studied in a number of standards bodies including ETSI, ITU-T, ATM Forum. The resources, object classes, requirements and definitions associated with "automated" Configuration and ATM VP Alarm Management for PVPs are mostly derived from or profiled from [6] and [10]. Extensions derived from these standards are provided below in order to include functionality for management of PVC services.

The term "PNO" is used to mean any interconnected Connectivity Provider (CP) and is chosen to maintain consistency with the object nomenclature in some of the relevant standards.

C.4.1 Object Classes

The object classes that are associated to user-to-user VPC services are described in [6] and [10]. Together with the additional object classes necessary for the other connection types mentioned in subclause C.3.1 they are described in brief below:

pnoVpSubnetwork (PNO Virtual Path Subnetwork)

A pnoVpSubnetwork (object) represents the complete Subnetwork of a certain Operator, from a topological point of view, at the Virtual Path (VP) layer.

A PNO VP Subnetwork offers external interfaces to other PNO VP Subnetworks through PNO NW ATM Access Points.

From a Connectivity point of view, pnoVpSubnetworks are crossed by Subnetwork Connections.

The pnoVpSubnetwork manages the establishment (reservation) and release of Subnetwork Connections. So pnoVpSubnetworkConnection object instances are created when reservations are requested.

The Notifications of this object must be broadcast to every PNO in the Network.

The Action reservePnoVpSubnetworkConnection is performed by the Initiating PNO over the A-,Transit- and Z-PNOs.

The Actions giveAvailableLinks and checkUser are performed by the Initiating PNO over the Z-PNO.

PnoNWAtmAccessPoint (PNO network ATM access point)

This object class represents either an endpoint of a physical link at the cell level, or a UNI.

PnoVpCTP (PNO Virtual Path Connection Termination Point)

This object class represents the endpoint of a PNO VpSubnetwork Connection, or of a VP Link Connection between two PNOs.

Two instances of the pnoVpCTP object are created when a pnoVpSubnetworkConnection instance is created.

The assignment of the VPI associated with this connection is done by the NearEnd OS.

PnoVpSubnetworkConnection (PNO virtual path subnetwork connection)

This object class represents the reservation of a Virtual Path connection across a PNO subnetwork.

The Initiating CP only views this connection as a whole, with no details regarding the identification of VP Cross Connects (VPCC's) and links between VPCCs, which compose this connection inside the PNO domain.

InterPnoTopologicalSubnetworkPair (inter-PNO topological subnetwork pair)

This object class represents a bundle of physical links between two PNOs at the cell level.

It gives information about the maximum capacity of these physical links. This information is used by path searching algorithms.

The InterPnoTopologicalSubnetworkPair is bi-directional.

PnoVpLinkConnection (PNO virtual path link connection)

This object class represents the reservation of a Virtual Path connection across an inter-Pno link.

The initiating PNO only views this connection as a whole, with no details regarding the identification of the network elements which compose this connection.

PnoVcSubnetwork (PNO virtual circuit subnetwork)

A pnoVcSubnetwork (object) represents the complete Subnetwork of a certain Operator, from a topological point of view, at the Virtual Circuit (VC) layer.

A PNO VC Subnetwork offers external interfaces to other PNO VC Subnetworks through PNO NW ATM Access Points.

From a Connectivity point of view, pnoVcSubnetworks are crossed by Subnetwork Connections.

The pnoVcSubnetwork object manages the establishment (reservation) and release of Subnetwork Connections. So pnoVcSubnetworkConnection object instances are created when connections are requested.

The Notifications of this object must be broadcast to every PNO in the Network.

The Action reservePnoVcSubnetworkConnection is performed by the Initiating PNO over the A-, Transit and Z-PNOs.

The Actions giveAvailableLinks and checkUser are performed by the Initiating PNO over the Destination PNO

pnoVcCTP (PNO virtual circuit connection termination point)

This managed object class represents the endpoint of a PNO VcSubnetwork Connection.

Two instances of the pnoVcCTP object are created when a pnoVcSubnetworkConnection instance is created.

The assignment of the VCI associated with this connection is done by the NearEnd OS.

Contention for a particular VCI may be a problem i.e. the attempt to simultaneously allocate the same VCI by two adjacent operators on the same Virtual Path. To avoid this, a scheme should be adopted whereby one operator starts selecting VCIs from bottom end of the VCI range, and the other starts from the top. This will be effected by agreement between PNOs.

PnoVcSubnetworkConnection (PNO virtual circuit subnetwork connection)

This object class represents the reservation of a Virtual Circuit connection across a PNO subnetwork.

The Originating PNO only views this connection as a whole, with no details regarding the identification of network elements and links between network elements, which compose this connection inside the PNO domain.

Conceptually it is presumed that the pnoVCSubnetwork exists as a separate entity and provides the capability for pnoVC Subnetwork connections between pnoVcCTP termination points. The network part of the NNI.easi specification [1] restricts individual VPI values to contain either PVPs or PVCs but for SVCs to be carried in separate PVPs.

PnoVpTTP (Pno VP trail termination point)

It is proposed that the VP Trail Termination Point is defined as a managed object that originates and terminates Trails and Subnetwork Connections in the Network viewpoint. An instance of this class may only have Trail relationships with Network Trail Termination Points which are at the same layer. The inheritance tree of the object classes showing traceability back to ITU-T Recommendation X.721 [20] is shown below in figures C.2 and C.3.

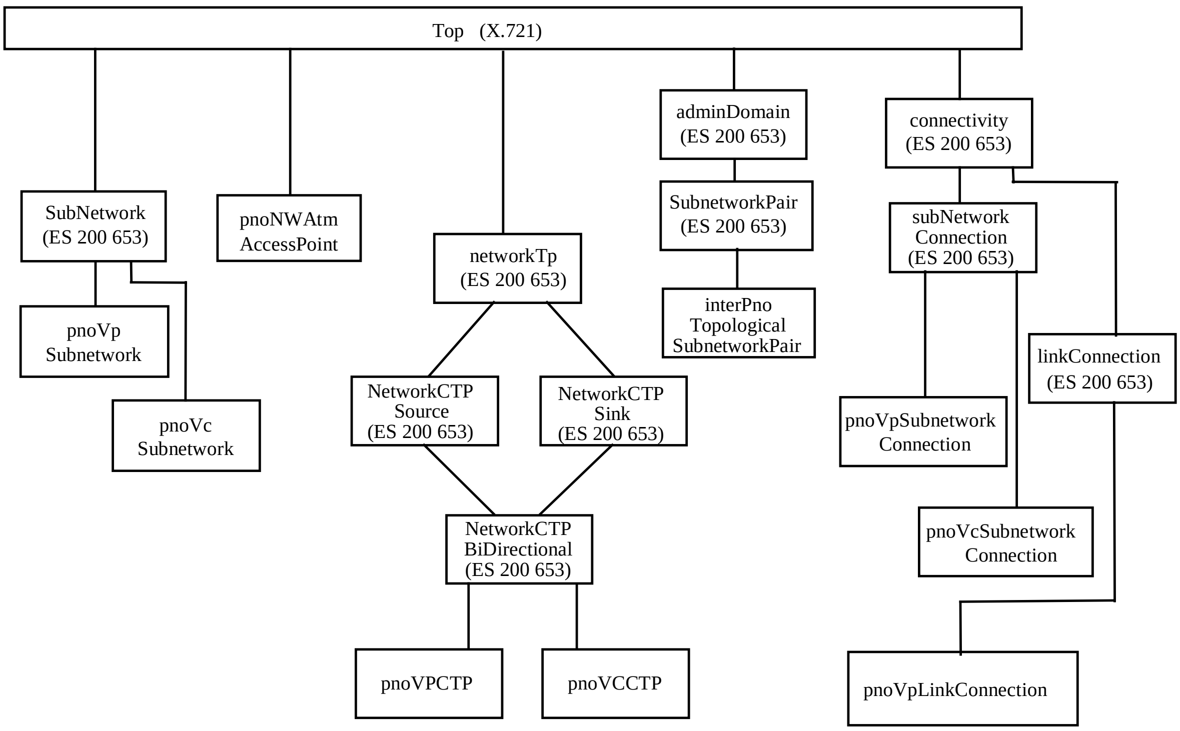


Figure C.2: Object Classes Inheritance Tree - Connectivity

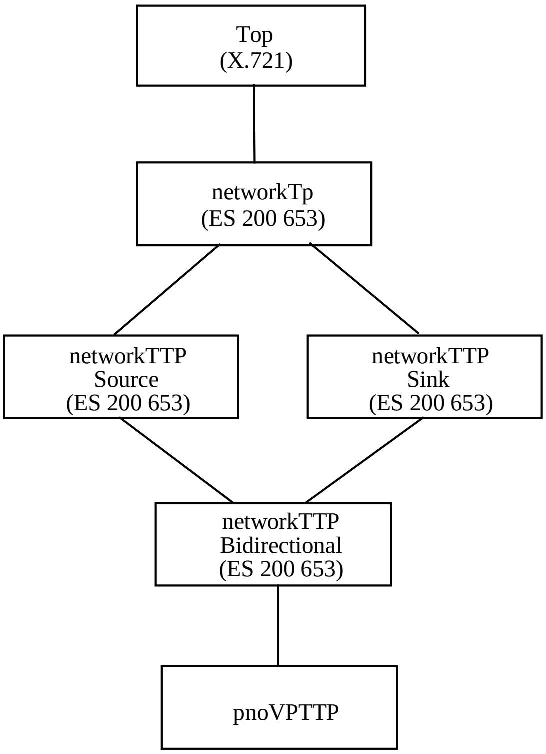


Figure C.3: Object Classes Inheritance Tree - Trail Termination Point

C.4.2 Entity relationships for VP- and VC- Connections

The relationships between existing and additional object classes, defined in subclause C.4.1 and depicted in figures C.2 and C.3, allow development of an extended Entity relationship (E-R) diagram, figure C.4. This follows the equivalent E-R diagram in the CM standard [6], but provides an extension such that VcSubnetwork connections exist in a similar way to VpSubnetwork connections.

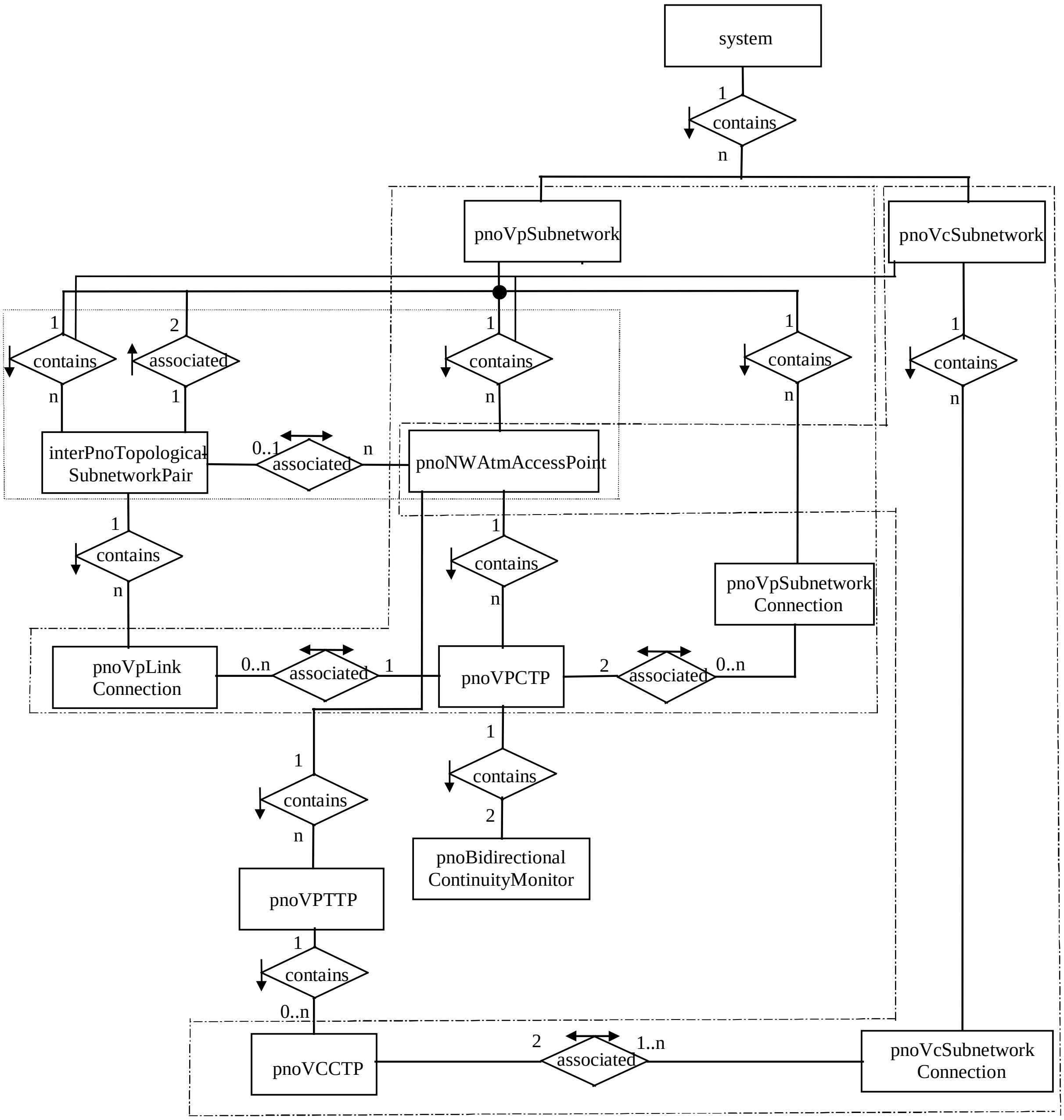


Figure C.4: Relationships and Cardinality between the Managed resources

The managed resources identified in the **left-hand** box of figure C.4 are associated with the major physical network links between the co-operating PNO's.

The managed resources identified in the **centre** box of figure C.4 are associated with Virtual Path reservations, including local access and delivery within the domain of the involved PNO's subnetwork.

The managed resources identified in the **right-hand** box of figure C.4 are associated with Virtual Circuit reservations, including local access and delivery within the domain of the involved PNO's subnetwork.

It is proposed to introduce OC *system* as a root for the Naming-tree in order to give every participant in the X.easi system the same root-element.

On the X.easi management level it is possible to set up VCCs independently of VPCs. This is modelled OC *pnoVcSubnetwork* which is independent from the OC *pnoVpSubnetwork*. (They have their physical resources in common)

There is an OC *pnoVcSubnetworkConnection* which has an analogous functionality as the OC *pnoVpSubnetworkConnection*; providing connections across subnetworks.

For subnetworkconnections the VPCs do not show their contained VCCs and the VCCs do not show the VPCs they are contained in. So there is no containment relationship between *pnoVpSubnetworkConnection* and *pnoVcSubnetworkConnection* and between *pnoVPCTP* and *pnoVCCTP*.

However, when requesting for a VCC the *I-CP* needs to know not only the VCI but also the VPI that is used for the part over the inter-Pno Link. The *pnoVPTTP*- instance has this information and therefore the *pnoVCCTP-instance* is bound by a *pnoVPTTP*-instance. This is modelled by a containment relationship.

In its turn, the *pnoVPTTP*-instance is bound by an instance of a Virtual Path Connection Termination Point belonging to a VpLinkConnection. Because not every one of these link connections needs to be visible across X.easi there is no containment between *pnoVPTTP* and *pnoVPCTP* .

The cardinality 0..n : 1 between OC *pnoVpLinkConnection* and *pnoVpCTP* describes that there can be VPCTP's (belonging to pnoVpSubnetworkConnections) without associated VP link-connections. The same applies to the cardinality 0..n : 2 between *pnoVpSubnetworkConnection* and *pnoVpCTP*. (There can be VPCTP's without associated *pnoVpSubnetworkConnections*.)

The cardinality between OC *interPNOTopologicalSubnetworkPair* and *pnoNWAtmAccessPoint* is 0..1 : n to account for the fact that a user-accesspoint is not attached to an *interPNOTopologicalSubnetworkPair*.

However, business model relationships between the VC Subnetwork and the related VP Subnetwork are not clear. It has to be assumed (at least for the Phase 1 solution in the present document) they are owned by the same Connectivity Provider as an administrative entity.

C.4.3 Relationship between VC Connections, VP Connections, Trails and Trail termination Points

A trail is an abstract concept which serves the VC Connection and is itself served by a VP connection. Figure C.5 summarizes the initial view of the relationship between these layers for a User-to-user Virtual Channel Connection.

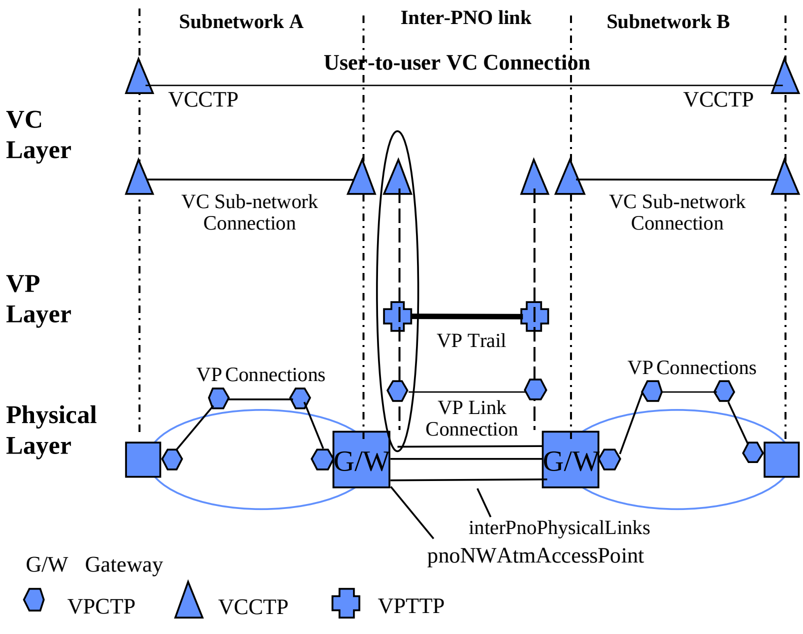


Figure C.5: Relationship between VP, VC and physical layers showing connection and trail topology

At the lowest level the physical layer provides the infrastructure for the VP Connections. The internal VP connections for each subnetwork are shown even though these are not visible across the X.easi interface; only the VPCTPs at the G/Ws need to be made visible to other PNOs.

Figure C.5 also shows how the VP Trails are formed using the VP link connection to support the VC connection in the layer above. The main thing to note is that there is a binding between the Termination Points especially at the pnoNWATMAccessPoints.

Regarding the overall connection types it should be emphasized that for X.easi the only trail that is of significance is the trail which is served by the Vp Link Connection.

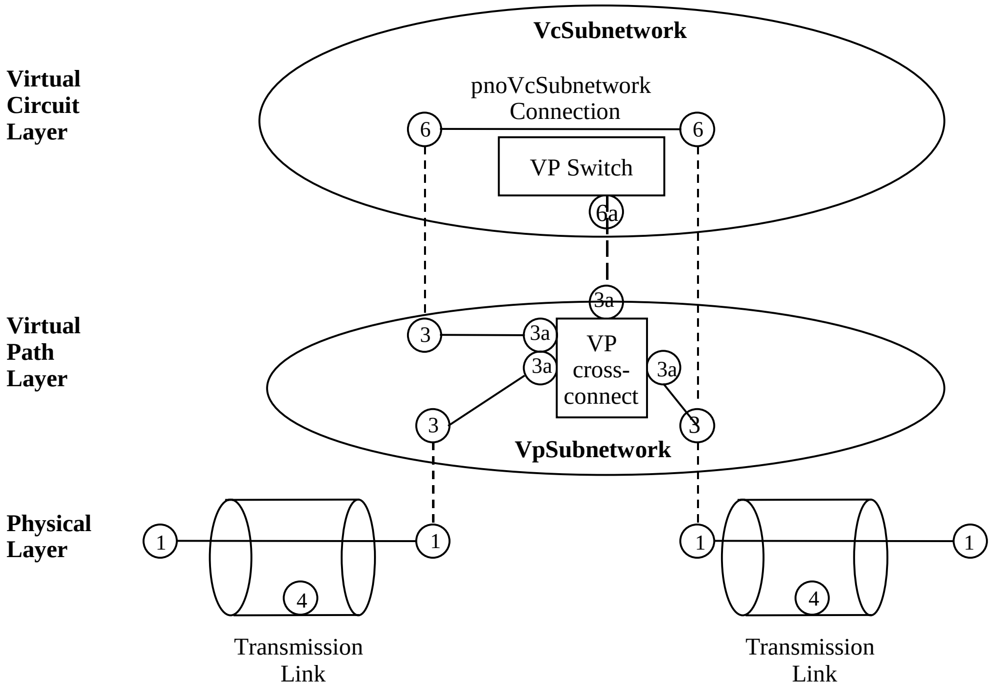
In [22] it is recommended to model only the abstract entities which need to be managed. In the case of the trail concept, only the VPTTP needs to be visible over the X.easi interface.

(In the case of an overall User-to-user VCC, the Vp Link connections that carry it over the interPno links do not need to be visible over X.easi; for the links, the VPTTPs will suffice. The situation is different when a Vp Link Connection is shown over the interface to serve as carrier for a User-to-user VCC.)

C.5 Example of the relationship of VP and VC objects to physical entities and identifier schemes

Figure C.5 in clause C.4 shows the modelling of VP and VP layer connections and trails. This subclause considers some aspects of a practical realization of the connection types in relation to the VP and VC objects and physical entities required to support end to end customer connections.

As an example, figure C.6 shows how the extension of pnoVpConnection termination points to identify links into inter-operator gateways (as defined in [1]) allows the currently-used identifier scheme [13] to be pragmatically extended to support ATM interconnect service operations.



Legend (referring to numbers in the Figure)
(1) pnoNWAtmAccessPoint (at the UNI or NNI interface)
(3) , (3a) pnoVpCTP at the Gateway or Cross-connect
(4) interPnoTopologicalSubnetworkPair
(6), (6a) pnoVcCTP at the Gateway or VP switch

Figure C.6: Example of internal PNO structure for international circuit designation

In this example, the PNO terminates some of the VPs from the pnoVpCTP Termination Points on internal terminations at a VP gateway crossconnect -these are shown as (3a). In current operational practice both termination points "3" and "3a" will be identified by designations defined by [13].

Some of these VPs can be connected to a Virtual Circuit Switch which then support the VC connections between pnoVcCTP Termination points. For the VCs a similar situation for designation will occur and both Termination Points "6" and "6a" above will be identified by ITU-T Recommendation M.1400 designations [13]. For further details on the numbering and addressing aspects in relation to the creation and management of ATM VP and VC services, refer to annex B.

C.6 Modelling the VP and VC bandwidth allocation within the data model

The data model developed in this annex, relating to PVP and PVC services, does not include any discussion of the requirements of interconnected ATM CPs for bandwidth allocation. Indeed, bandwidth allocation is an operational aspect of service provision which does not appear to have any influence on the data model. This is because the data model defines how management systems (OSSs) communicate with each other in order to establish and release resources associated with the provision of ATM services but is not primarily concerned with operator's policies as to the allocation of those resources.

For discussion on bandwidth allocation in relation to traffic and capacity management processes, refer to annex E.

Annex D (informative): Further details on Security processes and methodologies for the automated X.easi interfaces

Acknowledgement: annex D has been largely created from information contributed by: EURESCOM P710 [36].

D.1 Introduction

This annex starts by defining the general security requirements that are considered applicable for protecting a set of defined automated ATM X-interface (X.easi) management processes. Thereafter, a security solution is outlined together with a description of the implementation and experimentation effort being undertaken within EURESCOM in this context. Finally, some thoughts and recommendations for possible commercial exploitation are addressed.

D.2 Security Requirements

Automated X.easi interface security investments and the target level of protection should harmonize with the value of the assets that are at risk of being compromised.

Table D.1 is replicated from the main part of the present document to emphasize the overall security requirements identified as applicable for ATM X.easi interface management (some of which may have to be considered as applicable for Phase 2 only).

Table D.1: Security Service Requirements for ATM management

X-interface Security Services	Requirement Level	Comment
Peer-to-peer Authentication	High	Mutual authentication at the granularity of individual application or application entities is required.
Access Control at association establishment (*Only incoming access control is addressed*)	High	Access Control List scheme based on authenticated calling entity is preferred. Only incoming access control is addressed.
Access Control for requested management operations (*Only incoming access control is addressed*)	High	Access Control List scheme with supporting target granularity at the level of individual Managed Objects. Only incoming access control is addressed.
Access Control for notifications (*Only incoming access control is addressed*)	Low	Notifications should be accepted as long as they come from a known authenticated party.
Data Origin Authentication	Medium	The purpose of this service is to ensure prolonged authenticity of the communicating applications after association establishment has taken place. A full integrity service at application level will suite the same purpose.
Data Integrity Protection	High	
Data Confidentiality Protection	High	
Non-repudiation with proof of origin	Medium	Refer to the discussion at the end of this annex.
Non-repudiation with proof of delivery	Medium/High	Refer to the discussion at the end of this annex.

The security requirements listed in table D.1 are derived under the assumption that X.easi interfaces will be deployed with quite an extensive set of ATM VP/VC interconnect service operation processes supported in the configuration, repair, performance and accounting management functional areas.

This annex focuses on inter-operator security protection. Other related security areas (not elaborated in this annex) for which individual operators should ensure that adequate solutions are in place include:

- intra-domain (internal) threats to management applications;
- other network connection threats, e.g. from IP network connections into the TMN management platform.

Further general security requirements, for the X.easi interface should include [69]:

The X.easi security solution should be deployable in a multi-vendor TMN management platform environment.

- **To the extent that end-system integration is required, it should be as simple as possible to integrate the security solution with existing management platforms and management applications.**
- **In order to ensure a certain level of market acceptance and off-the-shelf security product support, the security solution should preferably conform to existing security standards, including emerging TMN security standards.**
- **The use of standard APIs for security services integration is preferred to facilitate easy replacement of security components and thereby a certain degree of security vendor independence.**
- **The solution should promote the reuse of management platform security capabilities, which possibly already exist, such as access control.**

D.3 Security Solution

P710 analysis has shown that, in order to provide an effective security solution, all services that require cryptographic transformations upon CMIP messages should preferably be communication protocol integrated.

Accordingly, the recommendation in this annex is to combine a basic DCN security solution with a complementary set of end-system application level security services as depicted in figure D.1.

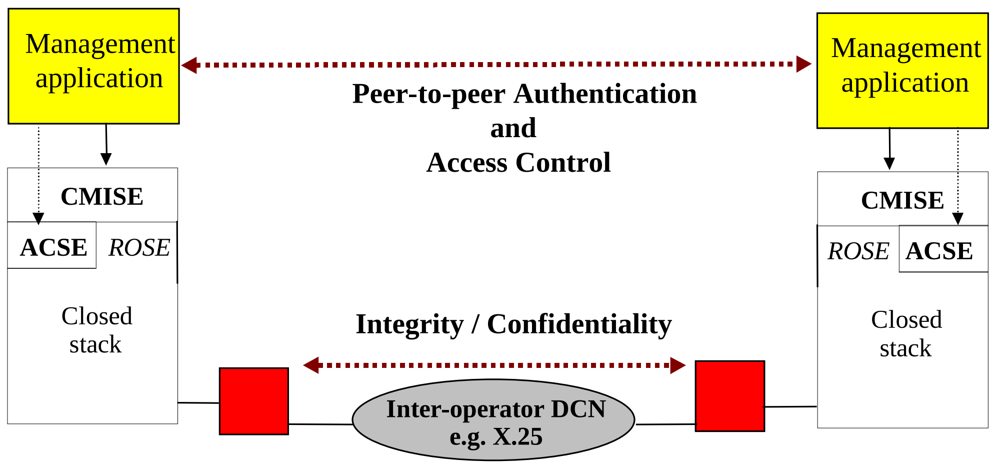


Figure D.1: Overview of Recommended X.easi interface Security Solution

The basic DCN solution will ensure integrity and confidentiality protection of exchanged management information (about interconnect service operation processes), on the basis that the (presumed) X.25 interconnections will be configured as a "closed user group" (CUG). Maintenance of secrecy of operator's X.25 addresses would have to be part of the Interconnect Service Operation Processes. (Millennium bug problems with X.25 circuits should not be overlooked!)

In addition, authentication and access control to operators' applications should be provided. The application level services will cover end-to-end authentication at the granularity of individual application entities including the necessary application level access control services. The only security service that is not supported by the depicted architecture is "non-repudiation" (a means of proving that the submission/receipt of a management message has taken place in case of a later potential repudiation dispute). The only way to get a good non-repudiation service for CMIP is through the use of STASE-ROSE [67]. This would also provide a much higher level of security for Integrity and Confidentiality requirements.

The following two subclauses respectively consider application level security solutions and DCN security solutions, in relation to the X.easi interface.

D.4 Application Level Security Solution

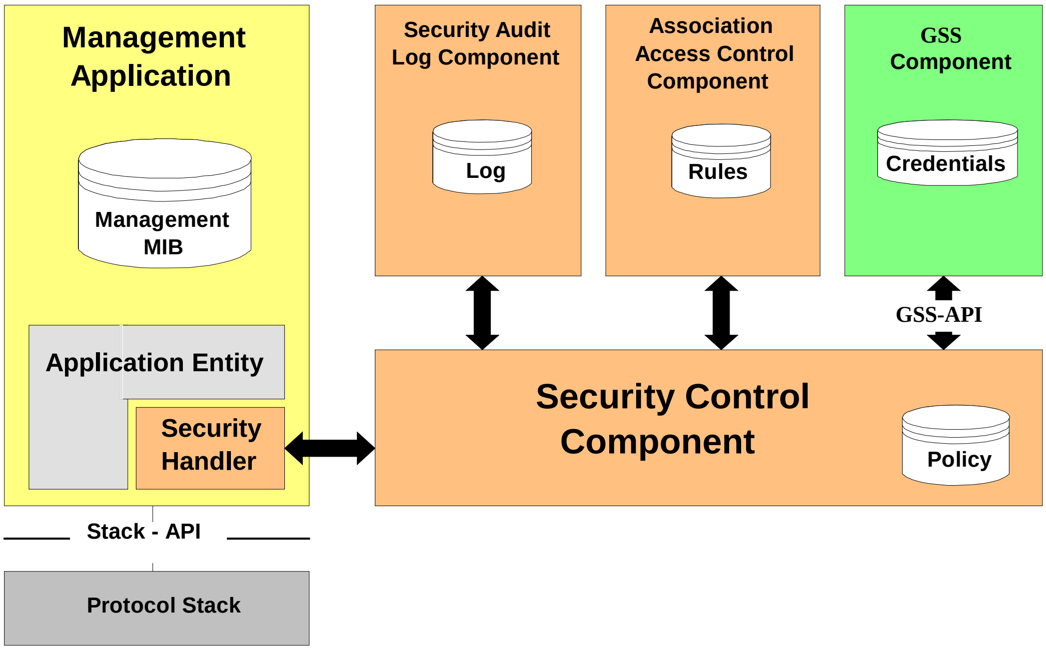


Figure D.2: Application Level Security Architecture

Figure D.2 depicts the chosen application level security architecture. The different architecture components are described briefly below:

Management Application Entity (MAE)

A Management Application Entity is, from a communications perspective, a distinguishable part of the management application (e.g. inter-operator CM processes). A MAE represents the entity that is authenticated at association establishment time. A single Management Application may consist of one or several MAEs and there may be one or several Management Applications running on the same management platform.

Security Handler (SH)

The Security Handler is a part of the Management Platform/System that handles all the security system interactions by communicating with the SCC. The Security Handler must be able to intercept and take control of all incoming and outgoing association establishment attempts. As opposed to the rest of the security architecture that may be platform independent, the SH implementation will be management platform specific.

Security Control Component (SCC)

The Security Control Component is the "intelligence" of the security system in the sense that its task is to co-ordinate the interactions between the other components of the architecture. The SCC behaviour for different types of communication sessions can be controlled through a dynamic configuration of a set of relevant security policy parameters. Different security policies can be configured for individual pair of communicating entities.

Security Audit Log Component (SALC)

This component is responsible for handling security audit logging. Relevant security information that is captured within the security system will be forwarded to this component for logging purposes. The purpose is to allow a security officer to audit security relevant events in connection with the establishment, release and abort of management associations.

Association Access Control Component (AACC)

The basic function of this component is to verify that the authenticated initiator entity is authorized to establish an association towards the requested target MAE. The database in figure D.2 contains the access control rules required for association access control.

Generic Security Services Component (GSSC)

The Generic Security Services Component should provide all the cryptographic functions that need to be performed and should be based on standard C-based API, GSS-API [53] towards the SCC.

The architecture should be designed to support the following important principles:

The SH logic and its interface towards the SCC are designed to be as simple as possible to ensure easy integration with existing management applications.

The SH is left to be the only platform dependent architecture component in order to ensure reuse of the other components within a multi-vendor TMN platform environment.

The use of GSS-API [53] provides a standardized solution for integrating cryptographic security services. This should ensure a certain degree of security product independence. In addition, since GSS-API [53] is a high level API, the effort needed for integration is minimal.

STASE-ROSE [67], if provided with GSS-API support, could be provided as an add-on capability at a later stage.

The AACC may be easily removed and an existing platform supported association access control system could be used instead.

The SALC can quite easily be extended to handle also security alarm reporting.

Access Control for management operations and management notifications has deliberately not been integrated with the platform independent security architecture. It is considered a better solution to consider these services separately. One reason is that their implementation probably needs to be TMN platform specific. Another reason is that several TMN platform vendors already are able to support these security services in one form or the other.

EURESCOM P710 and P708 have completed laboratory experiments to investigate commercial security products which are designed on the basis of many of the features listed above.

D.5 DCN (VPN) Security Solution

For Phase 1 automated X.easi interfaces, interconnection by an X.25-based DCN configured as a closed user group (CUG), may be considered as the practical and pragmatic solution. The requirements have been described previously in this annex.

Somewhat better than this would be to create a Virtual Private Network (VPN) as the DCN, using X.25 interconnection with additional hardware-based encryption devices under the control of each operator. Although desirable, this solution would create considerable (typically between 6 000 - 22 000 Euro per device depending on product) additional investment in hardware, software and inter-operator processes.

D.6 Implementation and Testing

Work has been undertaken in EURESCOM P708 to prototype, deploy and test security solutions associated with use of X.25 CUG's and commercial TMN platforms. The main purpose of this activity has been empirical validation of the solution's commercial applicability for future pan-European ATM service management and would therefore be suitable for the Phase 1 X.easi interface security management solution under consideration in the present document.

D.7 Commercial Exploitation

It is reasonable to state that commercial deployment of an automated X.easi interface without a reasonable level of security in place, would be unacceptable to both operators and their customers. Commercial TMN platforms that are available today have very limited support for X-interface security. If available, access control is the most likely service supported. For the security services that are not available, operators are left with two alternatives when considering an end system service integration, which are:

Integrate security services on the TMN platform in a way that does not require any modification to the management platform itself. This alternative is the one developed for EURESCOM P708 for testing authentication and access control in association with various management functions (i.e. at the applications level). As this implies a solution that is integrated above the platform API, the integration can in principle be performed by a 3rd party software developer, without any commercial support from the platform vendor. (In principle, the prototype solution that was developed in the course of the P710/P708 laboratory experiments could be made available, subject to EURESCOM approval, as a basis for a commercial development.)

The second alternative would be to persuade the TMN platform vendors into integrating security services as part of their commercial products. In this case security integration could be performed below the platform API, as a solution that might improve a few shortcomings of the "above the API" solution. Clearly, this could be an important area for cooperation with vendors interested in developing products suitable for ATM service introduction and management, in the inter-operator environment.

D.8 Concluding comments

This annex has discussed some of the details which operators and their associated equipment vendors should consider in relation to providing adequate security solutions for Phase 1 ATM service introduction, where managed using automated X.easi interface specifications.

Much more detailed descriptions of current and future solutions are described in various documents provided from the EURESCOM P710 project [36]. Some parallel standardization activities are also known to be taking place in ITU-T and these should be taken into account in ATM service deployment.

Note that from a European interconnected ATM services introduction perspective, the original ETSI TMN SEC group (standardizing security for TMN) was unfortunately closed down recently due to a lack of commitment from a sufficient number of partners. Hence, there is no specific TMN security activities going on within ETSI at the time of preparation of the present document. Activities are continuing within T1M1 and ITU-T. The only "important" document from ETSI is an approved EN on TMN Authentication. This EN is in-line with the P710 GSS-API solution and complies with STASE-ROSE.

Annex E (informative): Traffic and Capacity Management Processes

E.1 Introduction

This annex provides the linkage between the Interconnect Service Establishment and Administration processes, and the Interconnect Operation Process of Configuration Management.

It describes the Traffic and Capacity processes needed to support the X.easi operation. This support takes two forms:

Firstly it ensures that the capacity needed to support X.easi connection requests and reservations requested operate within the QoS targets agreed between operators.

Secondly it provides guidelines on the design and planning rules that must be used to achieve these targets, and most importantly, provides the rules that govern whether Xcoop connection requests and reservations requests can be accepted.

Much of the material is based upon selective extracts from the JAMES Project study on Guidelines on Design rules for ATM network planning. This annex limits itself to material related directly those issues identified above, and the needs of managing ATM Interconnection services. In order to provide sufficient context, some of the material used in the main part of the present document is replicated in this annex

E.2 Definitions

The majority of the definitions are taken from the JAMES documents. One term "ATM Link" has a special relationship with term Inter-PNO Physical Link in the ETSI X.easi standard. This is explained after the General Definitions, subclause E.2.1.

E.2.1 General

Manager: The single point of contact for each ATM Service Provider covering all aspects of the relevant process tasks.

A-End: The terminating manager taking prime responsibility for Deliverable.

Z-End: The terminating manager opposite the A-end.

PCP (Process Contact Point) - The person appointed for each process by an ATM Service Provider(ASP) with overall responsibility to ensure correct application of that process within the organization.

PA (Process Administrator) - Where X.easi has been adopted by a number of ATM Service Providers (ASP) in a multi-lateral agreement one PA for each process should be appointed. The PA will maintain liaison with the associated PCPs and assist in solving difficulties arising between ASPs during the running of the process.

Deliverable: Capacity to be offered/booked which can be either VPCs, or pure capacity on ATM links for support of future VPCs, PVPs, PVCs or SVCs.

M.1400 [13]: ITU-T Recommendation covering designation of capacity.

ATM subnetwork: a managed network resource that is able to switch ATM cells and to route and manage ATM connections. Three types of ATM subnetworks can be distinguished: VP, VC and VP-VC subnetworks. VP subnetworks can establish and manage VPs but not VCs and so they can switch VPs between different ATM links. VC subnetworks can establish and manage both VPs and VCs and can switch every VC (whether or not they start in the subnetwork) between different VPs. A VP-VC subnetwork is able to establish and manage both VPs and VCs; it can view the VCs carried on VPs starting or terminating in the subnetwork but it cannot view the VCs of the VPs not starting or not terminating in the subnetwork.

ATM Link: a Transmission Path (TP) interconnecting two ATM subnetworks. It is characterized by its **buffer capacity** (or buffer capacities, in case of more buffers, each of which is devoted to the cells associated to a specific class of service) and its **transmission rate** (e. g., for SDH systems, 45 Mbit/s 155 Mbit/s, 620 Mbit/s)

ATM connection: a VC or a VP.

VP switching: in an ATM subnetwork VP switching can modify the VP Identifier but not the VC identifier of ATM cells. VP switching allows to switch VPs between different ATM links.

VC switching: in an ATM subnetwork VC switching can modify both the VP Identifier and the VC Identifier of ATM cells. VC switching allows to switch VCs between different VPs, and then possibly between different ATM links.

ATM call: an "on demand" instance associated to a particular "switched service" from the calling user to the called user. An ATM call implies the establishment of one or more ATM connections, each with different bandwidth requirement and class of service characteristics, and with the same or the opposite direction of the call. A call can be accepted or refused by the CAC rules that are applied to each connection taking part in the call, depending on the state of occupancy of the network resources.

VP: a unidirectional user-to-user, user-to-network or network-to-network Virtual Path Connection. A VP has to be established on a chain of ATM links between the source subnetwork and the destination subnetwork of the connection; in other words a physical path is necessary to route the VP over the network. At every intermediate subnetwork, between the source and termination of a VP, the ATM cells belonging to that VP are subjected to "VP switching".

VP subnetwork: set of network-to-network VPs that have the same permanent and performance characteristic. Each VP subnetwork is characterized by the class of VC connections it has to carry and by an associated GoS requirement.

VC: a unidirectional user-to-user Virtual Circuit Connection. It can be supported on a VP subnetwork. A permanent VC is established on a chain of VPs between the source subnetwork and the destination subnetwork of the connection; in other words the VC is routed over a logical VP subnetwork. For a given VC established on a path of VP, the ATM cells belonging to the VC are subjected to "VC switching" at every VP termination.

Figure E.1 illustrates an ATM link of Capacity C. ATM links can have one or more buffers, depending on the implementation.

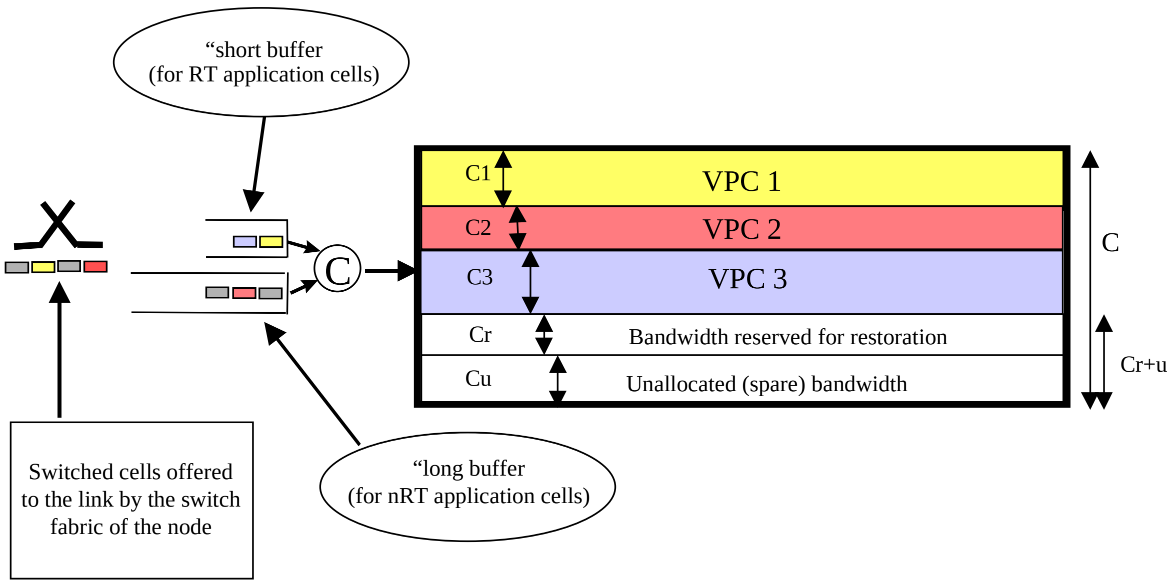


Figure E.1: Resources involved and capacity partitioning between VPs, Restoration bandwidth and Unallocated bandwidth in an ATM link

In the example of figure E.1 two buffers are associated to the ATM link: a "short" buffer for Real Time (RT) application (class I) and a "long" buffer for non Real Time (nRT) application (classes II, III and U). The illustrated ATM link carries three VPs: VP 1, VP 2 and VP 3, whose capacities are C1, C2 and C3 respectively. VP1 and VP3 supports connections for RT application, VP2 supports cells for non Real Time applications. The Unallocated Bandwidth is also represented and its Capacity is Cu = C - (C1 + C2 + C3 + Cr), where Cr is the bandwidth allocated for restoration purposes only.

Termination Point (TP): It denotes the end point of a connection at a specific layer. Depending on the direction of the connection, a TP can be Originating/Source or Terminating/Sink.

VP Link (VPL): Connect two subnetworks where VP identifier is terminated or translated.

VP Connection (VPC): Connect two subnetwork points where VP layer is terminated, and VC identifiers are translated.

VC Link (VCL): Connect two subnetworks where the VCI value is translated.

VC Connection (VCC): Concatenation of consecutive VCLs between two network end-points (ingress or source and egress or destination).

E.2.2 For a specific ATM Link

Link Bandwidth: Bandwidth available for corresponding link connection at ATM layer.

Total allocated bandwidth: Sum of all allocated bandwidth at VP layer.

Total used bandwidth: The part of total allocated bandwidth that carries actual user plane traffic.

Total unused bandwidth: The part of total allocated bandwidth that does not carry any VC user plane traffic, including bandwidth allocated for restoration.

Restoration bandwidth: Bandwidth pre-allocated at the link for restoration purposes. Its use is strongly related to the survivability strategy adapted.

Unallocated bandwidth: The bandwidth of the link not reserved for any use.

E.2.3 For a specific VP link defined on an ATM Link

Allocated bandwidth: Bandwidth reserved for a certain VP Link that traverses the ATM link.

Used bandwidth: This part of the allocated bandwidth that at a given time carries user plane traffic.

Unused bandwidth: This part of the allocated bandwidth that at a given time is not occupied by user plane traffic.

In short, every VPC gets some allocated bandwidth on an ATM link. Part of this bandwidth will actually be used for user plane traffic, whilst part of it may not be used at any given point in time. Of the remaining bandwidth, some is reserved for restoration purposes, while other is totally unallocated. It is the aim of efficient and intelligent resource management to minimize the total of unallocated and unused bandwidth within the network. This may be at the local level by adopting an intelligent multiplexing scheme for the individual traffic flows, and at the higher level by fine tuning the VPC layer to support the offered traffic at the network boundaries.

An example of segmentation of physical capacity on an ATM link is provided in figure E.2.

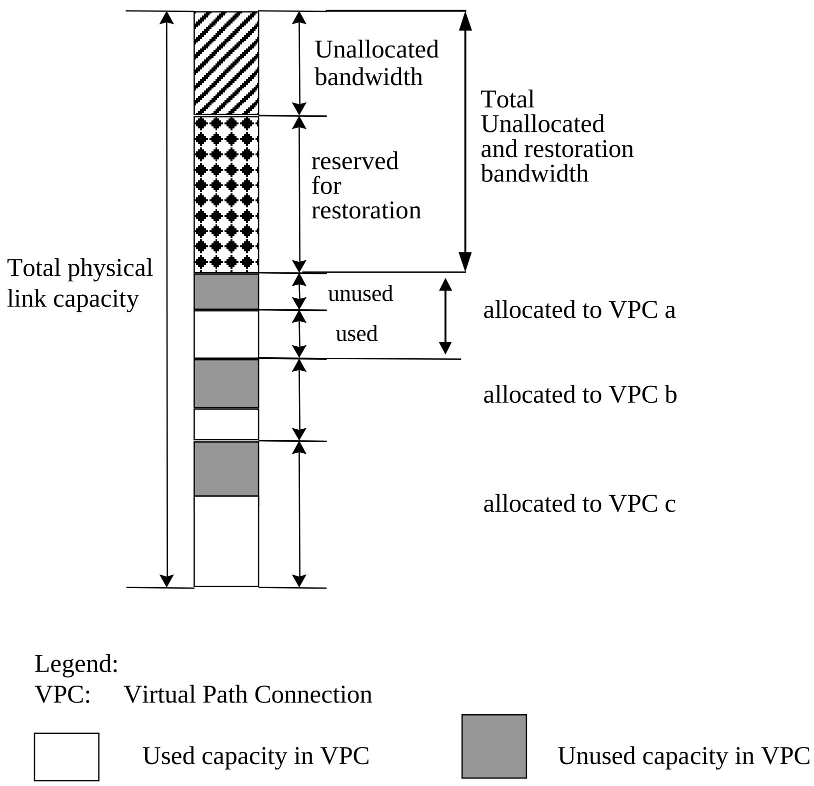


Figure E.2: Segmentation of Physical Capacity

E.2.4 Mapping of terms to the ETSI X.easi interface

ATM Link and IPPL

The terms ATM Link defined here and Inter PNO Physical Link (IPPL) are closely related. The IPPL definition comes from the ETSI X-interface standard [6], and is used to represent the physical requirements for interconnection to support the ATM Connections. For the purposes of traffic and capacity planning the IPPL is regarded as representing the ATM Link for the purposes of QoS calculations because both the losses in buffers and the effects of cell blocking on the link need be represented.

In the calculation of QoS for end to end connections, the QoS is segmented as follows:

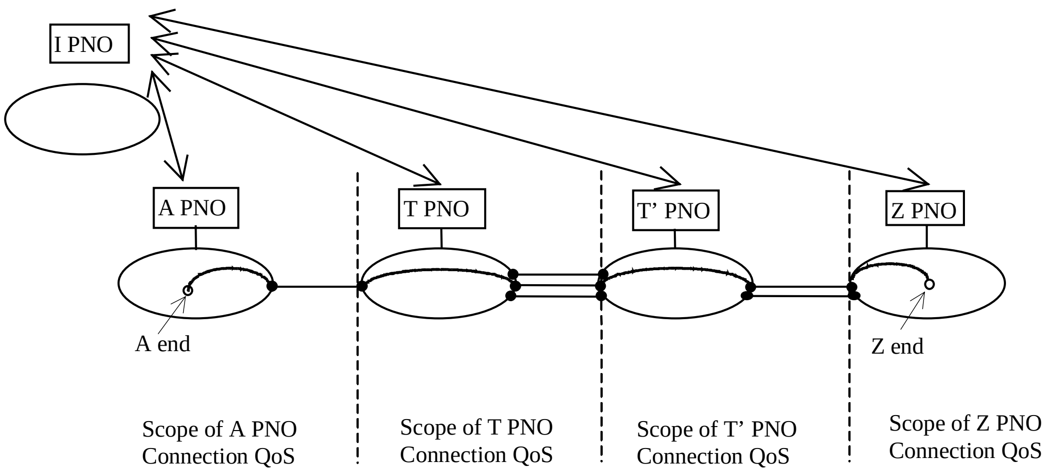


Figure E.3: Scope of QoS segmentation

From figure E.3 (derived from figure 5 in the main part) it can be seen that the ATM Interconnection Services have different scopes for the QoS. In the cases of the A-PNO , T-PNO and T' PNO connections the QoS in each case includes the subnetwork QoS, and the ATM Link QoS. The latter is made up of the Gateway QoS (ATM switch buffer loss), and the IPPL QoS (cell loss due to unavailable link capacity). In the case of the Z-PNO the QoS includes the subnetwork QoS and the Gateway QoS (ATM switch buffer loss).

E.2A Introduction to Traffic and Capacity Planning

Clause E.2A describes how Traffic and Capacity Planning (also known as Network Dimensioning) should be implemented by the NM OSS supporting the Phase 1 X.easi interface. Most of the model is derived from JAMES Deliverable G2-WP2 *"Guidelines and design rules for ATM network planning"*.

ATM Traffic and Capacity Planning focuses on the planning processes supporting the Interconnect Service Establishment Process (ISEP) and the Interconnect Service Administration Process (ISAP). Refer to clause 7 in the main part. The Capacity Planning processes support the ATM interconnect services - PVC, PVP and SVC as specified in Phase 1 and Phase 2.

Traffic Capacity Planning includes the following options:

ATM Service Provider is planning capacity on ATM links that can be used as VP or VC links.

ATM Service Provider is planning a VP network consisting of several VP connections(VPC).

ATM Service Provider is planning a VC network consisting of several VC connections including PVC and SVCs.

E.3 ATM and Physical Layer Planning

From the dimensioning point of view in an ATM network it is possible to distinguish between two distinct layers: the ATM Layer and the Physical Layer.

The **ATM Layer** includes:

- the set of VPs subnetworks, that are used to carry out the user-to-user VP and VCs belonging to separate classes of connections;
- the set of ATM Links/IPPLs that are needed to carry the VP/VC connections between subnetworks.

The **Physical Layer** is constituted by the set of Transmission Bearer Layer Connections (i. e. Transmission Paths) of the network that are provided to support the ATM Links between Operators. Within the X.easi specifications ATM Links are modelled as Inter PNO Physical Links (IPPLs). The Physical Layer eventually maps on the Physical Media Layer.

The term "ATM Links" corresponds to the combination of the IPPL together with the ATM cell buffers in the ATM Gateway.

The ATM Layer resources are represented by the entities shown in figure E.4. Also shown are the Physical Layer resources that for the ETSI NNI.easi [1] implementation consist of an SDH/E3 Layer and a Physical Media Layer.

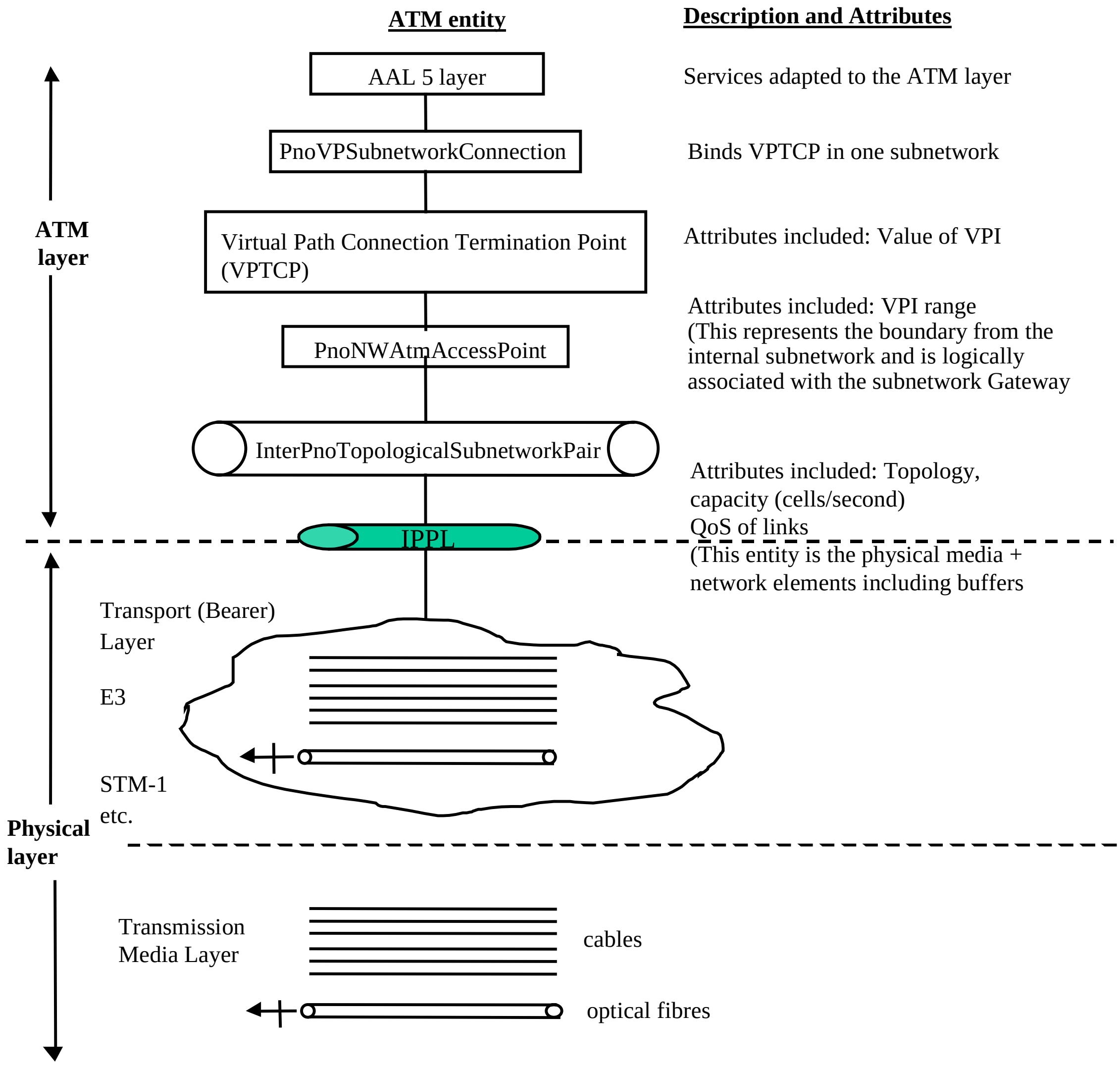


Figure E.4: Planning Resources for the ATM layer

The Planning processes in the present document focus on the ATM Layer and have to produce forecasts in two timeframes:

- a medium term timeframe to forecast the capacity requirements at the ATM layer typically 6 to 12 months ahead; and
- a long term timeframe (12 to 24 months) to provide input to the Physical Layer planning that is needed to provision the Physical Layer capacity to support the ATM Layer Capacity requirements on the IPPLs.

This is illustrated in figure E.5.

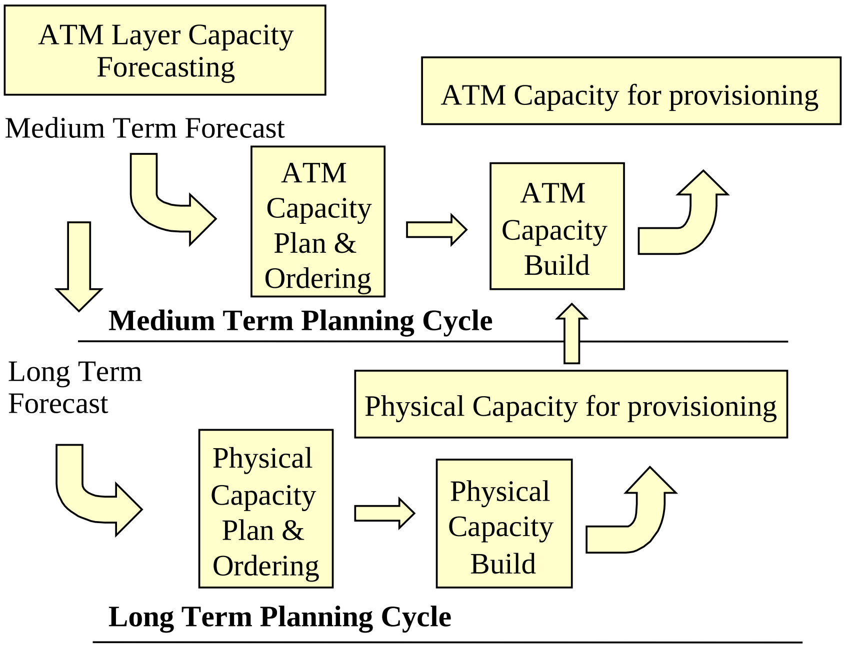


Figure E.5: ATM Capacity Forecasting relationship to Planning and Build

Figure E.5 illustrates how the ATM Layer Forecasts are used to drive the Capacity Ordering and Capacity build processes of the ATM Layer and the Physical Layer. One specific concern with ATM multi-service networks is that forecasting capacity involves more complex rules than is the case with traditional Circuit Switched constant bit rate networks. This is discussed in clause E.4.

The medium term forecasts are used to drive the Plan, Order and Build processes for the ATM Layer resources, so that when Configuration requests are received, the planned service QoS is achieved.

The long term ATM forecasts are used to drive mainly the Physical Layer Capacity Plan, Order and Build processes. These provision the physical infrastructure that support the IPPL requirements. These long term forecasts may also be used to plan long term call-off contracts with ATM resource suppliers.

E.4 Planning functions

The **ATM Traffic and Capacity Planning** (also known as Network Dimensioning) is a **task/function** whose:

> **inputs** comprise of both qualitative and quantitative information about the elements characterizing the network and a forecast of the future requirements (for both ATM and Physical Layers).
>
> **outputs** are specific dimensioning proposals for the future elements characterizing the network and specific operational rules for utilizing those resources - i.e. mainly the size of network resources and parameters for traffic control schemes.

Underpinning this task is the need to have a set of design rules and principles for taking raw forecasts of ATM capacity and determining the technical capacity requirements on the components in the ATM Layer and indirectly on the Physical Layer.

There are two aspects to this task:

> Firstly the capacity forecasts have to be presented in an agreed form between operators and
>
> Secondly the operators have to agree how they map the "raw" ATM Capacity requirements onto the capacity forecasts for the ATM and Physical Layer capacity.

Capacity requirements

Figure E.5 shows how each operators' ATM Capacity Forecast process results initially in a statement of ATM Traffic Requirements.

This is a multidimensional statement in the form of a list which forecasts for each subnetwork and inter subnetwork link (IPPL):

the interconnect service (A,T, Z-PNO connection) being requested by an initiating PNO;

the ATM Connection Type(s);

the ATM Transfer Capability including QoS;

the Source Traffic Descriptor that characterizes the cell rate requested;

this latter parameter needs to be modularized into ranges for two reasons:

- to make the mathematical calculations tractable.
- to align with the constraint that services and products offered to customers will most likely be based upon modular increments of cell rate capacity rather than a continuum.

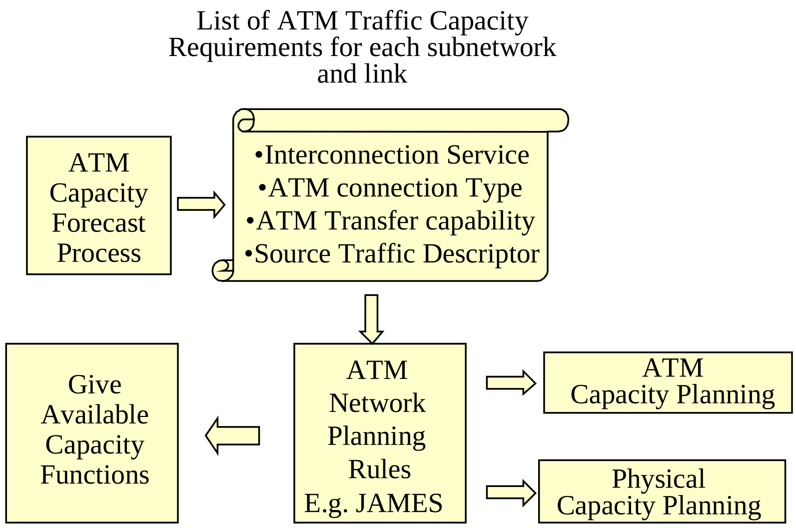


Figure E.6: ATM Capacity Forecasts and Planning Rules

The Capacity Requirements are input to a set of ATM planning rules that are used to determine the specific capacity requirements in the ATM Layer (ATM Capacity Planning) and in the Physical Layer (Physical Capacity Planning). These planning processes are assumed to have available to them the information on the current deployed capacity.

An important part of the forecasting is to determine the Effective Bandwidth of the VBR ATM traffic.

The recommended approach is the use of the Lindberger- Tidblom method. The Lindberger-Tidblom method is optimal for a network planning tool where a huge amount of iterations are performed. The results can be improved after the optimization procedure has been executed by using more exact methods on each ATM link. The routing has then been decided as part of the optimization procedure. For each ATM link an offered mix of traffic of different characteristics, as a result of forecasting and routing decisions, can then be used to calculate the needed capacity (final calculation) as a function of connection blocking objectives (e.g. multi-dimensional Erlang function, UUA). Refer also to subclause E.5.3.

Operation Processes - Give Available links

The way in which this operation process and function operates is completely predicated on the business model (described in clause 6) and the Network Planning rules. These rules provide the algorithms for the operational Configuration processes to determine whether an individual request to reserve additional capacity in a subnetwork or on the IPPLs can be satisfied or must be rejected.

E.5 ATM Layer Planning

The following subclauses describe the assumptions, principle and policies for traffic and capacity planning.

E.5.1 Find the way to carry ATM traffic over the ATM network

The EASI NNI specification [1] requires that VC connections are established on VP logical subnetworks. This means that the VP subnetwork topology must be determined by the planning process before the VC connections are assigned and the VP capacity determined

The NNI specification also requires different ATM VC connection types to be segregated onto different VP Connections.

If subnetworks are used, it is necessary to assign connection classes to each, and choose a topology.

Requests for end to end VP connections are mapped onto subnetwork connections across networks whose termination points are associated to ATM Network Access Points. These ATM Network Access Points are modelled as pairs that must be associated with the topology of the interconnecting Inter PNO Physical Links (IPPL).

PVC and SVC have to be mapped onto PVPs that have been pre-provided to connect to the appropriate switches or cross-connects at the PVC and SVC levels.

The ETSI NNI.easi specification [1] requires that a specific VC is mapped onto a VP that is dimensioned to meet the most stringent QoS requirement of the set of VCs offers to that VP. It does not, however, state how this is determined.

E.5.2 Find a logical topology for each subnetwork

Topologies can range from tree-like to fully meshed. The requirement is to define the topology of each subnetwork. The logical topology of IPPLs derives directly from the physical topology of the network.

The topology of interconnection to the VP subnetworks is modelled as an "Inter PNO Topological Sub Network Pairs" entity that records pairs of ATM Network Access Points that represents the topology of Inter PNO Physical Links (IPPLs).

E.5.3 Size the VPs of every VP subnetwork and/or the capacity reservations on each IPPL of each ATM link

This step concerns the dimensioning of VPs and capacity reservation on IPPLs. In general a model is necessary to represent the traffic over the network and this aim is based upon achieving the QoS requirement at call level.

JAMES determined that, given a forecast of total effective bandwidth, the sizing of the links depended on calculations of the QoS/GoS required on the ATM Links/IPPL.

The approach recommended in JAMES is the use of the Multi-dimensional Erlang Loss formula using two forms of numerical solutions: (i) the Lindberger approximation to carry out initial designs as the method is computationally efficient and (ii) to use the Uniform Asymptotic Approximation (UAA) method that gives the most accurate results.

E.5.4 Determine schemes and parameters associated to connection traffic control

This addresses aspects that are strictly connected with logical dimensioning. Most connection and traffic controls are known *a priori* and are inputs to the dimensioning task, but some traffic control parameters constitute an output of network dimensioning. For example, where alternative routes for switched calls are allowed, but the routing plan was not assigned, the search for the optimal routing plan could constitute one of the aims of the dimensioning task.

Another example could be the schemes to be adopted in order to protect some particular classes of connections when a mixture of classes are offered to the same logical subnetwork: in some cases these schemes can be *a priori* known while in other cases they have to be designed.

In the Design Process, Physical Layer sizing and routing of ATM connections are closely related.

E.6 Physical Layer Planning

E.6.1 Size the IPPLs in number, position and capacity

This is derived directly from the routing and assignment of VPs and VCs forecasts to IPPLs (ATM links) using the traffic an dimensioning rules.

E.6.2 Route and assign the VPs to the IPPLs (ATM link)

From another but complementary point of view, the routing and assignment of logical resources to ATM links can depend on the available capacity, position and size of the IPPL Links available within the interconnected network. In general a good approach to solve the dimensioning problem at physical layer should simultaneously take into account both ATM VP assignment of IPPLs, and IPPL capacity and location requirements.

E.7 Common planning for both ATM and physical layer

The business objective is to satisfy QoS requirements and implement the network in such a way that its economic cost is minimized.

Both network cost and QoS involve the network planning as a whole. At the Physical layer where there is no statistical multiplexing the QoS considerations are simply related to bit rate capacity and transport bearer transmission specifications.

In the case of the ATM Layer, where traffic of different types and statistical characteristics is supported, the QoS performance must be derived by statistical methods and calculations. QoS concerns both cell level and call level objectives. In general cell level QoS constraints (probabilities of delay and cell losses) are taken into account by assuming the same criterion (formula or algorithm) used by CAC in the evaluation of the equivalent bandwidth of the connections. Call level QoS objectives (probability of call losses) can be evaluated by an adequate call traffic model at network level.

A cost function taking into account the economic effort in implementing the network can be used in order to achieve a near minimum-cost solution. One of the most difficult tasks to overcome when introducing a cost criterion is to formulate a cost model for the network, because of the great complexity in evaluating the relative weight of different cost components (switching, signalling, routing, transmission and so on) contributing to the total cost. The use of an economic criterion to dimension the network is recommended whenever possible but it is not indispensable. Network resources can be sized only taking into account QoS constraints. When a cost criterion is assumed and QoS objectives are assigned the Network Dimensioning can be formulated as an optimization problem.

Many approaches are possible to face the ATM network dimensioning problem. In general tackling the task as a whole is not realistically possible due to huge complexity in trying to solve the entire problem in one step. In general, use of an approach that divides the problem into a certain number of sub-problems reduces its level of complexity and make it possible to find a solution in terms of algorithms.

E.8 Planning information

The following information must be available to be used by the planning functions, and everything not strictly related to internal management must be distributed by means of X.easi manual or automated processes.

Network Topology.

Interconnection Service Types (Originating , Transit, Terminating).

Set of ATM Connection services and their characteristics (Virtual Path, Virtual Channel Deterministic Bit Rate, Statistical Bit Rates).

Traffic requirement for each type of service Source Traffic Descriptor: PCR, SCR, Max Burst size, …

QoS at cell and call level for each type of service, CDVT, Cell Loss Rate, Cell Error Rate, …

Integration/segregation service policy and service protection scheme.

Routing strategy.

Strategy used at logical layer to carry out the traffic over the network, using or not using VP subnetwork to carry out different classes of on-demand connections.

Size of network resources (VPs and links).

Routing structure (number of routes and routing constraints).

Set of matrices (a busy hour traffic matrix for each service class).

Set of call blocking constraints (a maximum blocking probability for each service class).

Set of cost coefficients.

Global network costs.

Set of call blocking probabilities.

Mean offered traffic (Erlang).

Effective bandwidth (Bandwidth units).

Peakedness factor.

E.9 ATM Layer Medium Term Planning Process

Figure E.7 gives an overview of which processes interact with other processes, such as with each Operators' internal processes and with the planning processes managed by other Operators.

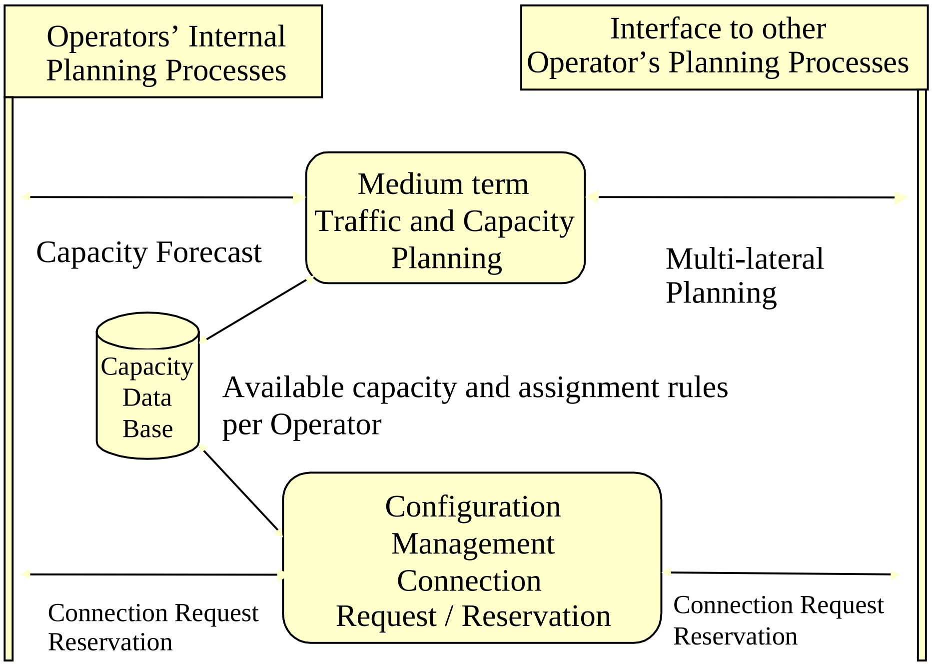


Figure E.7: Overview of Medium Term Planning Processes

Figure E.7 show that the Medium Term Planning (MTP) process builds up a database of ATM Layer Capacity and the assignment rules that govern its use by the Configuration Management Process using the X.easi interface.

The Configuration Management process updates the state of the capacity in the database as it is assigned and reserved and released. The MTP updates both the capacity and its state and all the rules for assignment. These can be used to limit the Configuration request by an interconnected operator to the forecasts agreed and within the Multi-lateral planning process which would have also established the business model agreements.

E.9.1 Medium Term Planning (MTP)

E.9.1.1 Definition of MTP

The Medium Term Planning (MTP) process produces a 6 to 12 month plan for the capacity needed for provisioning of SVC, PVC and PVP services. It may be triggered by periodic forecasts or may be reforecast to take account of specific planned events (such as major sporting or public events). The plan is the result of an optimization procedure between capacity offers and requests performed all Operators.

E.9.1.2 Objectives

The Objectives of Medium Term Planning are:

- Optimize network resources for a 6 to 12 month period on the basis of capacity forecasts.
- Produce a medium term plan for SVC, PVC and VPC capacity implementation.
- Achieve standard processes between all Operators.

E.9.2 Medium Term Planning Responsibilities

MTP Process Contact Point (PCP). The person within each ATM Service Provider (ASP) with overall responsibility for ensuring the implementation of MTP within that ASP.

MTP Process Administrator (PA). The Process Administrator is one of the MTP PCPs appointed to oversee the development and co-ordinate the running of the process.

The functions of a PA include:

- definition and control of the time scheduling of the Process (Support Planning Meeting organization);
- validation of static data (information related to network elements) at the end of the preparation phase (see below);
- control of common data broadcasting procedures at the end of the Process;
- assistance in solving difficulties arising between Operators in the implementation of the Process.

E.9.3 Medium Term Planning Inputs and Outputs

E.9.3.1 The MTP Inputs

Each PCP receives as input for MTP activities:

- from the MTP PA: Topology map (IPPLs/ATM links and ATM subnetworks) received from the CM PA. (The CM PA is the Process Administrator responsible for configuration management of ATM VPs and VCs. This is taken to be equivalent to the "Short Term Planning PA" described in JAMES and is discussed further in clause E.6.)
- from the CM PCPs: current fill level of IPPLs/ATM links.

E.9.3.2 MTP Outputs

Each PCP provides as output of MTP activities:

- to the MTP PA: The complete list of new, planned or withdrawn Capacity with RFS dates;
- to the relevant CM PCP: Expected capacity fill level of existing or planned ATM links with reference to the A-end forecast source.

E.9.4 Medium Term Planning MTP Process Description

Process Overview

The MTP Process is a co-ordinated process in which PCPs perform their activities in accordance with a given schedule. The MTP PA will provide in advance a detailed schedule including starting and finishing dates of the activities.

MTP Process can be divided in 4 different phases, which are elaborated below:

1) Preparation phase
2) Forecast elaboration and message exchange
3) Network optimization
4) Results broadcast

1. Preparation phase:

During this phase information regarding network elements is updated (Static Information). At this point MTP PCPs can introduce new planned network elements. They may also confirm or withdraw in-service network elements and resources.

At the beginning of this phase the most recent update of network elements issued by the CM PA is distributed. MTP PCPs discuss bilaterally the confirmation or introduction of network elements. Once an agreement is reached they sign a specified form for each type of element, containing all required information to be sent to the MTP PA for validation. This activity should be concluded before the start of any general gathering meeting for capacity forecast. The validation procedure performed by MTP PA consists of a check of the correctness and completeness of the received static information and in giving a unique reference number to the new network element.

2. Forecast elaboration and message exchange:

During this period PCPs input their agreed forecasts into the MTP database and run processing programs in order to produce messages to be sent to other relevant PCPs. At the end of this exchange procedure capacity forecasts are collected on a Links basis.

The PCPs input the results of a general meeting for gathering capacity forecast into a database MTP module. The database translates each capacity forecast from a sequence of Border Crossings into a corresponding forecast stated in terms of individual related Links. PCPs complete deliverable routing once this association procedure is complete. The deliverable forecast, originally expressed on a Border Crossing basis, is now translated in terms of Links. PCPs process the data utilizing the database which automatically produces messages, in paper or electronic format, to be sent to the relevant A-End PCPs of the Links involved. At the end of this phase each PCP collects capacity forecasts concerning those Links for which he is the designated A-end. Message exchange procedures can be performed before or during a global meeting for capacity planning (Support Planning Meeting).

3. Network optimization:

ASPs convene bilateral meetings in order to evaluate and agree on network elements and resources to be planned in order to meet with the expected deliverable requests. They check allocation of forecasted capacity on the agreed network elements and prepare feedback messages to Operators requesting capacity.

Having considered the capacity forecasts and other, more general, reports PCPs meet bilaterally during a Support Planning Meeting to decide:

- how to compose ATM subnetworks and ATM links in order to offer Capacity in the most optimized way;
- how to allocate expected capacity requests.

4. Results broadcast:

PCPs broadcast, globally, planned new network elements. They also transmit individually to the other PCPs the relevant detailed allocation of estimated capacity on the planned elements.

MTP PCPs produce a list of new network elements (agreed during bilateral meetings) to be declared as "planned", with the relevant characteristics (RFS, length etc.) and send it to the MTP PA for validation. Once this has been obtained, PCPs will send the results of capacity allocation, on the network elements, individually to each relevant deliverable I-end PCP. Note that in the X.easi environment the Initiating end may be the A-end operator or another. This is different from the earlier industry solution where the I-end PCP was always the A-end PCP.

Results of the capacity forecast (with the requesting I-end ASP indication) are the main output to the relevant CM PCPs. This information is shared by MTP and CM PCPs using some method such as a common database, groupware or paper documents. The same database is supported and displayed as below in figure E.8, in histogram format. This can then can be utilized and updated by CM PCPs during the implementation phase.

Capacity #n

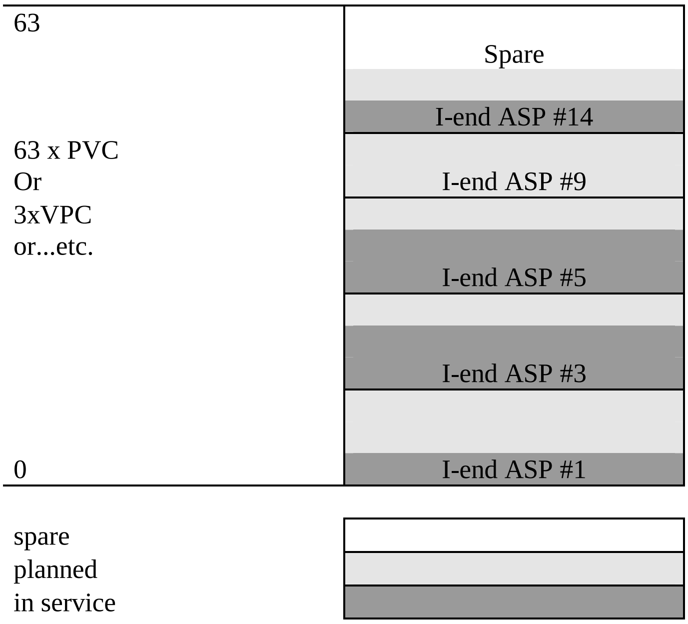


Figure E.8: Capacity Planning Histogram

E.10 Short Term Planning (STP)

In the industry and also in the JAMES Project, the processes for providing an interconnected VP connection have been and continue to be undertaken manually, in general. As the assignment of VP connections involves some "design and routing" assignments this is sometimes referred to as "Short Term Planning". These processes are exactly equivalent to the Configuration Management (CM) processes described in clause 9 of the main part of the present document. Accordingly, the term "Short Term Planning" is not used further or elsewhere in the present document and all relevant operations within this context are taken to be part of the CM processes.

Annex F (informative):
Positioning the X.easi interface in the TMN architecture

The basis for the Network Management solution, described in the main part of the present document, is the ITU-T Telecommunication Management Network (TMN) Architecture and principles, which are elaborated in detail in ITU-T Recommendation M.3010 [62].

Further details about the TMN approach to modelling all pertinent aspects of network management are described in many ITU-T Recommendations (M.3000 series, X.700 series, Q.800 series, etc.).

Within TMN, a Logical Layered Architecture for operations support functions (OSFs) is used which separates the OSF functions into those concerned with the Business Management, Service Management, Network Management, and Network Element Management Levels. This is depicted in figure F.1 in which the position of the X.easi interface is also indicated. Note that the X.easi interface is at both the Service Management and Network Management levels.

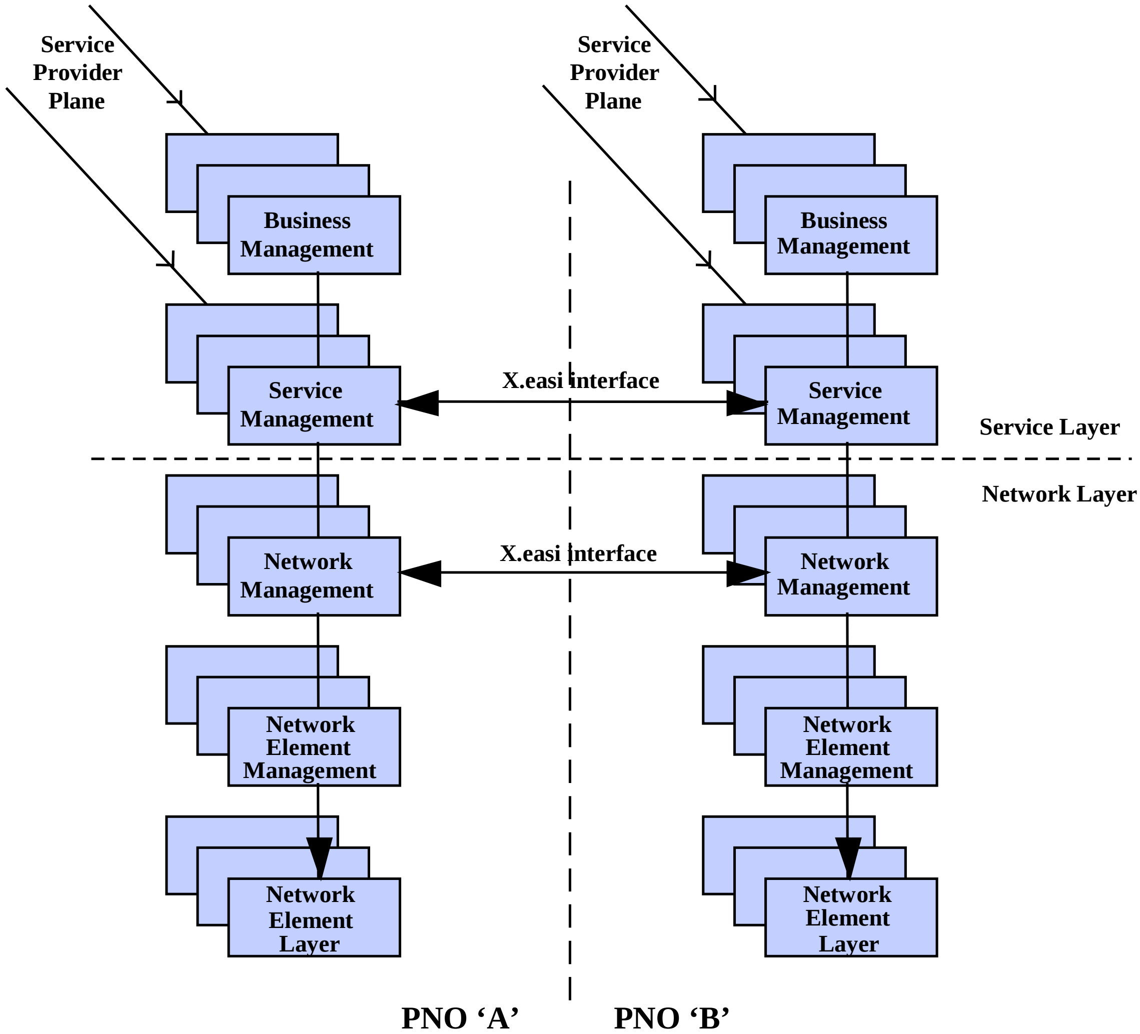


Figure F.1: Management Function Blocks and the TMN Layered Architecture

In figure F.1, the network management functions are taken to include Link and Network topology management with the exchange of information between operators on these functions taking place over the X.easi interface.

In addition to the basic layered architecture and interface reference point concepts, [62] provides examples of various functional architectures for the interconnection of PNO and other Service Provider (SP) resources. This is also depicted in figure F.1 where the diagram shows an example of two PNOs each of which could be interconnecting with a value added service Provider. For each level in the Logical Layered Architecture a set of logical Function Blocks is grouped within a Management system at that level, in order to facilitate the interconnection of one (or more) SPs. Other configurations are possible but this model is sufficient to explain the logical positioning of the of the X.easi network management interface within overall TMN architecture concepts.

Annex G (informative): Case studies on the degree of automation of interconnect processes

Interworking between Automatic and Manual Interfaces.

The concept of Manual and Automated X.easi interfaces is introduced in subclause 5.6.2.

This annex aims to provide a step-by-step description of the processes required to operate the X.easi interface, depending in particular on the relative level of automation of the interface under consideration.

In operation, the main problem that is likely to occur between cooperating operators (due primarily to the different level of automation which any particular operator may choose to provide) is that operators will have to enact different processes. Specifically, this will be dependent on the level of automation of the interface of the partner. For example, a situation may occur where, in order to set up an ATM connection crossing several administrative domains, an operator has to interact manually with some domains but is able to interact automatically with others, whilst having to keep relevant data bases consistent and updated accordingly.

The scenario and terminology on which this annex is based are depicted in figure G.1.

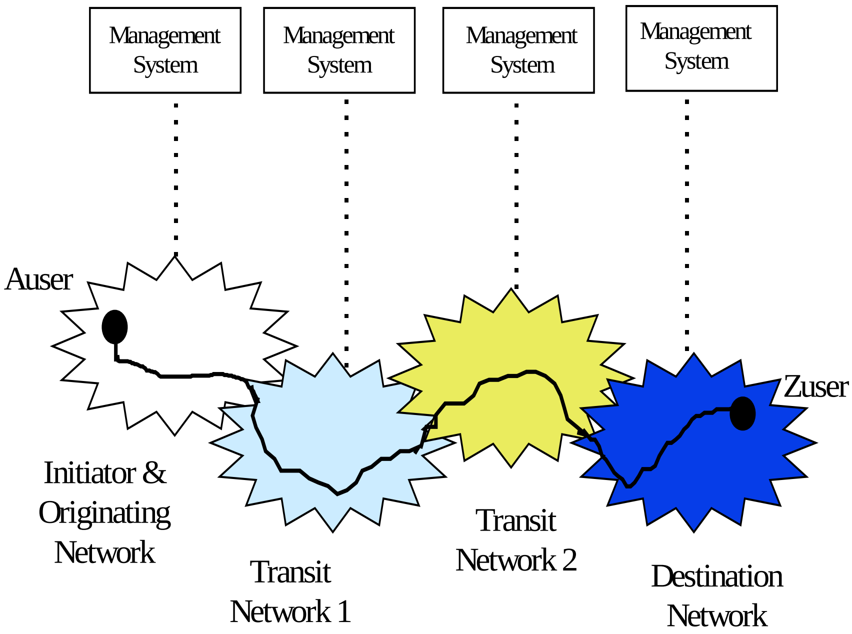


Figure G.1: Management Systems and Networks scenario

Case Studies

The three main cases identified are summarized in table G.1 and analysed in the remainder of this annex. For the example of Case 1, a reference diagram is provided and the process is divided into steps which are subdivided into "sequences", one for each interaction of the Initiator operator with the other cooperating operators.

The "Automated" case is sub-divided into two categories, as described in subclause 5.6.2.2:

- Automated (X+Q) implies computer-based communication between inter-operator management systems (X) and near-simultaneous computer based links to the underlying ATM network technology (possibly implemented on the same computer platform) in any given operator's jurisdiction (Q).
- Automated (X), with Manual (Q), implies computer-based communication between inter-operator management systems (X) whilst relying on a manual or human intervention to ensure communication with the related underlying network technology (Q).

The other cases involving possible automated or manual interface resources are summarized as follows:

- The case of Automated (Q) with Manual (X) is not considered.

Manual (X+Q) implies that communication between inter-operator management systems (X) is likely to be achieved using a conventional resource such as fax. Changes to network resources also require direct human intervention.

Table G.1: Summary of cases under consideration

	Case 1	Case 2	Case 3
Initiating/Origin	Automatic (X+Q)	Manual (X+Q)	Automatic (X), Manual (Q)
Transit 1	Manual (X+Q)	Automatic (X), Manual (Q)	Automatic (X+Q)
Transit 2	Automatic (X), Manual (Q)	Automatic (X+Q)	Manual (X+Q)
Destination	Automatic (X+Q)	Manual (X+Q)	Automatic (X), Manual (Q)

Case 1: **Case 1, Step 1:** This is illustrated by reference to figure G.2

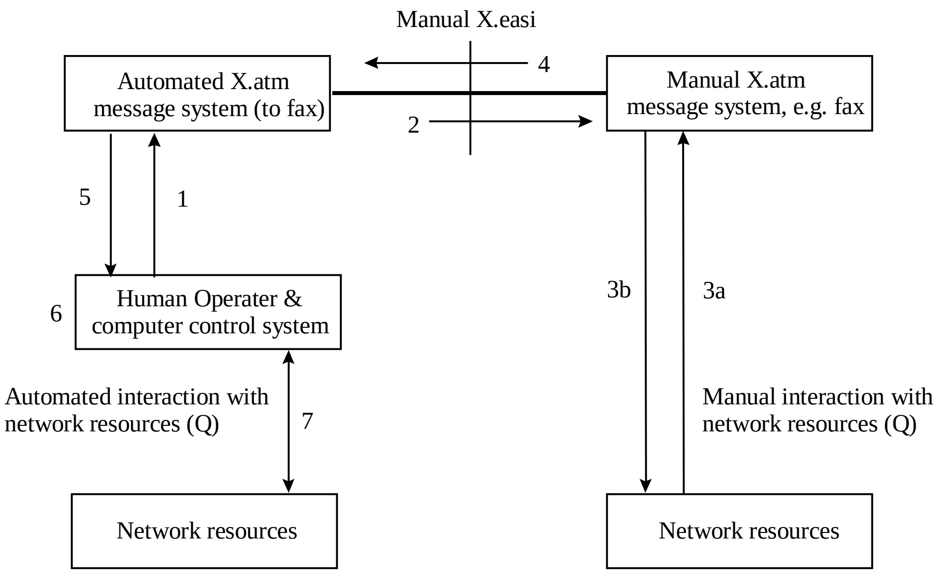


Figure G.2: Case 1, Step 1 scenario

The "sequence" numbers in Table G.2 refer to the processes in figure G.2.

Table G.2: operator resources and operation sequences for Case 1, Step 1

operator + Resource	Initiator and Originating: Automated (X+Q)	Transit 1: Manual
Sequence		
1	System produces a fax	
2	System issues a fax to Transit 1	
3a, 3b		Operator reads fax (3a) and makes any necessary changes to the Transit 1 network resources (3b)
4		Fax response sent to Initiator
5	Initiator reads fax	
6	Initiator inserts all Transit 1 information into the X.easi system using the computer platform	
7	Initiator issues any necessary operations on the network resources using an automated Q interface	

Case 1, Step 2: This is illustrated by reference to figure G.3

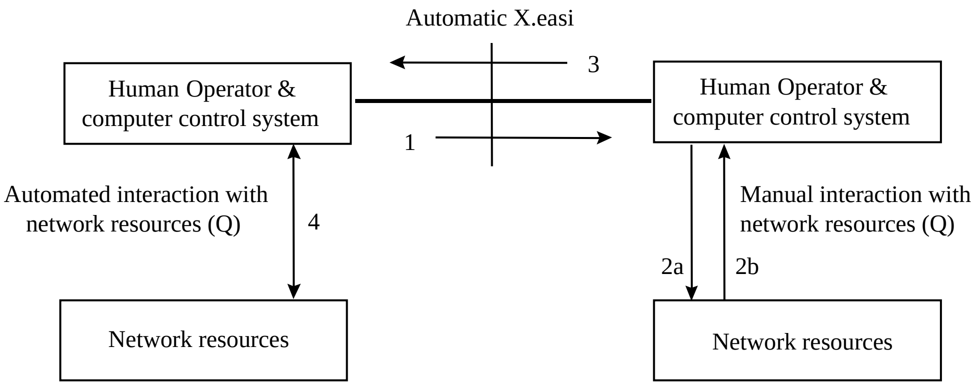


Figure G.3: Case 1, Step 2 scenario

The "sequence" numbers in Table G.3 refer to the processes in figure G.3.

Table G.3: operator resources and operation sequences for Case 1, Step 2

operator + Resource	Initiator and Originating: Automatic (X+Q)	Transit 2: Automatic (X) + Manual Q
Sequence		
1	Initiator interacts with Transit 2 using the automated X.easi interface and waits, as necessary	
2a, 2b		Operator reads message (2a) and makes any necessary changes to the Transit 2 network resources by manual means (2b)
3		Operator sends response back using the automated X.easi
4	Initiator issues any necessary operations on the network resources using an automated "Q" interface	

Case 1, Step 3: This is illustrated by reference to figure G.4

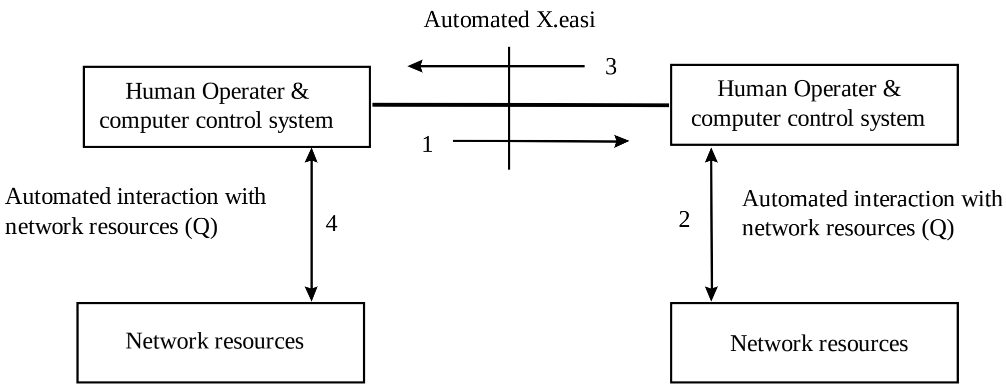


Figure G.4: Case 1, Step 3 scenario

The "sequence" numbers in Table G.4 refer to the processes in figure G.4.

Table G.4: Operator resources and operation sequences for Case 1, Step 3

operator + Resource	Initiator and Originating: Automatic (X+Q)	Destination: Automatic (X+Q)
Sequence		
1	Initiator interacts with Destination using an automated X.easi interface and waits, as necessary	
2		Operator reads message and makes any necessary changes to the Destination network resources by using an automated Q interface
3		Operator sends response back using the automated X.easi interface
4	Initiator issues any necessary operations on the network resources using an automated Q interface	

Cases 2 and 3 are described below but not illustrated by figures and sequence charts. The principles demonstrated above for Case 1 can be easily extended to the Case 2 and Case 3 scenarios.

Case 2: Case 2, Step 1

If the initiator is manual, it will issue a fax (1) with a request to Transit 1 (which is semi-automated). The operator will have to read the fax (2), manually insert the information into the X.easi semi-automated system (3), manually issue the possible operations on the real network (4), manually enter the results in the X.easi automated system (5), produce a fax (6) and send the answer by fax to the Initiating operator (7). It should be noted that steps 3 and 5, even if they appear not to be useful, are necessary in order to maintain the X.easi automated system up to date with the requests and modifications issued manually.

Case 2, Step 2

The manual Initiator will then issue the request to Transit 2 (automated) with a fax (1). The operator will have to read the fax (2), manually insert the information into the X.easi automated system (3), wait for the answer and then produce a fax (4) and send it to the Initiating operator (5).

Case 2, Step 3

The Initiator has now to send the last request to the Destination operator, which also has a manual interface. It will issue a fax (1) with the request to the Destination; the latter, after reading the fax, will manually issue (if any) the operations on the real network (2), produce a fax and send it back to the Initiating operator (3).

Case 3:

The initiator is now semi-automated, and things will work exactly the same way as Case 1 in this example because no interaction with the real network is implied for the Initiator. If Fault Management is considered, for example, then it will make a difference whether or not the Initiator has a fully automated X.easi system.

Conclusions

This annex has been produced in order to have a common framework in which all the issues relating to interfaces with different levels of automation may be discussed, together with a common terminology.

While this annex covers only the successful connection set-up procedure, a number of other cases need to be investigated, such as "Time outs" in the following situations:

a) Case 1: how much the Initiator will be able/willing to wait for Transit 1 to answer its request (and for Transit 2).

b) Case 1: if T1 and T2 are considered in the opposite order, there is also the issue of how long T2 would be prepared to keep its resources reserved while the Initiator sends the request and waits for the answer from T1 which is manual (this becomes crucial in a situation like "I=Manual, T1=Auto, T2=Manual, D=Manual, where T1 might need to wait a considerable amount of time).

c) Fault in the network of a semi-automated operator: how long will it take to report it to the Initiator if the latter is Manual (1) or Automatic/Semi-Automatic (2).

Annex H (informative): Overview of the issues associated with performance management for manual and automated X.easi interfaces

H.1 Introduction

This annex presents some further details associated with Performance Management (PM) using manual and automated X.easi management interfaces. It is improbable that automation for PM can be specified for Phase 1 ATM service introduction. However, the concepts and requirements are of importance as PM is related to "Quality of Service" – a subject perceived to be of increasing relevance in the area of ATM services provision and one which is likely to influence revenues generated from services provided. Quality of Service (QoS) may be defined as "the collective effect of service performances which determine the degree of satisfaction of a user to a specific service"

Issues raised in this annex should be considered for migration into the Phase 2 interface descriptions, if not for Phase 1.

Throughout this annex, the term "PNO" is used to denote an ATM network operator or carrier. This term is appropriate as it is used in the P708 Deliverables and appears in various managed object model definitions associated with the X-interface specifications.

H.2 Manual X.easi interface for Performance Management

Use of a "manual" interface may be taken to imply the exchange of appropriate PM information between PNOs by conventional (e.g. e-mail, fax) mechanisms, to an agreed scope and timetable. In order to be in a position to exchange such information, it may be necessary to deploy specialist performance measuring equipment, in addition to utilizing any performance data or statistics which may be available from network (gateway) switches.

The current state of available technology makes it very difficult to be prescriptive about either the PM measurements to be made or the external measuring technology to be deployed. A period of study, experimentation and cooperative development with switch vendors would seem to be imperative in the period leading to Phase 1 implementation of ATM based services. That said, recommendations for the specifications of equipment suitable for measuring the "Cell transfer performance of ATM connections" are provided in ITU-T Recommendation O.191 [66], for example. [66] is, however, restricted to measurements with the connection in an out-of-service mode whereas measurements suitable for an in-service mode would require alternative methodologies.

Given the availability of performance measurements and data, operators offering ATM interconnect services should use best endeavours to be able to provide a declaration of typical performance available from any ATM network which they may deploy.

At the individual network element level, the current state of the art concerning the availability of performance-related statistics from network switches is, at best, moderate and inconsistent. Where a TMN Q3 or Q3-like interface is deployed between an operations system (OS) and a switch (NE), it is unlikely that a full implementation of the associated ITU Standard [68] is available. The primary purpose of [68] is to provide a set of application messages and associated support objects for the parameter collection and thresholding aspects of Performance Management as related to a single monitored entity - typically a switch or individual part of the switch functionality.

With the above limitations in mind, it is likely that Performance Management in Phase 1 can only be specified on the basis of bi-laterally agreed "best efforts". Such bi-lateral agreements could, for example, specify measurement and exchange of PM data at agreed intervals on specific network elements (e.g. gateway switches) in order to build up a statistical view of the network behaviour over a period of time. Probably the most important PM function concerns "thresholding", whereby changeover to alternative resources is invoked when required to overcome degradation or failure in any specific VP or VC and thereby to maintain an adequate overall network performance or "Quality of Service".

In terms of TMN, [65] provides a succinct overview of Performance Management as follows:

The PM role is to gather statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the network, NE or equipment and to aid in planning and analysis.

Quality of Service includes monitoring and recording of parameters relating to:

- connection establishment (e.g. call set up delays, successful and failed call requests);
- connection retention;
- connection quality;
- keeping and examining of logs of system state histories;
- cooperation with fault, VP/VC alarm or maintenance management to establish possible failure of a resource and together with configuration management, to change routing and load control parameters/limits for links etc.;
- initiation of test calls to monitor QoS parameters.

Summarizing the [65] recommendation, - PM provides functions to evaluate and report upon the behaviour of telecommunication equipment and the effectiveness of the network or network elements.

The JAMES project described several tests in support of ATM network traffic characterization and performance measurements which may be related to the above [65] objectives. The test equipment is believed to have included HP 75000, Clemessy MAT34, Adtech AX/4000 etc. testers. One example involved the use of CBR test cells generated by appropriate test equipment in order to detect any ATM cell loss, error or misinsertion event. Tests then recorded events with the raw data which was then processed to obtain results for the following parameters (which are also applicable to the case of an automated interface described in subclause H.3):

- Availability Ratio (AR)
- Mean Time Between Outages (MTBO)
- Severely Errored Seconds (SES)
- Severely Errored Cell Block Ratio (SECBR)
- Cell Loss Ratio (CLR)
- Cell Error Ratio (CER)
- Cell Misinsertion Ratio (CMR)

Tests were conducted with variable parameters such as differing connection lengths, transmission technology and numbers of switches.

The actual results of the JAMES experiments are outside the scope of this annex but the test procedures, range of generated data and the standards-based basis for the tests should be considered by PNOs during any ATM service introduction phase. Indeed, for Phase 1 ATM service introduction, use of JAMES-based manual processes for inter-PNO PM should be considered for the basis of providing a minimum level of management information between PNOs.

For Phase 1, PM based on the discussion above will probably also have to have a significant degree of optionality devised around bi-lateral agreements. More sophisticated PM requirements will need to be specified in Phase 2 and it will be essential to get the support of the vendor community to implement the necessary degree of PM related data functionality onto switches in a comprehensive but cost-effective manner.

There would seem to be the need for a European Standard for in-service performance measurements, which draws from and develops the parameters associated with many of the various processes profiled from [56], [57] and [58].

H.3 Automated X.easi interface for Performance Management

P708 limited its scope to "Performance Monitoring" rather than the wider topic of "Performance Management" and restricted it to the requirements for the VP level. Accordingly, the requirements developed were tailored to the objective of providing a solution for VP Performance Monitoring and automated inter-PNO reporting, assuming the ETSI "Star" organizational model [6] and using the TMN X-interface. The solution assumes that the performance is monitored at network segment (or resource "ownership") boundaries between PNOs.

The requirements identified by P708 include:

- At the start of any monitoring period the activated semi-permanent VP connection is in an "available state". (Refer to [57] for the definition of Availability.)
- The "Severely Errored Second" in the ATM layer (SES_{ATM}) is used as a criterion for entry into the unavailable state [57].
- Therefore there is a requirement that the number of detected SES_{ATM} should be recorded appropriately.
- The requirement is that when an "unavailable state" is detected the monitoring process is stopped, the actual values of the traffic and performance parameters (CLR, CER, CMR, SECBR etc.) are stored, and a fault report is send to the initiating PNO across the X.easi interface with all relevant information.
- The consequent requirement is that inter-working between Fault and Performance management needs to be specified and defined. Further, these management functions can be expected to require interaction with Configuration and Accounting functions.

In turn, the definition of requirements for performance monitoring is based on five main categories of ITU-T defined ATM Transfer Capabilities (ATCs). Refer to [12] as follows:

- Deterministic Bit Rate Transfer capability (DBR - ATC)
- Statistical Bit Rate Transfer capability (SBR - ATC)
- Available bit rate transfer capability (ABR - ATC)
- ATM Block Transfer capability with Immediate Transmission (ABT/IT - ATC)
- ATM Block Transfer capability with Delayed Transmission (ABT/DT - ATC)

(Note the ITU-T ATM ATC's in the five bullets above have equivalent ATM Forum based categories, as described in table 3 of the present document.)

The general requirement is that in the event of one of the parameters exceeding a specified maximum threshold value, a Performance Report should be emitted towards the I-PNO which is also notified again, when the value of the parameter returns to an acceptable level.

Performance objectives, which may be used to define thresholds for the ATCs listed above, are provided in [56].

This following subclause presents and proposes the mechanisms and the information model produced by EURESCOM project P708 to exchange information about the performance and QoS of an ATM VP service in an inter-PNO environment. An automated X-interface implementation is assumed.

Performance Management Mechanisms and Information Model

The P708 X-interface Performance Management specification contains the functionalities to set up and stop the Performance Monitoring process, to notify Quality of Service (QoS) degradation and unavailability periods to the I-PNO (as defined in the "star model" [6]) and retrieve Performance information about the connection. The QoS of a connection should be requested and agreed during the VP configuration processes (although [6] may need an enhancement for this purpose).

The situation is that an I-PNO which has requested a connection running through the networks of several other PNOs can only directly monitor the performance for the portion of the connection within its own domain. Therefore, management processes are required to get information when performance degradation occurs or there are unavailability periods affecting parts of the connection across the networks of other PNOs. The advantage for the I-PNO is that it should receive information automatically about any performance degradation. This enables prompt reaction to such degradation, minimizing the impact on the service to customers and the other associated PNOs.

The performance monitoring specification relies on implementation of an OAM cell flow, as defined in [58] within network "segments". Such a segment is defined as the portion of a connection contained within a PNO's domain or between domains. The source and sink for the segment OAM flows are therefore within single PNO domains (subnetwork case) or at the gateways between two PNOs (inter-PNO physical link case).

An overview of the complete PM scenario, as developed by P708 (with minor modifications for this annex), is depicted in figure H.1.

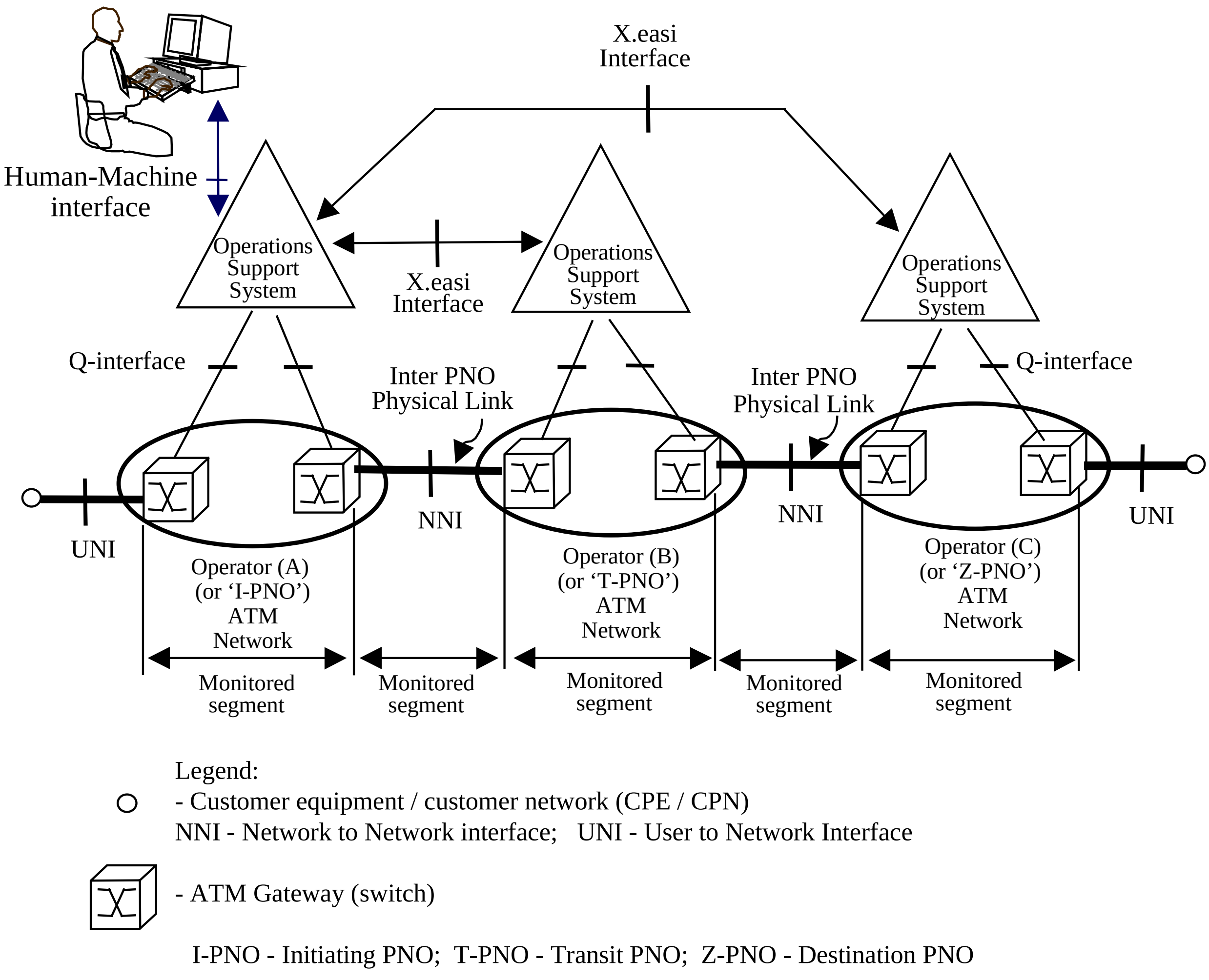


Figure H.1: Performance Management Scenario

Figure H.1 is equivalent to figure 4 in the main part of the present document, except that the I-PNO and A-PNO are the same organization in figure H.1.

Performance Monitoring may be achieved in two steps. The first step requires the I-PNO to request a certain QoS associated with the VP reservation request. This is indicated by choosing a set of specified performance parameter values derived from [56] and described previously in this annex.

The second step is the actual I-PNO request for activation of the performance monitoring, and can be done either together with the reservation request or later, when the VP connection is activated. The I-PNO can also at any time stop the performance monitoring on its reserved connections. To enable these and other related requests, standard messages have been defined in order for them to be exchanged between the PNO's management systems across the X.easi interface.

Note that no Performance Management is described or specified in this annex with respect to the UNI shown in figure H.1. (Inclusion of the UNI in figure H.1 is for illustrative purposes only.)

P708 developed the information models for PM PVPs whilst assuring alignment with the existing equivalent models for Configuration and Alarm Management of PVPs and PVCs [6], [10].

To meet the specific needs for Performance Management three new object classes were defined:

- pnoPerformanceData;
- pnoLCBidirectionalPerformanceMonitor;
- pnoSNCBidirectionalPerformanceMonitor.

Use of these object classes, with respect to a "containment tree" for one ATM subnetwork, is shown in figure H.2.

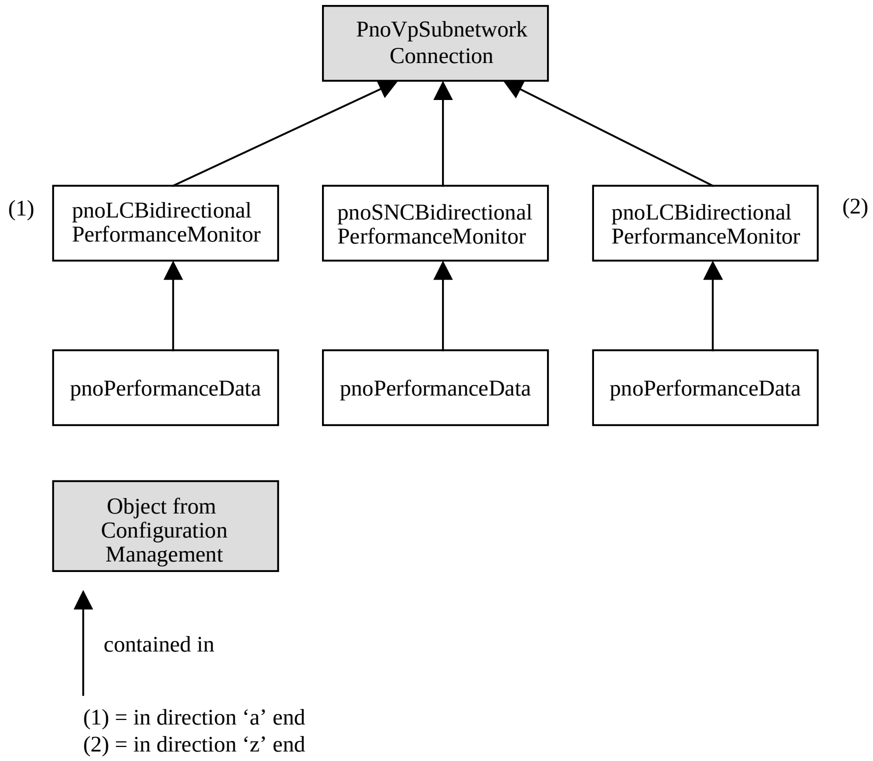


Figure H.2: Containment Tree for one Subnetwork

Details taken from the P708 PM object model are important and included in this annex because it relates to the three main parts of the performance monitoring mechanism, which are:

- requesting the possibility to monitor a VP connection (which should be done only once);
- starting and stopping the monitoring on that connection (which may be done several times during the connection lifetime if it is possible to monitor the connection);
- defining thresholds on one or more performance parameters to be notified when the actual performance of the connection falls below the threshold level (this works only while the monitoring is active).

This can be accomplished by using the three new managed object classes defined by P708, which are described in brief as follows:

- **pnoLCBidirectionalPerformanceMonitor**: it is created when a connection *can be* monitored and supports the monitoring of the **performance of a link connection** (i.e. the part of the connection running over an IPPL) in one or both directions. It can contain one sink and one source, whose corresponding source and sink (respectively) are contained in the domain of the adjacent PNO.

- **pnoSNCBidirectionalPerformanceMonitor**: it is created when a connection *can be* monitored and supports the mechanism for activating/deactivating performance monitoring in one or both directions. It can contain two sinks and two sources for measuring the **performance of a subnetwork connection**; one sink/source couple will be created for each direction of the connection to support the monitoring of a bi-directional connection.

- **pnoPerformanceData**: instances of this object class are created/deleted whenever a request to start or stop the performance monitoring is received from the Initiator. One instance is created for each pnoSNCBidirectionalPerformanceMonitor and pnoLCBidirectionalPerformanceMonitor object instance already associated to the monitored connection. They keep the current performance parameter values (e.g. CTD, CLR, CER, CDV, CMR and SECBR) for the portion of the ATM connection monitored. Additionally these instances keep the threshold values of the performance parameters of the connection, as requested by the I-PNO.

Objects of the first two classes are created in the MIB of the PNOs providing the connection as a side effect of accepting the Reserve Request if performance monitoring has been requested in the set-up message. The objects are deleted when the connection reservation expires or the connection is explicitly deleted.

Objects of the last class are created and instantiated below the previous ones when a "Start Performance Monitoring" message from the I-PNO is received and answered positively and deleted either when the connection is released by the I-PNO, or when a "Stop Performance Monitoring" message is received.

The creation of the monitor objects is the key point for the monitoring process.

At any time when performance monitoring is active on a connection the performance values measured on the network are compared with the thresholds to trigger the emission of a "threshold crossing" notification towards the I-PNO. Outstanding QoS notifications are cleared when the measured performance of the connection attains the allowed value range again.

During the lifetime of the connection for specific monitoring purposes the I-PNO might be able to request the setting of additional threshold values.

Finally, inputs from the P708 work have been contributed to ETSI as the proposed basis for a new standard [32] in the area of Performance Management for the ATM X-interface.

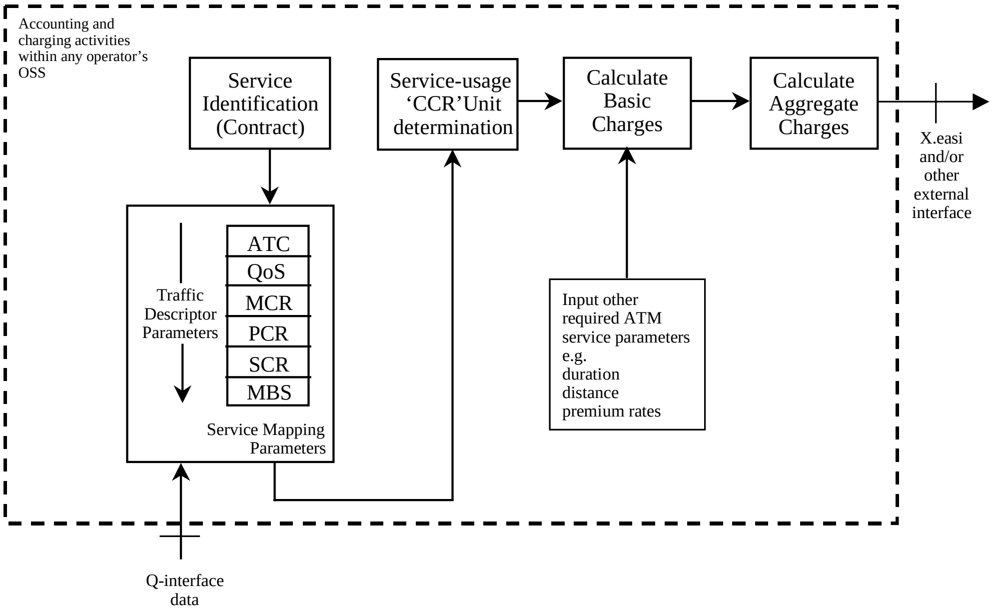
Recommendation to ETSI and concluding comments

The current situation for X-interface performance management of ATM connections provided by multiple operators is in need of further development. A draft standard EN 300 820-3 [32] is currently under consideration within ETSI to provide a functional specification in alignment with [6] and [10]. This standard should provide guidance for specifying the minimum level of acceptable PM functionality, for manual and automated X.easi interfaces in support of interconnected European ATM networks and services. The automated interface concepts should generally be developed and considered for Phase 2 implementation.

Annex I (informative): The ITU-T "D.224" Chargeable Cell Rate for use with the X.easi interface

I.1 Introduction

The purpose of this annex is to provide guidance on the processes which might be applicable to establish methods for calculation for charges for customers or other PNOs or SPs for their ATM service-usage. Figure I.1 illustrates some accounting and charging activities which might need to be supported in the OSS of any operator. The depiction of the OSS and the Q and X.easi interfaces is in alignment with figure 4 in the main part of the present document. The issue to be resolved is whether accounting data or charging data (or both types of data) is exchanged over the X.easi interface.



Legend:

ATC - ATM Transfer Capability	QoS - Quality of Service Class
MCR - Minimum Cell Rate	PCR - Peak Cell Rate
SCR - Sustainable Cell Rate	MBS - Maximum Burst Size
CCR - Chargeable Cell Rate	Q-interface - Operator's management interface to its network technology
OSS - Operations Support System	

Figure I.1: Service Mapping and Rating scheme

Figure I.1 combines ideas generated by CANCAN and ITU-T Recommendation D.224 [35] where, in particular, the use of the Chargeable Cell Rate (CCR) is described. The CCR and charging issues are described subsequently in this annex. In figure I.1, the Service Identification (contract) has to be associated with the VP for which accounting and charging processes are required. Traffic descriptor and service mapping parameters and other service parameters are combined and input to a charging formula to calculate basic charges. Further parameters (e.g. a performance factor) may be input to calculate aggregate charges before final information is processed into a data file for exchange over the X.easi interface. Central to the aggregate charge calculation is the CCR calculation, which is described in clause I.2.

I.2 Use of a Chargeable Cell Rate (CCR)

I.2.1 Rationale for use of a CCR

The reason for definition of the CCR is **simplicity.** For ATM VP/VC accounting, aggregation over several parameters for each possible type of connection is complex and the concept of the CCR has been postulated [35] in order to reflect, **as a single cell charging rate,** the chargeable impact of the connection on network resources. The CCR is a concept intended to be used only in the context of charging and accounting. The calculation of CCR for each type of connection is operator specific, and therefore conducive to the requirements of an open competitive market. Because the calculation of CCR is likely to reflect reservation of network resources, its probable derivation will be based on connection parameters such as ATC, QoS, MBS and the cell rates shown in figure I.1, together with a number of other service definition parameters or tolerances.

I.2.2 CCR Unit determination (with an example)

Calculation of an aggregate charge for any given VP/VC service, using the CCR approach, depends on a calculation of the appropriate CCR for the connection and the number of CCR units of usage that have been consumed. Once the number of CCR units has been calculated it needs to be combined with the other service parameters in the charging formula to arrive at the correct charging for the ATM service. The draft ITU-T Recommendation [35] offers examples of CCR calculation. One example from an original draft of [35] is replicated as follows:

An SBR3 connection with QoS class 3 and PCR = 5 000 cells/s, SCR = 2 000 cells/s and MBS = 200 cells could be simplified for accounting, in an operator-specific calculation on CCR, to:

SBR3, QoS class3, CCR = 3 000 cells/s.

(This calculation for CCR could also be modified by factors such as the number of tagged cells (CLP = 0, CLP = 1) delivered.)

The simplest aggregation for cells transferred at an interconnection interface (typically, an ATM Gateway switch, with reference to figure 4 in the main part of the present document) is to aggregate for all connections in a given direction, their CCR and their lifetime. Then for CCR = 3 000 cells/s active for one hour (3 600 seconds) during a given aggregation period, the net contribution for calculation of charges is 3 000 x 3 600 = Volume = 10 800 000 cells. The use of the "Volume" of cells transferred would then be used in the calculation of basic charges.

It may be presumed that where an ATM service is provided using CBR (or DBR) ATC, the CCR would be equal to the CBR, less any adjustments for service performance (i.e. cells not delivered) factors.

Clearly, where aggregations are differentiated by ATC/QoS/charging period combinations, there will be a separate accounting parameter for each combination which will yield a value for the CCR and number of chargeable cells transferred across the network boundary. Accordingly, the CCR values should be contained in a reasonably short look-up table for onward transfer into the calculations of basic charges. (In the most simple of cases, an operator could choose to use a single CCR value for all reservation and usage cell prices for all ATC/QoS combinations and for all charging periods.)

I.3 Concluding comments

The purpose of annex I is to provide an indication of a pragmatic means of calculating an effective charge for the various ATM-based VP/VC services which may be provided using an interconnected operator environment. The basis of such charge calculations is the ITU-T inspired CCR [35]. Considerable elaboration of the concepts described in this annex is to be found in the EURESCOM P708 Deliverables associated with Accounting Management [34].

The originating operator, which organizes provision of a VP/VC service for a paying customer, will need to assess what fraction of the charge for the service is due to other interconnected operators which also contribute to the resources required to deliver the service to the end-user. These aspects of the accounting, charging and revenue settlements remain to be defined for the X.easi interface and certainly need to be established in a standards format.

The ETSI standards developments process should consider use of [35] and related parameters in the definition of a standard for the exchange of accounting and related charging data for ATM services.

Annex J (informative): A brief synopsis of ITU-T "D-series" Standards for interconnect service operation accounting processes

Annex J aims to provide a superficial review (or précis) of a number of the ITU-T D-series Recommendations, "General tariff principles". This review is provided in order to illustrate the principles on which international tariffs, accounting and settlements are made for current services such as ISDN, Frame Relay, Telex and for Signalling System No 7 usage. It is reasonable to assume that similar standards could be developed for accounting for ATM based services provided by cooperating operators. Terms such as "international" should generally be applicable to any "inter-operator" situation in the developing European ATM market.

The following points were identified from the standards documents referenced below:

- ITU-T Recommendation D.170 [45]

This identifies "traffic sampling" as a basis for international accounts as an option to avoid the necessity for continuous traffic measurements. The timing, duration and frequency of such sampling requires bi-lateral agreements. This method may be used for monthly telephone settlements.

- ITU-T Recommendation D.285 [46]

This provides "guiding principles for charging and accounting for IN supported services". This states that "charges may be applicable for the use of resources associated with network intelligence, such as databases and signalling networks, or service profile management".

- ITU-T Recommendation D.232 [47]

This considers ISDN supplementary services. The tariff and accounting principles identified valid areas for charging based on provision of supplementary services such as call waiting, call transfers, conference calling, call transfer, call forwarding, private numbering plans with public number plan translations.

- ITU-T Recommendation D.230 [48]

The principle is stated that the above ITU-T Recommendation D.232 services may be charged for with revenue shared by initiating, transit and destination administrations.

- ITU-T Recommendation D.225 [49]

For Frame Relay data services there are various charging options which include flat rate and reservation and usage. The Reservation and Usage option has two clear chargeable components, (i) reservation, (ii) traffic usage. This may be based also on portions of PVCs provided by co-operating Administrations in the service provision. However, traffic usage rates may be charged differently in the network of each Administration in order to establish competitive market principles.

- ITU-T Recommendation D.212 [50]

This considers usage of Signalling System No. 7 charging and accounting principles. There are circuit-based and non-circuit based principles. The circuit-related principles depend on Administration costs. Non-circuit related charging principles are usually based on options (a) by volume of data exchanged (octets) (b) by a per message fee (c) by a flat rate rental or subscription according to commercial arrangements.

- ITU-T Recommendation D.211 [51]

This considers usage of the Signal Transfer Point (STP) in SS No. 7. This is important in encouraging bi-lateral network resilience. Volume traffic settlements may be made with differing charge rates depending on demand. Settlement payments may or may not be necessary depending on whether mutual usage of other co-operating Administrations' signalling resources is in broad balance. There is a principle that different charging rates may be made according to whether STP resources are used in high or low traffic demand periods.

- ITU-T Recommendation D.210 [52]

This clarifies that charging and accounting principles may have "access" and "utilization" components. The access component is likely to be based on the cost of customer connections. The utilization component is likely to be based on use of network resources and whether additional functionality is required by the customer.

Annex K (informative): Fax forms used in the JAMES project for ATM connections

K.1 Introduction

Interconnect service operation processes, which are undertaken using manual X.easi interfaces, generally require the exchange of information between operators by means of faxes. Such faxes will generally take the form of standard templates with fields filled by the operator requiring the exchange of management information. A number of examples of the fax templates developed within the European ATM Pilot and subsequent JAMES project for ATM connection procedures are attached below.

K.2 Destination Availability Checking (EAP Form1)

Originator Ref. NUMBER: ______________________________

EAP FORM 1 **TITLE**

DESTINATION AVAILABILITY CHECKING

ORIGINATOR of the VPC

Name: ____________ **Fax:** ____________ **OC:** ____________

DESTINATION of the VPC

Name: ____________ **Fax:** ____________ **OC:** ____________

VP Connection Id: ______________________________

N_VPC_CHECKING INFORMATION

Page 1 of: ____________

Time of Sending (UTC): ________________________ **(YY/MM/DD/HH/mn)**

Ans. Requested By (UTC): ________________________ **(YY/MM/DD/HH/mn)**

ORIGIN User

NAME: ________________________

E164 ID: ________________________

DESTINATION User

NAME: ________________________

E164 ID: ________________________

Connection Type

Unidir Bidir. Sym Bidir. NoSym **(Circle)**

Subscription Mode

PERM. OCCAS. DAILY WEEKLY **(Circle)**

Service: ________________________

Application: ________________________

N_VPC_CHECKING_CONFIRM INFORMATION

Page 1 of: 1

Time Sending Back (UTC) : ________________________ **(YY/MM/DD/HH/mn)**

ANSWER OK NOT OK **(Circle)**

Available Preceding SubNetworks (OK) Subnetwork ID	CAUSE (NOT OK)

K.3 Connection Reservation (EAP Form2)

Originator Ref. NUMBER:				
EAP FORM 2		TITLE		
	CONNECTION RESERVATION			
ORIGINATOR of the VPC				
Name:		Fax:		OC:
RECIPIENTS				
TRANSIT1				
Name:		Fax:		OC:
TRANSIT2				
Name:		Fax:		OC:
TRANSIT3				
Name:		Fax:		OC:
TRANSIT4				
Name:		Fax:		OC:
DESTINATION				
Name:		Fax:		OC:
VP Connection Id:				

N_VPC_REQUEST INFORMATION					
		Page of:			
ORIGIN User					
	NAME:				
	E164 ID:				
DESTINATION User					
	NAME:				
	E164 ID:				
Connection Type					
	Unidir	Bidir. Sym	Bidir. NoSym		(Circle)
Subscription Mode					
	PERM.	OCCAS.	DAILY	WEEKLY	(Circle)
Service:					
Application:					

CONTINUES ON NEXT PAGES

N_VPC_REQUEST_CONFIRM INFORMATION					
		Page of:			
(UTC)	(YY/MM/DD/HH/mn)				
	Time Sending from origin		Answer Requested by		Time Returning Back
TRANSIT1					
TRANSIT2					
TRANSIT3					
TRANSIT4					
DESTINATION					

ROUTING TABLE

	SNetwork Id	LL Id (Outgoing)	VPI	OK or NOT OK
ORIGIN				
TRANSIT1				
TRANSIT2				
TRANSIT3				
TRANSIT4				
DESTINATION				

CAUSE (IF NOT OK):

FINAL N_VPC_RESERVATION INFORMATION			
	Page of:		
Time & Date of broadcast (UTC) :			(YY/MM/DD/HH/mn)
Reservation Result	OK	NOT OK	(Circle)
CAUSE IS EXPLAINED ABOVE IF NOT OK			

K.4 Connection Release (EAP Form3)

Originator Ref. NUMBER:			

EAP FORM 3		TITLE			
	CONNECTION RELEASE				
ORIGINATOR of the VPC					
Name:		Fax:		OC:	
RECIPIENTS					
TRANSIT1					
Name:		Fax:		OC:	
TRANSIT2					
Name:		Fax:		OC:	
TRANSIT3					
Name:		Fax:		OC:	
TRANSIT4					
Name:		Fax:		OC:	
DESTINATION					
Name:		Fax:		OC:	
VP Connection Id:					

N_VPC_RELEASE INFORMATION					
		Page of:			
Time of Sending (UTC):					(YY/MM/DD/HH/mn)
Procedure Initiatiated by:		ORIGIN	DESTINATION		(Circle)
Time & of Sending (UTC):					(YY/MM/DD/HH/mn)
PLEASE RELEASE THE NETWORK RESOURCES ALLOCATED TO THE					
VPC WITH THE ABOVE VP CONNECTION ID					
CAUSE					

N_VPC_RELEASE_CONFIRM INFORMATION					
ON RECEPTION OF THIS FORM, CANCEL THE VPC,					
SEND BACK TO ORIGINATOR WITH THE TIME AND DATE					
(UTC)		Answer		Time	
(YY/MM/DD/HH/mn)		Requested by		Returning	
TRANSIT1					
TRANSIT2					
TRANSIT3					
TRANSIT4					
DESTINATION					

K.5 Modify Bandwidth Procedure (EAP Form4)

Originator Ref. NUMBER:		

EAP FORM 4		TITLE			
	MODIFY BANDWIDTH PROCEDURE				
ORIGINATOR of the VPC					
Name:		Fax:		OC:	
RECIPIENTS					
TRANSIT1					
Name:		Fax:		OC:	
TRANSIT2					
Name:		Fax:		OC:	
TRANSIT3					
Name:		Fax:		OC:	
TRANSIT4					
Name:		Fax:		OC:	
DESTINATION					
Name:		Fax:		OC:	
VP Connection Id:					

N_VPC_MODIFY_REQUEST INFORMATION		
NEW REQUESTED SCHEDULE (Occasional or Permanent)		
OCCASIONAL SCHEDULE REQUESTED		
START:		(UTC) (YY/MM/DD/HH/mn)
END:		(UTC) (YY/MM/DD/HH/mn)
FORWARD:		(Cell per second)
BACKWARD:		(Cell per second)
PERMANENT SCHEDULE REQUESTED		
START:	(YY/MM/DD/HH/mn)	
FORWARD:	Cell per second	
BACKWARD:	Cell per second	

N_VPC_MODIFY_CONFIRM INFORMATION					
(UTC)(YY/MM/DD/HH/mn)		Time Sending from origin	Answer Requested by	Time Returning	OK or NOT OK
	TRANSIT1				
	TRANSIT2				
	TRANSIT3				
	TRANSIT4				
	DESTIN.				

FINAL N_VPC_RESERVATION INFORMATION			
Time of broadcast (UTC) :			(YY/MM/DD/HH/mn)
Modification Result	OK	NOT OK	(Circle)
IF NOT OK CANCEL, IF OK ACTIVATE AT (UTC) :			
IF OK ACTIVATE AT (UTC) :			(YY/MM/DD/HH/mn)

K.6 Fault Procedure (EAP Form5)

Originator Ref. NUMBER:

EAP FORM 5 **TITLE**

FAULT PROCEDURE

ORIGINATOR of the Fault Message

Name:	**Fax:**	**OC:**

RECIPIENTS

Name:	**Fax:**	**OC:**
Name:	**Fax:**	**OC:**
Name:	**Fax:**	**OC:**
Name:	**Fax:**	**OC:**
Name:	**Fax:**	**OC:**
Name:	**Fax:**	**OC:**

VP Connection Id:

LEGEND:

N_VPC_FAULT:
A fault has occured in the network element designated below

N_VPC_FAULT_RECOVERY:
The network element above has recovered from its fault cond.

N_VPC_FAULT_NON RECOVERY:
The network element below has not recovered.
The reconfiguration (or release) procedure may be activated

FAULT_PROCEDURE INFORMATION

TYPE OF MESSAGE (Circle):
N_VPC_FAULT
N_VPC_FAULT_RECOVERY
N_VPC_FAULT_NON RECOVERY

ELEMENT DESIGNATION (FILL ONLY THE CORRECT FIELD) :
NETWORK ELEMENT DESIGNATION :
PHYSICAL LINK DESIGNATION : **(M140)**

EXPECTED DURATION OF THE FAULT:

CAUSE OF THE FAILURE:

K.7 Permanent Schedule (EAP Form6)

EAP FORM 6		TITLE	
	PERMANENT VP SCHEDULE		
VP Connection Id:			
SCHEDULE REQUESTED			
START:			UTC (YY/MM/DD/HH/mn)
FORWARD:			Cell per second
BACKWARD:			Cell per second

K.8 Occasional Schedule (EAP Form7)

EAP FORM 7		TITLE	
	OCCASIONAL VP SCHEDULE		
VP Connection Id:			
SCHEDULE REQUESTED			
START:			UTC (YY/MM/DD/HH/mn)
END:			UTC (YY/MM/DD/HH/mn)
FORWARD:			Cell per second
BACKWARD:			Cell per second

K.9 Daily Schedule (EAP Form8)

EAP FORM 8	TITLE	
	DAILY VP SCHEDULE	
VP Connection Id:		
SCHEDULE REQUESTED		
SCHEDULE BOUNDARIES		
START:		(UTC) (YY/MM/DD/HH/mn)
END:		(UTC) (YY/MM/DD/HH/mn)
FIRST ACTIVATION		
START:		(UTC)(HH/mn)
END:		(UTC)(HH/mn)
FORWARD:		(Cell per second)
BACKWARD:		(Cell per second)
SECOND ACTIVATION		
START:		(UTC)(HH/mn)
END:		(UTC)(HH/mn)
FORWARD:		(Cell per second)
BACKWARD:		(Cell per second)
THIRD ACTIVATION		
START:		(UTC)(HH/mn)
END:		(UTC)(HH/mn)
FORWARD:		(Cell per second)
BACKWARD:		(Cell per second)
FOURTH ACTIVATION		
START:		(UTC)(HH/mn)
END:		(UTC)(HH/mn)
FORWARD:		(Cell per second)
BACKWARD:		(Cell per second)

K.10 Weekly Schedule (EAP Form9)

EAP FORM 9	TITLE		
	WEEKLY VP SCHEDULE		
VP Connection Id:			
SCHEDULE REQUESTED			
FILL AS MANY AS NECESSARY			
THIS SCHEDULE IS MADE OF :		PAGES	
THIS SCHEDULE IS MADE OF :		ACTIVATIONS (28 MAX)	
SCHEDULE BOUDARIES	(FOR FIRST PAGE ONLY)		
START:		(UTC) (YY/ MM/ DD/ HH/ mn)	
END:		(UTC) (YY/ MM/ DD/ HH/ mn)	
INDICATE DAY (day) by using : MON,TUE,WED,THU,FRI,SAT,SUN			
ACTIVATION NUMBER :	1		
START:		(UTC) (day/HH/mn)	
END:		(UTC) (day/HH/mn)	
FORWARD:		(Cell per second)	
BACKWARD:		(Cell per second)	
ACTIVATION NUMBER :	2		
START:		(UTC) (day/HH/mn)	
END:		(UTC) (day/HH/mn)	
FORWARD:		(Cell per second)	
BACKWARD:		(Cell per second)	
ACTIVATION NUMBER :	3		
START:		(UTC) (day/HH/mn)	
END:		(UTC) (day/HH/mn)	
FORWARD:		(Cell per second)	
BACKWARD:		(Cell per second)	
ACTIVATION NUMBER :			
START:		(UTC) (day/HH/mn)	
END:		(UTC) (day/HH/mn)	
FORWARD:		(Cell per second)	
BACKWARD:		(Cell per second)	
ACTIVATION NUMBER :			
START:		(UTC) (day/HH/mn)	
END:		(UTC) (day/HH/mn)	
FORWARD:		(Cell per second)	
BACKWARD:		(Cell per second)	

Annex L (informative): An estimation for values for star- and cascaded organization

In this annex a simple comparison for estimated values between the star- and cascaded organizational models is performed. For this estimation, the next two cases are presumed:

- **Case 1**

A total of 10 interconnected networks with an X.easi management interconnection, each having, on average, 8 bundles of links with the other networks, and 5 physical links per bundle. This means there are 400 physical links in the system. (It is presumed that there can be more than one bundle between two subnetworks.)

Each day, on average, one percent of those links generate messages.

On average, each operator makes 5 end-to-end X.easi reservations per day, each going across 3 networks.

- **Case 2**

A total of 80 interconnected networks with an X.easi management interconnection, each having, on average, 8 bundles of links with other networks, and 5 physical links per bundle. This means there are 3200 physical links in the system. (It is presumed that there can be more than one bundle between two subnetworks.)

Each day, on average, one percent of those links generate messages.

On average, each operator makes 40 end-to-end X.easi reservations per day, each going across 5 networks.

Furthermore, it is presumed that the initiator is always the A-operator.

These presumptions give the following results:

- **Star organization**

For case 1, each operator will have to maintain the data of 400 physical links (bandwidth, QoS, operational state, access-points).

For Case 2, each operator will have to maintain the data of 3 200 physical links.

However, databases can cope with this.

Each operator will receive 4 (case 1), respectively 32 (case 2) topology-messages per day over the X.easi interface.

The number of X.easi requests an operator will have to deal with:

Case 1: An operator will request 10 reservations per day, and he will receive 10 requests.

Case 2: An operator will request 160 reservations per day, and he will receive 160 requests.

(There is no difference with the cascaded organization.)

In case 2, each operator must be able to make management connections to 79 other operators. However, not necessarily at the same time.

- **Cascaded organization**

Each operator will receive 0,4 topology messages per day. Messages regarding the links only need to be sent to the "adjacent" operators and most probably will be sent on bilateral basis.

As for the number of X.easi requests for one operator, there is no difference with the star organization:

Case 1: An operator will request 10 reservations per day, and he will receive 10 reserve-requests.

Case 2: An operator will request 160 reservations per day, and he will receive 160 reserve-requests.

Each operator must be able to make management connections to 8 other operators. However, not necessarily at the same time.

Annex M (informative): Pre-selection of carriers and the X.easi policy rules

Carrier pre-selection

For pre-selection of carriers the possibilities shown in figure M.1 can be considered:

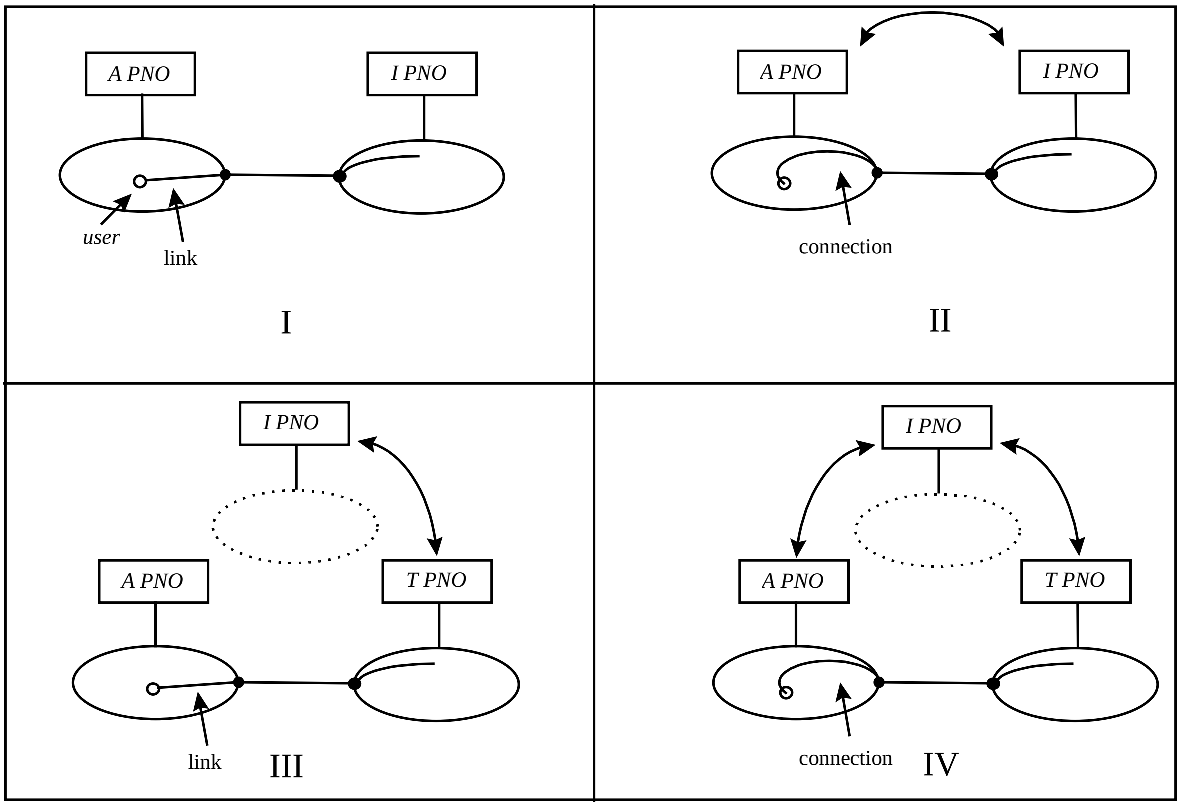


Figure M.1: Carrier pre-selection

Pre-selection of carrier applies to the case that a user is physically located within the local network (subscriber + secondary + primary circuit) of an operator, but he wants to use the facilities of another operator without explicitly having to request this with each connection set-up. It stems from telephony where customers are within the local network of a "traditional operator".

The question is whether this historic situation also applies for modern ATM networks.

There are four possible cases to examine:

Case I: The I-PNO administratively owns a user-link which is physically in the network of the A-PNO. The user has a connection to the I-network without the need for X.easi commands. Towards the user, the I-PNO is responsible for the overall reservation.

Case II: The I-PNO makes an X.easi reservation in the A network. Towards the user, the I-PNO is responsible for the overall reservation.

Case III: The same as Case 1, but the I-PNO's network is no part of the overall connection.

Case IV: The same as Case II, but the I-PNO's network is no part of the overall connection.

Within the framework of the policy rules it appears that only case II can be part of the X.easi interface. The other cases are the responsibility of the individual operators and subject to bilateral agreements.

Annex N (informative): Issues, Gaps, Dependencies and Assumptions identified for the Phase 1 X.easi interface

N.1 Configuration Management (CM)

N.1.1 Issues and gaps

- It should be noted that the approach adopted by JAMES and ETSI [6] only supports provisioning of virtual path connections (PVPs). Accordingly, it is likely that an extension of the available X-interface (X.easi) specifications to support PVCs will be necessary to align with the requirements for automated management of such services.
- Operators should be aware that there will be a minimum level of technical detail required to be exchanged to progress a provisioning order from respective customer sales to operations departments where the use of two or more operator's networks is concerned. The configuration management processes for the exchange of such details remain to be defined for ATM networks. ITU-T Recommendations [59], [60] and [61] provide possible requirements and procedures. Annex A (to the main part of the present document) explores some of the possibilities, processes and issues.
- It would appear that the European standard for Configuration Management [6], in respect of the ATM VP/VC cross connected network, is silent on the semantics of "Check available cell rate" which is part of a more general "Give available links" request. There seems to be an assumption that either or both of these queries is all that is required for managing (VP/VC link) capacity. (Or, - put in an alternative way - that there is always sufficient capacity available on all links to meet any reservation request at any time.) Furthermore, the standard does not consider the possible operational requirement to send different ATC and QoS with "Give Available Links". The current text seems to limit the use to a CBR-only service with a presumption that the link is supporting a VP or group of VCs all carrying the same ATM service class/ATC/QoS. Certainly, there is no explicit consideration of the case of a link simultaneously supporting a range of different ATM services and service classes. Specifically, the current definition of the "Traffic Descriptor" in the standard is not sufficiently sophisticated to cope with these types of complex operational requirements.
- In general, [6] seems to be deficient in that it provides no process or policy for managing infrastructure capacity or partial rejections of reservation requests and there may be other related shortcomings. By contrast, the TMF Peer to Peer Service Configuration models, consider the availability of the infrastructure capacity and assumes that the SP or its customer may **reserve** this infrastructure capacity, if it is available.

In summary, the questions that the perceived shortcomings in [6] raise should include:

i) Does "Give available links" mean the capacity that is physically available on a link or does it mean the capacity that the link-owning PNO is prepared to make available to the I-PNO wishing to create a reservation for VP/VC service? (Note that the answer is probably the latter case.)

ii) What policies may be applied to responses on "Logical available capacity", - that is capacity which may be carried on diverse routes or is available for purposes such as reconfiguration or protection?

iii) What is the policy for logical sub-division of a VP into VCs supported on a fixed physical link, such as 155 Mb/s. e.g. are the VCs available in units of 64 kb/s, 1, 2, 4, 10 etc. Mb/s etc.?

iv) What policies or responses should be given for a situation of "Rejected timeslots"?

That is, the reservation schedule (= bandwidth + time) can be partially fulfilled. Examples may include:

(a) Reservation request is for a 34 Mb/s link for 24 hours. 30 Mb/s is available for these 24 hours. Should the response be "Schedule not available" (as in the standard) or "Reduced schedule of 30 Mb/s is available" (this would need a standard enhancement). The reserving PNO could then decide if a reservation of 30 Mb/s is sufficient and start the reservation procedure again with the knowledge of this maximum bandwidth available.

(b) Reservation request is for a 34 Mb/s link for 24 hours. 34 Mb/s is available for 22 hours but 10 Mb/s is available during 12.00 – 14.00. Should the response be "Schedule not available" (as in the standard) or "Schedule available, except during 12.00 – 14.00 10Mb/s is available" (this would need a standard enhancement). The reserving PNO could then decide if the disruption in the reservation is acceptable and start the reservation procedure again with the knowledge of the resources available during the timeslot required.

With regard to the possible requirement for SVC configuration management, it may be presumed that each operator is responsible for its own routing tables and network dimensioning (trouble tickets, performance and usage information can be exchanged periodically).

- An ETSI standard is required for the area of ATM VC Configuration Management. This is expected to take the form of an enhancement to EN 300 820-1 [6].

N.2 Maintenance and Repair Processes

N.2.1 Issues and gaps

Currently the ITU-T and EURESCOM work has assumed that circuit and path designations will be based upon extensions to ITU-T Recommendation M.1400 [13] which have been reviewed and accepted by the ITU-T. Another possibility is to recommend the use of E.164 [44] and NSAP addresses. However, this would lead to a discrepancy that would need resolution.

- There may be conflict between the EN 300 820-2 [10] and the M.3208.1 [27] being aggressively developed by United States-based companies in the ITU-T Study Group 4 (SG4).
- The exact test suites, to be used for both automated and manual procedures, need to be checked against the tests used in the JAMES project. (Refer to P813/Deliverable 3 – "Operator's Handbook" [3].)
- An ETSI standard is required for the area of Fault Handling including ATM VP/VC Alarm Reporting and Trouble Ticket exchange aspects.

N.2.2 Dependencies and assumptions

There is an assumption that some minimum level of network protection and resilience should be specified for Phase 1 service introduction. This minimum may simply relate to the "Responsibility Rules" provided in clause 4 of the Configuration Management standard [6] or may take advantage of a more detailed specification provided by P708 Deliverable 5 [38].

N.3 Performance and QoS Processes

N.3.1 Issues and gaps

An ETSI standard is required for the area of ATM VP/VC Performance Management. This should be based on performance monitoring of accessible parts of the network segments supporting ATM VP/VC services and an exchange of information using a manual X.easi interface for Phase 1.

N.4 Accounting and Billing Processes

N.4.1 Issues and gaps

- A detailed ETSI Standard should be developed for the exchange of accounting and charging information, to which TS 101 674-2 [2] should be able to refer.

- There seems to be a lack of suitable interface specifications and products at present to support automated ATM service usage based accounting and charging.

- "Flat Rate" accounting has been proposed as the solution for Phase 1 ATM service introduction in the main part of the present document.

One issue is that an alternative method of providing inter-operator accounting management, may be on the basis of **usage-based"** measurements. If switched services (SVCs) are specified for Phase 1, usage-based accounting should be viewed as an additional requirement, subject to technology availability. For this purpose, usage metering functions would have to be available in the networks, where appropriate. Usage metering is the set of activities that monitor the utilization of network resources allocated for and used by each ATM connection. The information is recorded by the generation of Connection Detail Records (CDRs). The inter-operator interconnect service operation process requirement would then be to exchange CDR information over the X.easi interface in order to provide a means of mutual accounting and verification of charging-related data between interconnected operators.

If the network elements are capable of providing usage-based accounting information for switched ATM services, it should also be possible to apply the usage measurement techniques to semi-permanent services (i.e. PVPs, PVCs). Usage-based accounting processes for Phase 1 semi-permanent services would seem to be too ambitious to specify. However, a general migration to usage-based accounting for Phase 2 solutions would seem to be a desirable progression because end-users and operators are believed to be attracted to the notion of payment for actual ATM service usage, rather than be charged on comparatively unattractive flat-rate schemes.

Finally, the use of the CCR, described further in annex I, can be adapted to the usage-based accounting approach (as well as for the flat-rate accounting approach). In both cases, the requirement reduces to a simplification of data into manageable units and quantities for exchange using the X.easi interface (in either a manual or automated mode).

N.4.2 Dependencies and assumptions

It may be assumed that operation of commercial ATM based services which involve operator interconnect processes, will be dependent on a fair, consistent and mutually auditable means of accounting for services supplied and resources utilized.

N.5 Security Processes

N.5.1 Issues and gaps

Considerable support to the ITU-T proposal is coming from US suppliers of network management products for STASE ROSE [67] (refer also to annex D). It was approved as an ITU-T Recommendation, (ITU-T Q.813) in July 1998 and has a number of technical merits which include:

- Capability to support several OSI Applications (Management, FTAM, Directory Services, EDI).

- A similar conceptual level of abstraction in the transport protocol stack as found in common Information Technology industry Remote Procedure Call based models such as DCE and CORBA.

This implies that integration with these technologies and migration will be easier.

- By comparison with the proposals for a Phase 1 security solution (refer to the present document, subclause 6.6 and annex D), Phase 2 should consider deployment of a much more future oriented solution for VPN encryption technology based on the use of IPsec (Internet Protocol security). This may require the use of cryptographic security services requiring public key management and could significantly increase the implementation difficulties and costs.

  Alternatively, whilst IPsec supports the possibility of using an advanced public key management system (so-called PKI solution), its use is not absolutely necessary. It is possible to use an IPsec VPN where key management is handled through configuration of the devices by applying a shared secret at the time of installation (this is part of the IPsec standard). This was the solution that was used for IPsec VPN testing within P79. Hence, the deployment and use of such devices does not need to be very complex. The implementation difficulty depends on the ease of interconnecting platforms using CMIP over IP (an X.25 network may still be used as a DCN - i.e. IP over X.25).

In conclusion, no real problems in deploying a VPN solution are envisaged if the investment can be justified from a security requirements point of view.

N.5.2 Dependencies and assumptions

It is assumed that any proposal for a security solution for the X.easi interface is supportable by the majority of Network Management platforms which are commercially available.

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- ITU-T Recommendation X.711 (1997): "Information technology - Open Systems Interconnection - Common Management Information Protocol: Specification".
- ITU-T Recommendation X.722 (1992): "Information technology - Open Systems Interconnection - Structure of management information: Guidelines for the definition of managed objects", plus later amendments and corrigenda.
- ACTS (AC014) - CANCAN (Contract Negotiation and Charging in ATM) Project Deliverable 10 - Architecture and Systems Issues for ATM Accounting and Contracts, September 1997.
- JAMES AC111-RE1011/Teie/R/N/R/D14a1: "JAMES User Manual – Version 2".
- JAMES Project Deliverable 13 "Supervision of the performance of the JAMES network", August 1996 (JAMES confidential).
- NMF 502 "Peer-to-Peer Service Configuration Business Agreement, Issue 1.0", April 1997.
- Project James C111 – RE1011, 31st December 1997, "Guidelines and design rules for ATM Network Planning", editor Telenor.
- Project James Operations and Maintenance Manual Deliverable 13 AC111-RE1011/PT/N/DS/I/D13/a113_oam.
- EURESCOM P408 Deliverable 7 (November 1996): "Specifications of the Xuser Interface for ATM Network Management", Volume 1 (of 5) main part.
- JAMES AC111 – RE1011, Deliverable G2-WP2 (December 1997): "Guidelines and design rules for ATM network planning", Ed Telenor.
- EURESCOM Project P707, PIR 2.1e: "Requirements for Administration of Network Management Capability".
- JAMES AC111-RE1011/Teie/R/N/R/D14a1: JAMES User Manual – Version 2.
- JAMES Project Document AC111 - RE1011/FT-G2WP4.2-001, version 4 (final), 31st October 1996: "Definition of Xcoop", Ed. Michel Diverchy (France Telecom).

NOTE: This document is also informally known as "TC-2".

History

Document history		
V1.1.1	June 2000	Publication