The ATM Forum

Technical Committee

ATM APS Requirements and Logical MIB

af-nm-0183.000

March, 2002

The ATM Forum
Presidio of San Francisco
P.O. Box 29920 (mail)
572B Ruger Street (surface)
San Francisco, CA 94129-0920
Tel: +1-415.561.6275
Fax: +1-415.561.6120

Acknowledgements

The following people were instrumental in the development of the ATM Layer Automatic Protection Switching specification:

Ted Chang,
Weijing Chen,
Anthony Cooper,
Roger Kosak,
Kung Loh,
Gerhard Maegerl,
Scott Mansfield,
Tom Meserole,
Andrew Mayer,
Hiroshi Ohta,
Ken'ichi Sakamoto,
Ana Szpaizer,
Atahan Tuzel

Editors: Per Ferngren, Kin Yip Wong

TABLE OF CONTENTS

1. Introduction

ATM level protection switching (APS) is useful, from the service reliability point of view, to protect a Point-to-Point (PTP), Virtual Path (VP) or Virtual Channel (VC) connection or a logical group of VP/VC connections against service disruption due to failure, whether the failure occurs at the switch, the lower physical layer, or the ATM layer. Indeed, the ATM layer PS shall provide fast recovery time in case of a connection failure. The ATM level protection switching shall complement other protection switching capabilities, such as those provided by the physical layer (i.e., SONET/SDH) protection switching. This ATM level protection switching becomes a highly desirable capability for situations where physical layer protection switching is not supported or not operational.

1.1. Scope

In this document, the management and control requirements for the ATM APS will be presented from the network element point of view. The types of protection described here is the 1+1 and 1:1 types for PVCs, as these types of protection are the only ones fully specified in ITU-T I.630 [1]. The document covers protection of single PVC connections and PVC connection groups (VPG/VCG). The PVC connections are also limited to be of bi-directional type, that is the cell flow of the connections are bi-directional.

ATM Protection of point-to-multipoint connections is not described in this document. The reason for this is that there are currently no OAM mechanisms described for point-to-multipoint in ITU-T I.630 [1] which is the basis for this document.

1.2. Document organization

The document is organized as follows:

- Section 2 presents highlights of ITU-T's I.630 as the basis for the ATM APS requirements identified in this document.
- Section 3 describes generic ATM APS requirements.
- Section 4 describes configuration management requirements for ATM APS.
- Section 5 describes fault management and control requirements for ATM APS.
- Section 6 describes performance management requirements for ATM APS.
- Section 7 describes the M4 logical MIB for ATM APS based on the NE view.
- Section 8 provides the references.
- Appendix A presents the State Transitions Tables for ATM APS Working and Protection Entities.
- Appendix B presents a mapping between requirements in I.630 and those this document.

In the requirement sections (R) denotes mandatory requirements and (O) objectives. Note that support of ATM APS is *optional*, hence all requirements are *conditional* that they apply when the NE supports ATM APS.

2. Highlights of ITU-T's I.630 Document on ATM Layer Protection Switching

2.1. ITU-T's I.630 - Highlights

ITU-T's I.630 [1] document will be used as the basis of requirements for ATM layer APS. In addition, it will be used as input to the requirements for management and control, as described in this document.

This section will briefly highlight the content of I.630 on ATM APS. For details of each section, please refer to the relevant section(s) of the original document.

Section #	***Sub-Section #***	***Section/Sub-section Title***	***Brief Description***
1		Scope	Defines the scope of ATM APS.
2		References	A list of ITU-T recommendations is given.
3		Definitions	A comprehensive list of definitions used in ATM APS is given.
4		Symbols and Abbreviations	Lists all symbols and abbreviations used.
5		Protection Switching Principles	
	5.1	General Principles, Requirements and Objectives	Lists five main principles of ATM APS, and nineteen requirements and objectives.
	5.2	Examples of Network Protected Domains	Figure 2/I.630 presents four examples of protected domains.
	5.3	Extent of the Protected Domain	Figures 3-7/I.630 presents five examples of extents of protected domains.
	5.4	Dependency on Physical Layer Network Configuration	States that the protection and working entities should be routed on physically diverse transport entities.
	5.5	Protection Switching Configurations	Defines 1+1, 1:1 protection switching configurations.
	5.6	Protection Switching Performance	Defines a temporal model for ATM APS. *Note: No requirement on protection switching time is described or defined.*
	5.7	Hold-off Function in ATM Survivability Escalation	Explains why hold-off time is required.
	5.8	Protection Switching Control Protocol	Defines the ATM APS cell for exchange of coordination information exchange between protection switching nodes.
6		ATM VP/VC Protection Switching	
	6.1	Specific Requirements and Objectives	See 5.1.
	6.2	Protection Switching Trigger Mechanism	Lists four protection-switching triggers.
7		ATM VP/VC Group Protection Switching	
	7.1	Specific Requirements and Objectives	See 5.1.
	7.2	Architecture	Describes how a group of VPs/VCs can be protected using ATM APS. Figure 10/I.630 shows an example of a VPG. Describes the

			general characteristics of a VPG/VCG PS, and two architectures: 1+1 and 1:1.
	7.3	Protection Switching Triggering Mechanism	Lists four protection-switching triggers.
Annex A		Protection Switching Coordination Protocol for 1+1/1:1 Configuration	
	A.1	General Introduction	
	A.1.1	Application Architecture	Describes the 1+1 architecture (Figures A.1, A-2/I.630), and 1:1 architecture (Figures A-3, A-4/I.630) in some details.
	A.1.2	Compliance with Network Objectives	Describes various items related to ATM APS: extent of protection, switching types, protection switching protocols, operating modes, manual control, and other PS criteria.
	A.2	1+1/1:1 Linear Protection Switching Protocol	
	A.2.1	Switch Initiation Criteria	Describes the external, internal and state-induced switch initiation criteria.
	A.2.2	K1/K2 Bytes Generation Rules	Describes how the bits are defined and used in the K1 and K2 bytes in an ATM APS CP cell. Also defines the K1 Byte Coding of Requests (Table A.1/I.630).
	A.2.3	1+1/1:1 Linear Protection Switching Algorithm	Describes the principle of the 1+1/1:1 PS algorithm (Figure A.6/I.630). Describes the revertive and non-revertive modes, and transmission and acceptance of K1/K2 bytes. Two protocol examples are also presented: Table A.2/I.630 for 1+1, and Table A.3/I.630 for 1:1.
Annex B		1+1 Uni-directional SNC and Trail Protection Switching Operation	
	B.1	Application Architecture	Outlines the use of uni-direction PS in the 1+1 architecture.
	B.2	Compliance with Network Objectives	Describes various items related to ATM APS: switching types, protection switching protocols, operating modes, manual control, and other PS criteria.
	B.3	Switch Initiation Criteria	Describes the external, internal and state-induced switch initiation criteria. Table B.1/I.630 gives all local requests and their priorities that are important in the uni-directional 1+1 architecture.
	B.4	Protection Switching Protocol	States that no CP is required.
	B.5	1+1 Uni-directional Protection Switching Algorithm Operation	Describes various items such as control of the selector/bridge and the support of revertive/non-revertive modes in the uni-directional PS architecture.

2.2. Acronyms

AIS	Alarm Indication Signal
APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
CBR	Constant Bit Rate
CDV	Cell Delay Variation
CLR	Cell Loss Ratio
CP	Coordination Protocol
CTD	Cell Transfer Delay
FS	Forced Switch
LOS	Loss of Signal
MS	Manual Switch
NE	Network Element
NPC	Network Parameter Control
OAM	Operations and Maintenance
OS	Operation System
PCR	Peak Cell Rate
PD	Protected Domain or Protection Domain
PNNI	Private Network-Network Interface
PS	Protection Switching
PTP	Point-to-Point
PVC	Permanent Virtual Connection
QoS	Quality of Service
RDI	Remote Defect Indication
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SF	Signal Fail
SNC	Sub-Network Connection
SONET	Synchronous Optical Network
TTL	Trace Transit List
UPC	Usage Parameter Control
VBR	Variable Bit Rate
VC	Virtual Channel
VCC	Virtual Channel Connection
VCG	Virtual Channel Group
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VP	Virtual Path
VPC	Virtual Path Connection
VPG	Virtual Path Group
VPI	Virtual Path Identifier
VPL	Virtual Path Link
WTR	Wait-to-Restore

3. Generic ATM APS Requirements

3.1. Protection Connection/Entity

A network element supporting ATM APS shall be able to both protect:

- an end-to-end connection (a VP or VC trail) represented by two VPC termination points or VCC termination points in the NEs at the edge of the protected domain
- a part of a connection (a VP or VC sub-network connection) for example a connection segment represented by two VPL termination points or VCL termination points in the NEs at the edge of the protected domain.

(R-3.1)-1 An NE supporting ATM APS shall be able to handle protection of both VP or VC trails (VCC/VPC) and VP or VC sub-network connections (VPL/VCL).

(R-3.1)-2 The route and bandwidth of the working entity and the protection entity shall be provisioned by the user at set-up time once the two endpoints of a protection domain are known.

(O-3.1)-1 It is highly desirable that the protection and working entities should be routed on physically *diverse* transport entities.

It is desired that the working entity and the protection entity shall be provisioned to have the same characteristics so that any switching between the two entities will affect the protected connection (or connection group) in a minimal way. The characteristics that are of interest may vary depending on the application using the PVC, but the goal shall be to fulfill as many of the connection characteristics specified in (R-3.1)-3 and (R- 3.1)-4 as possible. These requirements are based on the ATM service architecture and the quality of service definitions specified in the ATM Forum Traffic Management specification [10]. The traffic control (UPC/UPC) functionality is also described more in detail in ITU-T I.371 [6].

(R-3.1)-3 The protection entity shall be provisioned to have the same (or similar) cell transfer characteristics as the associated working entity. The characteristics of interest here are:
- Conformance definition and Service category (CBR.1 , VBR.1 , VBR.2 etc)
- Cell delay variation (CDV)
- Policing behavior (UPC/NPC)
- Cell transfer delay (CTD)
- Shaping behavior
- Cell loss ratio (CLR)

(R-3.1)-4 The protection entity shall be provisioned to have the same bandwidth (PCR, SCR etc) as the associated working entity.

3.2. Protection Schema and PD Endpoints

(R-3.2)-1 The following ATM APS protection schema shall be supported:

- 1+1
- 1:1

(R-3.2)-2 For a 1+1 protection scheme, the source node shall provide a permanent bridge function for each protected VP/VC carried within a PD.

(R-3.2)-3 For a 1+1 protection scheme, the sink node shall provide a selector function for each protected VP/VC carried within a PD.

(R-3.2)-4 An ATM NE supporting a 1+1 protection scheme shall be also capable of operating in the 1+1 uni-directional protection scheme.

(R-3.2)-5 An ATM NE supporting a 1:1 protection scheme shall be also capable of operating in the 1+1 uni-directional protection scheme, or in the 1+1 bi-directional protection scheme.

3.3. VPG and VCG

(R-3.3)-1 The ATM PS capable NE shall support VPG and/or VCG.

(R-3.3)-2 If both VP and VPG (or VC and VCG) are supported in an ATM network, the VP and VPG (or VC and VCG) protection domains shall start and end between any two nodes capable of providing PS. However, the case in which exact overlapping of a VP PD and a VPG PD (or VC PD and VCG PD) is not allowed.

3.4. Protection Domains

(R-3.4)-1 The coupled and de-coupled protection domain shall be supported[1]

(R-3.4)-2 In an ATM network, the following topologies of PDs shall be supported:

- Cascaded PDs: where a PD's endpoints are all *outside* of another PD.

provided that this is consistent with the requirement that the PS action within a PD shall not interfere with the PS actions of other PDs.

[1] Note that for the cascaded and embedded cases, no overlapping of endpoint shall be allowed. In addition, the mixed cases where both the cascaded and embedded PDs are present shall be allowed. However, the complexity in configuring and maintenance may be quite substantial.

3.5. Impairment Clearing Condition

(R-3.5)-1 For signal fail condition, an impairment declaration shall be cleared after the AIS state remains continuously cleared for 5 seconds.

3.6. ATM APS Triggering

The standard OAM cells according to [2] will be used for ATM APS triggering.
Two cases exist:

- Coupled case: The protected domain is aligned with an OAM segment or end-to-end connection. In this case normal OAM end-to-end or segment termination functionality will be used to handle the APS triggering.
- De-coupled case: The protected domain is not aligned with a connection segment or end-to-end connection. In this case non-intrusive monitoring of the segment or end-to-end OAM flows must be used for APS triggering.

A protected group may be considered to be of the coupled type. In this case, the configured ATM APS channels (VPC/VCC test trails) are the connections that are coupled to the protection domain.

(R-3.6)-1 The existing OAM AIS cell described in I.610 [2] shall be used to communicate the ATM fault events for ATM APS.

(R-3.6)-2 The *coupled* VP/VC PS mechanism shall operate using the AIS and ATM APS coordination cells carried on either end-to-end or segment OAM cells of the VP/VC.

(R-3.6)-3 The *de-coupled* VP/VC PS mechanism shall operate using the AIS and the ATM APS coordination cells carried on either end-to-end or segment OAM cells of the VP/VC.

(R-3.6)-4 The VPG/VCG PS mechanism shall operate using the AIS and the ATM APS coordination cells carried on end-to-end or segment OAM cells at the ATM APS channels (VPC/VCC test trails) of the VPG/VCG.

(R-3.6)-5 The following ATM APS triggering events shall be supported:
-A locally detected impairment at the sink node e.g. Signal Fail or Signal Degrade[2]
-Reception of an AIS indication by the sink node.
-Local craft command directed toward the sink node.
-APS Coordination cells received by the end nodes.
-A WTR timer expires.

(R-3.6)-6 The PS mechanism shall take bridge/switch action based on the status of both the working and protection entities.

[2] Note that how to implement a trigger on Signal Degrade is for further study according to [1].

3.6.1. APS Inter-layer Escalation Strategy

(R-3.6.1)-1 The PS mechanism shall support a hold-off time at the sink node to delay the initialization of ATM APS.

(R-3.6.1)-2 The value of the hold-off time ranges from 0 to 10 seconds in 500 ms increments, with a default value of 500 ms.

(R-3.6.1)-3 After expiration of the hold-off time, and with continued detection of the impairment, the PS shall be activated.

3.6.2. Protection Switching Commands

(R-3.6.2)-1 The following automatic and external commands shall be supported by an ATM APS-capable NE:

- Clear
- Freeze
- Lockout of Protection
- Signal Fail for Protection
- Forced Switch for Working
- Signal Fail for Working
- Signal Degrade for Protection
- Signal Degrade for Working
- Manual Switch for Protection
- Manual Switch for Working
- Wait-to-Restore
- Do Not Revert
- No Request

(R-3.6.2)-2 The protection switching commands as listed in requirement (R-3.6.2)-1 shall be handled in the priority order defined in ITU-T I.630 table A.1 and table B.1.
Note: As seen in these tables the ‘Forced switch for working’ and ‘Signal Fail for protection’ have different priority order depending on if the protection switching is uni-directional (not using the APS coordination protocol) or bi-directional.

3.6.3 ATM APS Channel

A protected VP or VC will use the standard OAM cells according to [2] for APS signaling. For example, a protected VP will use either an OAM cell with VCI=3 (segment) or an OAM cell with VCI=4 (end-to-end) for signaling of the APS commands. This means that no provisioning of a separate ATM APS channel is needed for a protected VP or VC. A VPG/VCG on the other hand,

needs a separately defined ATM APS channel (test trail VPC/VCC) for the working and the protection entity, where the ATM APS signaling may be carried.

(R-3.6.3)-1 For each protected VPG/VCG, a bi-directional ATM APS channel (VPC/VCC) shall be set up on both the working and protection entities in the associated *de-coupled* PD.

(R-3.6.3)-2 For each protected VPG/VCG, the ATM APS channel shall be composed of a VPC/VCC whose endpoints correspond to the source and sink nodes of the *de-coupled* PD.

(R-3.6.3)-3 For a protected VPG/VCG, the source node and the sink node shall each maintain the following information:

- A VPG/VCG identifier.
- The VPIs/VCIs of the associated VPs/VCs that belong to the VPG/VCG.
- The ATM APS channel number (i.e., VPI or VPI/VCI) of the VPG/VCG for both the working and protection entities.

3.6.4. ATM APS Coordination Protocol and Messages

(R-3.6.4)-1 An ATM APS capable NE shall support the exchange of *one* coordination message (i.e., one OAM APS CP cell) to carry out a PS, for all protection switching schema where this is needed: 1+1 bi-directional, 1:1 bi-directional.

(R-3.6.4)-2 The coordination protocol shall be carried on an OAM APS CP cell.

(R-3.6.4)-3 The *Group* and *Individual* functional types in the OAM APS CP cell shall be supported.

(R-3.6.4)-4 For a *coupled* PD, all OAM APS CP cells shall be carried on the protection entity. OAM cell SF-P and SD-P (for monitoring the protection entity) shall be carried on the working entity.

(R-3.6.4)-5 For a *de-coupled* PD, all OAM APS CP cells shall be carried on the ATM APS channel associated with the protection entity. OAM cell SF-P and SD-P (for monitoring the protection entity) shall be carried on the ATM APS channel associated with the working entity.

(R-3.6.4)-6 The coordination message shall be carried by two bytes, K1 and K2 within the OAM APS CP cell.

(R-3.6.4)-7 The K1 and K2 bytes shall indicate respectively the protection switching requests, and the entity to which the request applies (See Table A.1/I.630 and section A.2.2 of I.630).

(R-3.6.4)-8 The OAM APS CP cell shall be emitted as soon as possible after a change in the K1/K2 bytes occurs.

(R-3.6.4)-9 After emitting an OAM APS CP cell triggered by a change in the K1/K2 bytes, an OAM APS CP cell shall be emitted once every 5 seconds to ensure proper protocol operation where the OAM APS CP cells are lost or invalid.

3.7. Revertive/Non-revertive Modes and Timer

(O-3.7)-1 An ATM APS capable NE that supports the 1+1 protection scheme may be required to support non-revertive mode.

(O-3.7)-2 An ATM APS capable NE that supports the 1:1 protection scheme may be required to support non-revertive mode.

(R-3.7)-1 If both revertive and non-revertive modes are supported, then the default mode shall be non-revertive.

(R-3.7)-2 In a revertive mode of operation, working traffic shall be switched back to the working entity when the impairment has been cleared, the Wait-to-Restore (WTR) timer expires, or is overridden.

(R-3.7)-3 The WTR timer shall be initiated after the impairment is repaired.

(R-3.7)-4 The WTR shall be user settable from 1 to 30 minutes, in increments of 1 minute. The default value is 12 minutes.

3.8. Handling of Extra Traffic in 1:1 Protection Scheme

(R-3.8)-1 If Extra Traffic is supported on the protection entity, it shall be dropped (disconnected) immediately when the protection entity takes over the working traffic.

(R-3.8)-2 If Extra Traffic is dropped due to a PS, then an AIS signal shall be inserted at the sink node[3] for the Extra Traffic.

(R-3.8)-3 If Extra Traffic is supported, then it shall be allowed to be re-inserted again once the protection entity is cleared from carrying the working traffic.

[3] Where the selector function resides.

4. ATM APS Configuration Management Requirements

4.1. VP/VC

(R-4.1)-cm-1 The M4 Interface of an ATM NE that supports ATM VP/VC PS shall support management systems request to configure a VP/VC working /protection connections. The following ATM APS parameters shall be supported:

- Designate which VP/VC connection as *working* or *protecting*.
- Designate the protection scheme used, i.e., 1+1, 1:1
- Designate the protection as *uni-directional* or *bi-directional*.
- Designate the protection switching as *revertive* or *non-revertive*.

(R-4.1)-cm-2 At an ATM NE that is an ATM VP/VC protection switching point, its M4 Interface shall support management systems request to configure the hold-off time at each VP/VC connection selector/switch point. The hold-off timer shall be set to a value from 0 to 10 seconds, in 500 ms increments. The default value shall be 500 ms.

(R-4.1)-cm-3 At an ATM NE that is an ATM VP/VC protection switching point, its M4 Interface shall support management systems request to configure the expiration time of the Wait-to-Restore (WTR) timer for each protected VP/VC connection switch point, if revertive mode is supported. The WTR shall be configured from 1 to 30 minutes, in 1-minute increment. The default value shall be 12 minutes.

(R-4.1)-cm-4 The M4 Interface of an ATM NE that supports ATM VP/VC PS shall support management systems request to configure a protected VP or VC as a coupled or *de-coupled* protected VP or VC.

(O-4.1)-cm-1 The M4 Interface of an ATM NE that supports ATM VP/VC PS should support management systems request to configure the triggering mechanism (e.g. end-to-end AIS, Signal Loss etc.) to use for the ATM APS.

(R-4.1)-cm-5 The M4 Interface of an ATM NE that supports ATM VP/VC PS shall support management systems request to retrieve information of a VP/VC that has ATM APS capability.

(R-4.1)-cm-6 The M4 Interface of an ATM NE that supports ATM VP/VC PS shall support management systems request to retrieve the PD endpoints of the VP/VC.

(R-4.1)-cm-7 The M4 Interface of an ATM NE that supports ATM VP/VC PS shall support management systems request to retrieve the protection mode (i.e., revertive, non-revertive).

(R-4.1)-cm-8 The M4 Interface of an ATM NE that supports ATM VP/VC PS shall support management systems request to retrieve the protection scheme used (i.e., 1+1, 1:1).

(R-4.1)-cm-9 The M4 Interface of an ATM NE that supports ATM VP/VC PS shall support management systems request to retrieve the protection direction (i.e., uni-directional, bi-directional).

4.2. VPG/VCG

(R-4.2)-cm-1 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to configure the *working* and *protecting* VPG/VCG. For each VPG/VCG, the following parameters shall be supported:

- A VPG/VCG identifier.
- Designate which VPG/VCG as *working* or *protecting*. Both shall use the same VPG/VCG identifier.
- The VPIs/VCIs of the associated VPs/VCs that belong to the VPG/VCG.
- The ATM APS channel number (i.e., VPI or VPI/VCI) of the VPG/VCG for both the working and protection entities.
- Designate the protection scheme used, i.e., 1+1, 1:1.
- Designate the protection as *uni-directional* or *bi-directional*.
- Designate the protection switching as *revertive* or *non-revertive*.

(O-4.2)-cm-1 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to configure the *working* and *protecting* VPG/VCG. For each VPG/VCG, the following parameter should be supported:

- Triggering mechanism to use (end-to-end AIS, Signal Loss , etc)

(R-4.2)-cm-2 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to add/delete a VP/VC to/from an existing VPG/VCG. The VP/VC that is added shall have the same endpoints as that of the VPG/VCG.

(R-4.2)-cm-3 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve information of a VPG/VCG that has ATM APS capability.

(R-4.2)-cm-4 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve the number of VPGs/VCGs being provisioned.

(R-4.2)-cm-5 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve the VPs/VCs that are associated with a specified VPG/VCG.

(R-4.2)-cm-6 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve the PD endpoints of the VPG/VCG.

(R-4.2)-cm-7 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve the ATM APS channel associated with the working and protection VPG/VCG.

(R-4.2)-cm-8 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve the protection mode (i.e., revertive, non-revertive).

(R-4.2)-cm-9 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve the protection scheme used (i.e., 1+1, 1:1).

(R-4.2)-cm-10 The M4 Interface of an ATM NE that supports ATM VPG/VCG PS shall support management systems request to retrieve the protection direction (i.e., uni-directional, bi-directional).

4.3. Miscellaneous

The following requirements are for both VP/VC PS and VPG/VCG PS.

(R-4.3)-cm-1 The M4 Interface of an ATM NE that supports ATM APS should support management system requests to retrieve the current ATM APS command/request (according to (R.3.6.2)-1) of highest priority at each end of the protected domain. This is the request that is currently in operation thus affecting the bridge and/or selector status and any APS signaling from the APS End Point.

(R-4.3)-cm-2 The M4 Interface of an ATM NE that supports ATM PS shall support management systems request to perform the following commands towards each end of the protected domain for a protected VP/VC or a protected VPG/VCG:
-Freeze local protection switching function
–Lockout of protection
–Forced switch for working entity
–Manual switch for protection entity
–Manual switch for working entity
–Clear (clears any or the requests above)

(O-4.3)-cm-2 The M4 Interface of an ATM NE that supports ATM PS should support management systems request to retrieve the current values of the K1 and K2 bytes.

(R-4.3)-cm-3 The M4 Interface of an ATM NE that supports ATM PS shall support management systems request to retrieve state information on a working/protection entity. The following states from M.3100 [3] shall be supported: *operationalState* and *administrativeState,* in addition, the following status from X.731 [4] shall be supported: *availabilityStatus*.

(R-4.3)-cm-4 State transitions of the working and protection entities shall be consistent with the state transitions shown in Table -1 (See Appendix A).

(O-4.3)-cm-3 The M4 Interface of an ATM NE that supports ATM PS may optionally support management system requests to configure extra traffic to the interface where the protection entity is located. The extra traffic shall be associated with the protected individual connection (VP or VC) or with the protected group (VPG/VCG).

(CR-4.3)-cm-1 If the ATM NE supports extra traffic for ATM APS then it shall allow the management system to configure extra traffic with a maximum bandwidth not exceeding the reserved bandwidth for the associated working/protection entity.

(CR-4.3)-cm-2 If the ATM NE supports extra traffic for ATM APS then it shall allow the management system to configure extra traffic onto the protection interface only using other VPI/VCI values than used by the protection entity itself.

5. ATM APS Fault and Control Management Requirements

The following requirements apply to both source and sink nodes of a PD.

(R-5)-fm-1 The M4 Interface of an ATM NE that supports ATM PS shall generate notifications to report service interruptions. It shall report the value of the Defect Type associated with a PS event. The following events shall be reported for each protected connection associated with the VP/VC, or for each VPG/VCG:

- Local automatic switch from working to protection entity.
- Local automatic reversion from protection entity to working entity.
- Local failure to switch after detection of Signal Fail/Signal Degrade that persists for at least the hold-off time.
- Local failure to switch after expiration of Wait-to-Restore timer.
- Local failure of a bi-directional protection entity to switch after a switch at the far-end of the PD.
- Failure of the far-end of a bi-directional protection entity to switch after the near-end is switched.
- Detected far-end use of an external command, i.e., Lockout of Protection, Forced Switch, Manual Switch, Freeze, and Clear.

(R-5)-fm-2 The M4 Interface of an ATM NE that supports ATM PS shall generate a notification to report a mismatch between the received far-end bridge/selector status and the local bridge/selector status. It shall generate a notification if the mismatch persists for more than m seconds. For cases where the mismatch is caused by lost OAM APS CP cells, the value of m shall be long enough for 3 lost OAM APS CP cells.

6. ATM APS Performance Management Requirements

The following requirements apply to both source and sink nodes of a PD.

(R-6)-pm-1 The M4 Interface of an ATM NE that supports ATM PS shall be able to retrieve ATM APS counts. The ATM APS capable NE shall collect ATM APS counts at either *one* of the endpoints of a PD for a bi-directional protection type, and at both endpoints of a PD for an uni-directional protection type.

(R-6)-pm-2 The M4 Interface of an ATM NE that supports ATM PS shall be able to retrieve *failed* ATM APS counts. The ATM APS capable NE shall collect *failed* ATM APS counts at either *one* of the endpoints of a PD for a bi-directional protection type, and at both endpoints of a PD for an uni-directional protection type. The *failed* ATM APS count shall cover the following failures:

- Local failure to switch after detection of Signal Fail/Signal Degrade that persists for at least the hold-off time.
- Local failure to switch after expiration of Wait-to-Restore timer.
- Local failure of a bi-directional protection entity to switch after a switch at the far-end of the PD.
- Failure of the far-end of a bi-directional protection entity to switch after the near-end is switched.

(R-6)-pm-3 The M4 Interface of an ATM NE that supports ATM APS shall be able to retrieve the number of successful of APS switching events. The ATM APS capable NE shall be capable to collect the *successful switchover count* at either one of the end points of a protected domain for bi-directional protection switching, and at both endpoints of the protected domain for an uni-directional protection type.

The *successful switchover count* shall be the sum of:
- the number of successful switchovers from the working entity to the protection entity and the number of successful switchovers from the protection entity to the working entity

7. M4 Logical MIB

7.1 Administrative and Operational state

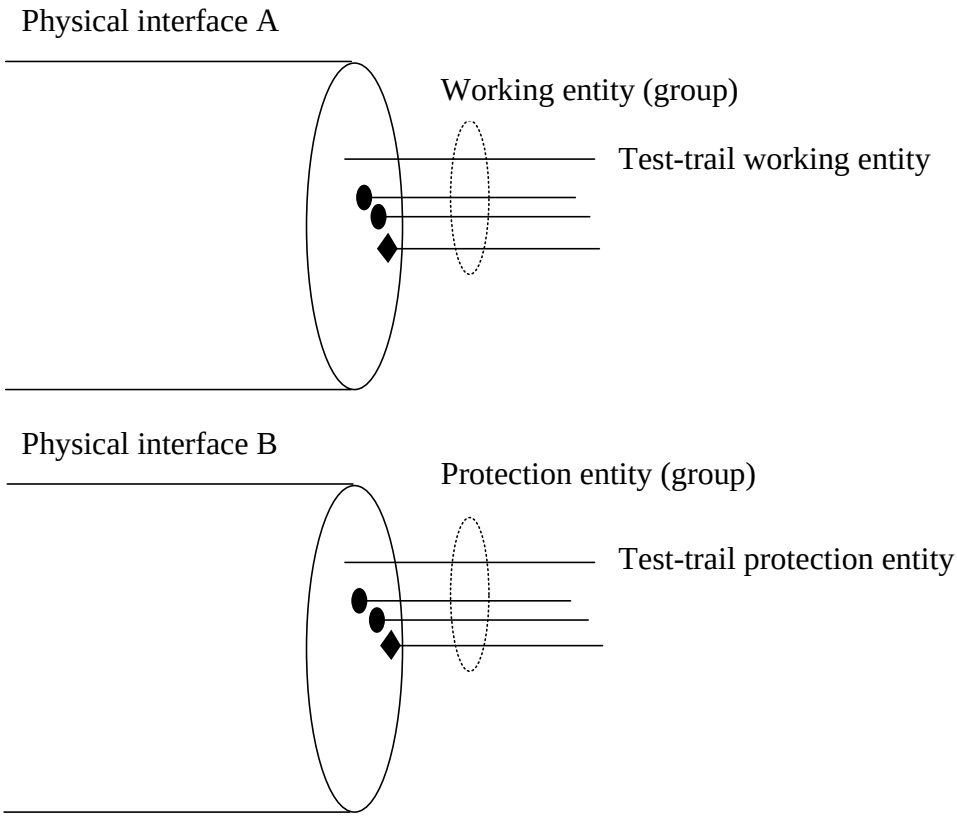
The ATM APS managed entities described in section 7.4 do not have an administrative state attribute. This is because the underlying entities such as the VPL, VCL etc already have an administrative state associated with them. The same situation is also true for the operational state. As this is already present in the underlying entities it is not implemented in the ATM APS entities as well. An ATM APS Availability Status attribute, that is more suiting to the ATM APS functionality, has been included instead.

7.2. Group protection

Group protection may be used to protect a logical bundle of connections with another bundle of similar connections. The idea here is to protect all connections set up within a logical bundle at the working interface by creating the same type of connections at the protection interface. This is illustrated in the figure 1 below where the connections at interface A are protected with a similar group of connections at interface B. The test trails needed for the working and protection entity are also shown in the figure. The group illustrated in the figure can be seen as a mixed VPG/VCG, that is, both VPs and VCs are protected in this case.

All connections within the protected group will be protected pair-wise. Each VP (or VC) at Interface A is protected by a similar VP (or VC) at Interface B. In the logical MIB the two VPs (or VCs) will be associated with one instance of the *ATM APS Working/Protection Pair* managed entity. That is, the protected group will consist of several *ATM APS Working/Protection Pair* managed entities all of them belonging to one *ATM APS End Point* (See also figure 7).

NOTE: To protect all the VCLs within a VPC Termination Point is suggested to protect the VPC Termination Point itself instead of grouping the individual VCLs into a protection group (See figure 8). The two different approaches will however give the same behavior for the individual VCs.



Legend:

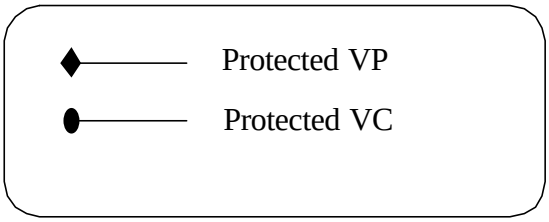


Fig 1:Illustration – Group protection

7.3. Extra traffic

For an ATM APS entity using the 1:1 protection scheme, it is optionally possible to use the bandwidth of the protection entity to transport other traffic (extra traffic) during time periods when the protection entity is operating as a standby. As soon as a protection switch occurs from the working to the protection entity the extra traffic associated with the protected connection (or protected group) will be disconnected. When the 'normal traffic' switches back to the working entity (for example at revertive switching) the extra traffic at the protection entity will be enabled again.

The bandwidth of the extra traffic associated with the APS End Point may not exceed the bandwidth configured to the protection entity itself (see (CR-4.3)-cm-1). The extra traffic must also use different VPI/VCI values than the ones used by the protection entity according to (CR-4.3)-cm-2.

A separate ATM APS Extra Traffic managed entity is provided that will allow the configuration of extra traffic into the protection entity. See figure 6 for an example of how the ATM APS Extra Traffic may be used together with a protected VCL.

7.4. MIB entries

7.4.1. ATM APS End Point

An instance of this managed entity is used to represent one of the two ATM APS end points that delimit a protection domain. A pair of instances of ATM APS End Point shall be used to define a protection domain. These two ATM APS endpoints will always be located in two different Network Elements.

If a VP PD and a VPG PD (or a VC PD and VCG PD) are supported by an ATM node (i.e., both PDs have this ATM node as an ATM APS end point), the VP (or VC) end points of these PDs shall not coincide (see (R-3.3)-2). For this ATM node, two separate ATM APS End Point instances shall be used: one for the VP PD (or VC PD), and another for the VPG PD (or VCG PD).

Attributes

Managed Entity Id: This attribute provides a unique name for the ATM APS End Point instance. (R, Set-by-Create) (mandatory)

Protection Scheme: This attribute denotes the scheme of ATM APS protection supported by the NE - 1+1, or 1:1. (R, W) (mandatory)

Protection Direction: This attribute denotes if one or both directions of the cell flow will be affected when a protection-switching event occurs. Valid values are: uni-directional, bi-directional. (R, W) (mandatory)

Protection Mode: This attribute denotes the ATM APS protection mode - Valid values are: revertive, and non-revertive. Default is non-revertive. (R, W) (mandatory)

Group Protection Indicator: This attribute identifies if the ATM APS end point is used for group protection (VPG/VCG) or not. Possible values are true or false. If the attribute is set to true the ATM APS end point is used for group protection otherwise it is used for protection of an individual connection (R, W) (mandatory)

Working/Protection Pair List: This attribute points to the Working/Protection Pair managed entity (or entities if group protection) associated with the ATM APS End Point.
(R) (mandatory)

ATM APS Test Trail Working Entity: This attribute specifies the used VPI/VCI of the test trail (APS channel) associated with the working entity at group protection. (R) (mandatory)

ATM APS Test Trail Protection Entity: This attribute specifies the used VPI/VCI of the test trail (APS channel) associated with the protection entity at group protection. (R) (mandatory)

Coupling Indicator: This attribute denotes whether the associated ATM end point is an OAM flow end point. Valid values are: none, end-to-end point, and segment-end point. Note that the value 'none' is only applicable for group protection or for a non-intrusively monitored ATM APS connection. The value of the attribute will be automatically set depending on the properties of the associated managed entities (Properties of the VP or VC termination points associated with the Working or Protection entities) (R) (mandatory)

ATM APS Trigger List: This attribute identifies the list of trigger mechanisms used.
Valid values in the list are (order in the list is not important):
-End-to-end AIS (Alarm Indication Signal)
-Segment AIS
-Signal Degrade
-Loss Of Signal
(Note that how to implement a trigger on Signal Degrade is for further study according to [1]). (R, W) (optional)

Hold Off Timer: This attribute defines the duration of the hold-off timer in ATM APS. Valid values are : 0 ms or multiples of 500 ms with a maximum of 10 s. Default is 500 ms. (R, W) (mandatory)

WTR Time: This attribute defines the duration of waiting time before reversion. Valid values are: 1 to 30 min. Default is 12 min. (R, W) (mandatory)

ATM APS Request List: This attribute displays a list of the local ATM APS requests (operator initiated or automatically initiated) that currently are active. The list is sorted in priority order. Valid requests in priority order are:
-Freeze
-Lockout of protection entity

-Signal fail for protection entity[a]
-Forced switch for working entity[a]
-Signal fail for working entity
-Signal degrade for protection entity
-Signal degrade for working entity
-Manual switch for protection entity
-Manual switch for working entity
-Wait to restore for working entity
-Do not revert for working entity
-No Request (None of the requests above is currently in operation)
(R) (mandatory)
a) Note: As noted in requirement (R-3.6.2)-2 the 'Forced switch for working' and 'Signal Fail for protection' have different priority order depending on if the protection switching is uni-directional (not using the APS coordination protocol) or bi-directional.

Current K1/K2 Byte: This attribute denotes the current K1 and K2 byte values. (R) (mandatory)

Selector Status: This attribute provides information about if incoming ATM cells are received at the Working or the Protection entity. Valid values are: working, protection. (R) (mandatory)

Bridge Status: This attribute provides information about if outgoing ATM cells are sent into the Working or the Protection entity or both. Note that for 1+1 protection the attribute will always have the value both. Valid values are: working, protection, both. (R) (mandatory)

ATM APS Availability Status: This attribute denotes the operational states of the ATM APS End Point instance. When the ATM APS end point cannot provide its service, i.e. when both the working and protection entity are out of service this attribute will be set to disabled. If either the working or the protection entity (but not both) is out of service this attribute will be set to degraded. Valid values are: fully operational, degraded, disabled. (R,) (mandatory)

Actions

Add ATM APS Working/Protection Pair: This operation adds an ATM APS Working/Protection Pair (W/P Pair) managed entity to the ATM APS end point. This is done through selecting a Working Entity and a Protection Entity from the available termination points in the NE. The termination points attached to an ATM APS W/P Pair must be of the same type and with identical (or similar) characteristics according to (R-3.1)-3 and (R-3.1)-4. If the type or characteristics of the two termination points does no match this operation will be rejected.
The possible termination point types that may be attached to an ATM APS W/P Pair are VCLs, VPLs, VCC or VPC termination points.
In case of group protection, several ATM APS W/P Pair managed entities may be attached to the ATM APS End Point. The working entities of the protected group shall be located at the same physical device (interface) as the ATM APS test trail of the working entity (see below). The protection entities of the protected group shall be located at another physical device. This device shall be the same as the one where the ATM APS test trail of the protection entity is located.

Delete ATM APS Working/Protection Pair: This operation deletes an ATM APS W/P Pair managed entity from the ATM APS End Point.

Create ATM APS Test Trail: This operation will create a test trail for the Working or Protection entity if group protection is used. Input data is:
-If the test trail shall be added for the working or protection entity
-The Interface and VPI of the test trail if the test trail is of VPC type or
-The Interface, VPI and VCI of the test trail if the test trail is of VCC type (In this case, VPCs to carry the test trail VCCs must have been created in advance at the interfaces associated with the working and protection entities)

The test trails for the working and protection entity shall be created prior to adding any ATM APS Working/Protection Pairs to the ATM APS end point. The test trails for the working and protection entity shall be created at different physical devices (interfaces).

Delete ATM APS Test Trail: This operation will delete a test trail from the Working or Protection entity if group protection is used. Input data is if the test trail shall be deleted for the working or protection entity.

Set ATM APS Request (*ManualRequest*): This action will set (activate) the *ManualRequest* at the ATM APS End Point. Valid manual requests in priority order are:
-Freeze
-Lockout of protection entity,
-Forced switch for working entity
-Manual switch for protection entity
-Manual switch for working entity
For a description on the manual requests above see 7.4.1.1. Note that the freeze request may be combined with any of the other requests in the list above.

Clear ATM APS Request (*ManualRequest*): This action will clear (de-activate) the indicated *ManualRequest* at the ATM APS End Point. For a description on the available manual requests see 7.4.1.1.

Notifications

ATM APS Status Change: This notification will be sent as soon as any of the status attributes of the ATM APS point change. The status attributes that shall be supervised are:
- ATM APS Request List
- ATM APS Availability Status
- Selector Status
- Bridge Status

ATM APS Switch Fail Indication: This notification will be sent when the protection switching has failed at the ATM APS end point. The notification shall if available contain detailed information about the cause of the outage, e.g.:

- Local failure to switch after detection of Signal Fail/Signal Degrade
- Local failure to switch after expiration of Wait-To-Restore timer
- Local failure to switch after a switch in the far end (at bi-directional protection switching). The notification shall in this last case be sent after a time period allowing 3 lost OAM APS CP cells (see (R-5)-fm-2).

Attribute Value Change: This notification is used to report change to the attributes of this managed entity instance. The notification shall identify the attribute that has changed, its old value, and its new value. (mandatory)

Managed Entity Creation: This notification is used to report the creation of an instance of this managed entity. (mandatory)

Managed Entity Deletion: This notification is used to report the deletion of an instance of this managed entity. (mandatory)

Relationships

One instance of the ATM APS End Point shall be instantiated for each end of a protected domain. Multiple instances of the ATM APS End Point managed entity may exist for each ATM APS-capable ATM node which is also one of the pair of ATM nodes that delimit a protection domain.

Each instance of the ATM APS End Point managed entity is associated with one or several (if group protection) instances of the ATM APS Working/Protection Pair (W/P Pair) managed entity. The ATM APS W/P Pair entity in turn is associated with two termination points of identical type (either VPC, VPL, VCC or VCL) and with similar characteristics (according to (R-3.1)-3 and (R-3.1)-4).

7.4.1.1. Manual request descriptions

The following manual requests can be set or cleared using the ‘Set ATM APS Request’ or ‘Clear ATM APS Request’ actions of the ATM APS End Point:

- Freeze: This operation will freeze (maintains) the current protection switch positions and the currently transmitted K1/K2 byte values for the local protection switching function. It has the highest priority of all external commands other than Clear. I.e., all commands other than Clear are ignored when Freeze is enabled.

- Lockout of Protection: This operation will deny all working traffic (but not Extra Traffic) access to the protection entity.

- Forced Switch for Working: This operation will bridge/switch the working traffic to the protection entity.

- Manual Switch for Protection: This operation will deny working traffic access to the protection entity unless a higher priority request is in effect, in which case this command is preempted (removed) by the higher priority request.

- Manual Switch for Working: This operation will bridge/switch working traffic to the protection entity unless a higher priority request is in effect or an impaired condition is detected on the protection entity, in which case this command is preempted (removed) by the higher priority request.

7.4.2. ATM APS Working/Protection Pair

An instance of this managed entity is used to represent a pair of working and the protection entities associated with an ATM APS End Point instance. Note that this ATM APS Working/Protection Pair (W/P Pair) Entity instance *does* not represent the *entire* working and protection entity that may contain several ATM nodes. Indeed, this instance only represents the portion of the protection domain that is APS-controllable by the instance of the ATM APS End Point.

Attributes

Managed Entity Id: This attribute provides a unique name for the ATM APS W/P Pair entity instance. The identifier could for example be the interface identifier, VPI (and VCI) of the termination point associated with the Working Entity. The identifier is assigned when the ATM APS W/P Pair entity is created. (R, Set-by-Create) (mandatory)

Supporting Working Termination: This attribute identifies the termination point (VPL, VPC, VCL or VCC) associated with the Working Entity. Note that the underlying termination point specified in this attribute will be of the same type as the one specified in the Supporting Protection Termination attribute below. (R, Set-by-Create) (mandatory)

Supporting Protection Termination: This attribute identifies the termination point (VPL, VPC, VCL or VCC) associated with the Protection Entity. Note that the underlying termination point specified in this attribute will be of the same type as the one specified in the Supporting Working Termination attribute above. (R, Set-by-Create) (mandatory)

Notifications

Attribute Value Change: This notification is used to report change to the attributes of this managed entity instance. The notification shall identify the attribute that has changed, its old value, and its new value. (mandatory)

Managed Entity Creation: This notification is used to report the creation of an instance of this managed entity. (mandatory)

Managed Entity Deletion: This notification is used to report the deletion of an instance of this managed entity. (mandatory)

Relationships

One instance of this ATM APS Working/Protection Pair Entity shall be instantiated for each protected connection (VPL, VPC, VCL or VCC) at each end of the protected domain (in a 1+1 or 1:1 protection scheme).

At protection of a single connection one instance of this managed entity is associated with the ATM APS End Point. At group protection several instances of this managed entity are associated with the ATM APS End Point. One instance of this entity is then created for each protected connection within the group.

One instance of the ATM APS Working/Protection Pair is associated with two termination point instances where the two termination points shall be of the same type (either VPC, VPL, VCC or VCL) and with similar characteristics (See (R-3.1)-3 and (R-3.1)-4).

7.4.3. ATM APS Extra Traffic

An instance of this managed entity shall be created for each VC or VP used to carry extra traffic associated with a certain ATM APS End Point. The entity is only possible to create when the protection type associated with the APS end point is of 1:1 type. Several connections (VPs and/or VCs) may be used to carry extra traffic on the protection entity of the APS End Point. The bandwidth of the Extra Traffic Links (VPLs or VCLs) associated with the APS End Point may not exceed the bandwidth configured to the working entity itself (see (CR-4.3)-cm-1). The extra traffic must also use different VPI/VCI values than the ones used by the protection entity according to (CR-4.3)-cm-2. See figure 6 for an example of how the ATM APS Extra Traffic may be used.

Attributes

Managed Entity Id: This attribute provides a unique name for the ATM APS Extra Traffic entity.

Extra Traffic Link: This attribute points at the VPL or VCL used to carry extra traffic at the interface associated with the protection entity of the ATM APS End Point.

Relationships

One instance of this entity shall be created for each connection carrying extra traffic for a certain ATM APS End Point. Several instances of this entity may thus be related to one ATM APS End Point.

7.4.4. ATM APS Current Data

An instance of this managed entity is used to collect and report data associated with the ATM APS function supported by the ATM APS End Point.

Instances of this managed entity are created by the ATM NE upon instantiation of an ATM APS End Point instance, or by request of the managing system for selected instances of ATM APS End Point managed entity.

Instances of this managed entity are deleted by the ATM NE upon deletion of the associated ATM APS End Point instance, or by request of the managing system.

Attributes

Managed Entity Id: This attribute provides a unique name for the managed entity instance in the ATM NE. (R, Set at Creation) (mandatory)

Administrative State: This read/write attribute is used to activate (unlock) and deactivate (lock) the data collection function performed by this managed entity. (R, W) (mandatory)

Suspect Flag: This attribute indicates the reliability of the ATM APS Current Data collected by the managed entity. This attribute may take on one of two possible values: reliable and unreliable (suspect). (R) (optional)

Elapsed Time: This attribute represents the difference between the current time and the start time of the present summary interval. (R) (optional)

Threshold Data Id: This read/write attribute provides a pointer to an instance of the Threshold Data managed entity that contains the threshold values for the performance monitoring data collected by this managed entity. (R, W) (mandatory)

Number Of Suppressed Intervals: This attribute is present only if the ATM NE is suppressing ATM APS History Data creation when the current interval terminates with "all-zeroes" performance measurements. (R) (mandatory)

Failure to Switch on SF/SD: This attribute provides a raw, thresholded count of the number of failure to switch after detection of SF/SD (R, S=D, D=0) (mandatory)

Failure to Switch after WTR expired: This attribute provides a raw, thresholded count of the number of failure to switch after the expiration of the Wait to Restore timer. (R, S=D, D=0) (mandatory)

Failure to Switch after Far-End Switch: This attribute provides a raw, thresholded count of the number of failure to switch at the near-end, after a switch at the far-end of the PD for a bi-directional protection entity. (R, S=D, D=0) (mandatory)

Failure to Switch after Near-End Switch: This attribute provides a raw, thresholded count of the number of failure to switch at the far-end, after a switch at the near-end of the PD for a bi-directional protection entity. (R, S=D, D=0) (mandatory)

Successful Switches: This attribute provides a raw, thresholded count of the number of successful protection switching events that has occurred at this end of the PD (near end) during this measurement interval. The *Successful Switches* shall be the sum of the number of switchovers from the working entity to the protection entity and the number of switchovers from the protection entity to the working entity (R, S=D, D=0) (mandatory)

Actions

Reset: This operation resets a given Current Data Counter. (Optional.) This operation allows the user to reset a given current data counter within the Current Data managed entity.

Notifications
Threshold Crossing Alert: This message is used to notify the management system when the value of the above count exceeds a pre-set threshold. The following information shall be supplied with this notification: (optional)

- The ID of the Managed Entity reporting the Threshold Crossing Alert
- The type of performance parameter that exceeds the threshold

Relationships

One instance of this managed entity will be created automatically for each instance of the ATM APS End Point. The ATM APS Current Data managed entity and the associated ATM APS History Data managed entities will be deleted when the corresponding ATM APS End Point is deleted.

7.4.5. ATM APS History Data

This managed entity contains all the previous ATM APS Current Data for a specific ATM APS End Point instance that is produced as a result of forming ATM APS Current Data.

Measurement attributes in the History Data managed entity are an exact copy of the attributes in the corresponding Current Data managed entity at the end of the interval. The time at the end of the interval is indicated by the value of the attribute "Period End Time."

Instances of this managed entity are automatically created by the ATM NE upon instantiation of an ATM APS End Point instance. Instances of this managed entity are
deleted by the ATM NE upon deletion of an instance of the associated ATM APS End Point instance, or by request of the managing system.

Attributes

Managed Entity Id: This attribute provides a unique name for the managed entity instance in the ATM NE. (R, Set at Creation) (mandatory)

Period End Time: This attribute records the time at the end of the interval. (R) (mandatory)

Suspect Flag: This attribute indicates the reliability of the performance monitoring data collected by the managed entity. This attribute may take on one of two possible values: reliable and unreliable (suspect). (R) (optional)

Number Of Suppressed Intervals: This attribute is present only if the ATM NE is suppressing ATM APS History Data creation when the current interval terminates with "all-zeroes" performance measurements. (R) (optional)

Failure to Switch on SF/SD: This attribute provides a raw, thresholded count of the number of failure to switch after detection of SF/SD (R, S=D, D=0) (mandatory)

Failure to Switch after WTR expired: This attribute provides a raw, thresholded count of the number of failure to switch after the expiration of the Wait to Restore timer. (R, S=D, D=0) (mandatory)

Failure to Switch after Far-End Switch: This attribute provides a raw, thresholded count of the number of failure to switch at the near-end, after a switch at the far-end of the PD for a bi-directional protection entity. (R, S=D, D=0) (mandatory)

Failure to Switch after Near-End Switch: This attribute provides a raw, thresholded count of the number of failure to switch at the far-end, after a switch at the near-end of the PD for a bi-directional protection entity. (R, S=D, D=0) (mandatory)

Successful Switches: This attribute provides a raw, thresholded count of the number of successful protection switching events that has occurred at this end of the PD (near end) during this measurement interval. The *Successful Switches* shall be the sum of the number of switchovers from the working entity to the protection entity and the number of switchovers from the protection entity to the working entity (R, S=D, D=0) (mandatory)

Actions

No actions have been defined for this managed entity.

Notifications

No notifications have been defined for this managed entity.

Relationships

A new instance of this entity is created at the end of each 15-minute interval for each current data object. This managed entity will create a copy of the performance management attributes that are

present in the associated current data managed entity at the end of the 15-minute interval. At least thirty-two instances of this managed entity shall be supported for each current data managed entity.

7.5. ATM APS Managed Entity relationships

This document defines an information model that provides a formal representation of the information exchanged across the standard based (e.g., CMIP, CORBA or SNMP) interface used to manage the ATM APS.

7.5.1. Entity Relationship and Instance Diagrams

Figure 2, 3 and 4 illustrate the entity relationships among the managed entities that are relevant to ATM APS management. Figure 2 shows the relation between the ATM APS entities and the different termination points (VPLs, VCLs, VPCs and VCCs). Figure 3 shows the relations between the ATM APS entities and a cross-connected VPL or VCL. Figure 4 shows how the ATM APS Extra Traffic object is related to the different termination points.

To give a better view how these objects are related in a real scenario a number of instance diagrams have been added (figure 5, 6, 7 and 8):

- Figure 5 shows one end of a protected sub-network connection that in the concerned NE will show up as an ATM cross-connection protected at one side.

- Figure 6 shows an example with a protected VCL and extra traffic configured to the interface of the protection entity.

- Figure 7 illustrates the case where a group of VC connections (in this case VCLs) are protected by another group of similar connections at the protection interface. The figure also illustrates the two test trails that have been created for the APS coordination protocol and APS fault detection. One test trail has been created for the interface where the ‘working’ VCLs are located, another test trail has been created for the interface of the ‘protection’ VCLs. The VCLs at the working interface are in this example cross-connected to VCLs at a non-protected interface.

- Figure 8 shows one end of a protected VP trail, which will show up as a protected VPC termination point in the NE view. Note that in the Network view it may be possible to in one end of the PD have a protected VPC end point and in the other end a protected VPL which will be the combination of the two cases illustrated in Figure 5 and Figure 8.

- The figure 8 also illustrates how a VCL may be created in the ‘Working VPC Termination Point’ of the protected VP trail. This VCL will automatically be protected, using the same VCI at the Protection VPC Termination Point. In the ‘Protection VPC Termination Point’ only VCLs that are intended for extra traffic may be created (in case of 1:1 protection).

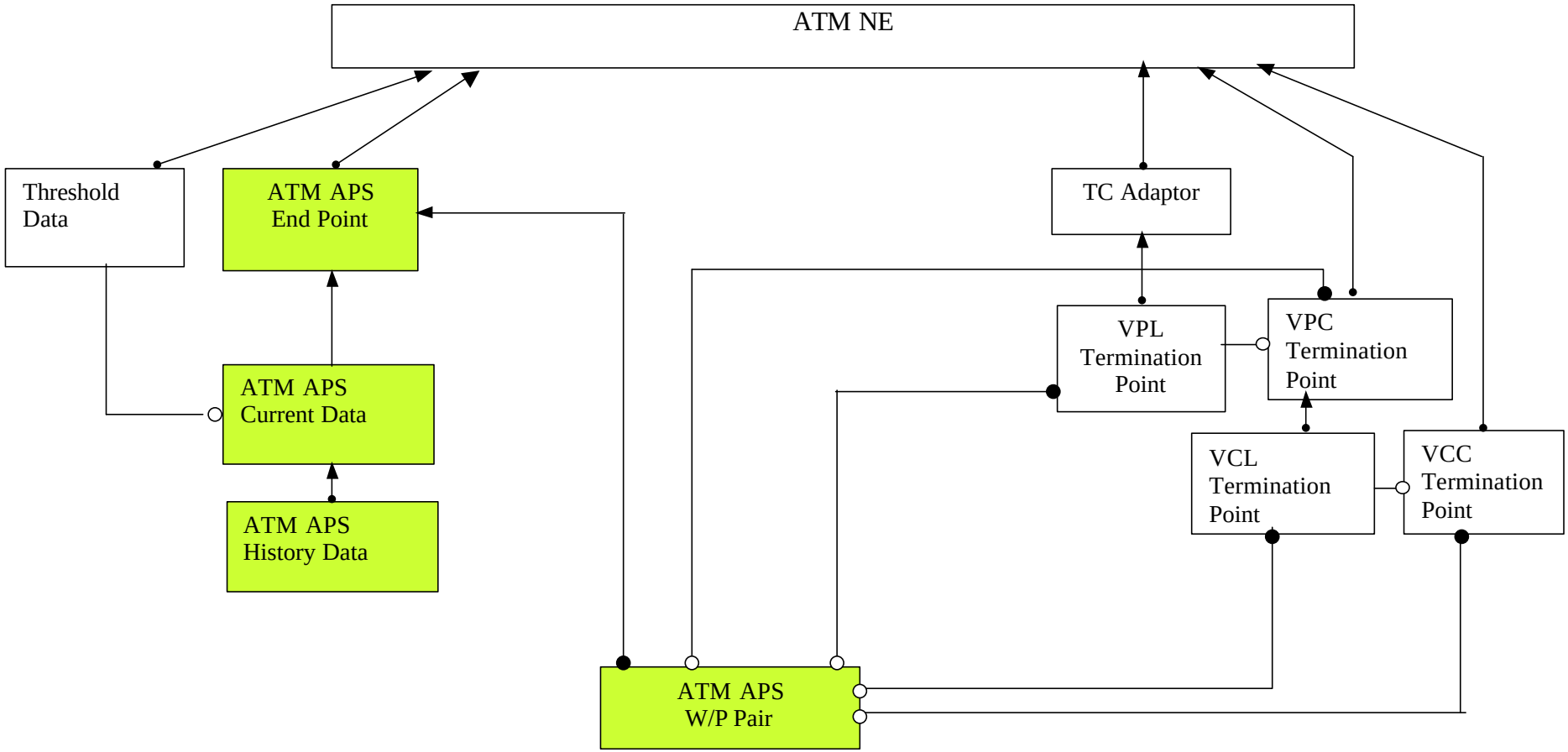
7.5.2. Inter-working of the ATM Cross Connect Objects and the ATM APS Objects

As illustrated in figures 3, 5, 6 and 7 below, the ATM Cross Connection (according to [9]) will also in the ATM protection case be related to two VPLs or VCLs as for a ‘normal’ non-protected connection.

In the protected case the ATM Cross Connection will always be connected between the ‘Working entity’ (VCL or VPL) of the protected side and the ‘normal’ VCL or VPL at the non-protected side. An example of this is given in figure 5, which shows an instance diagram with a protected cross-connected VP connection.

The described object relationships imply that protecting a non-protected ATM Cross-Connect will be accomplished by:

- Creating a new VCL or VPL (protection entity) for the protected side of the cross connect,
- Creating an ATM APS End Point,
- Creating an ATM APS Working Protection Pair object to associate the working and the protection entities with each other at the protected end of the cross-connect.



Legend:

: Managed Entity from af-nm-0020.001[9]

: Managed Entity for APS

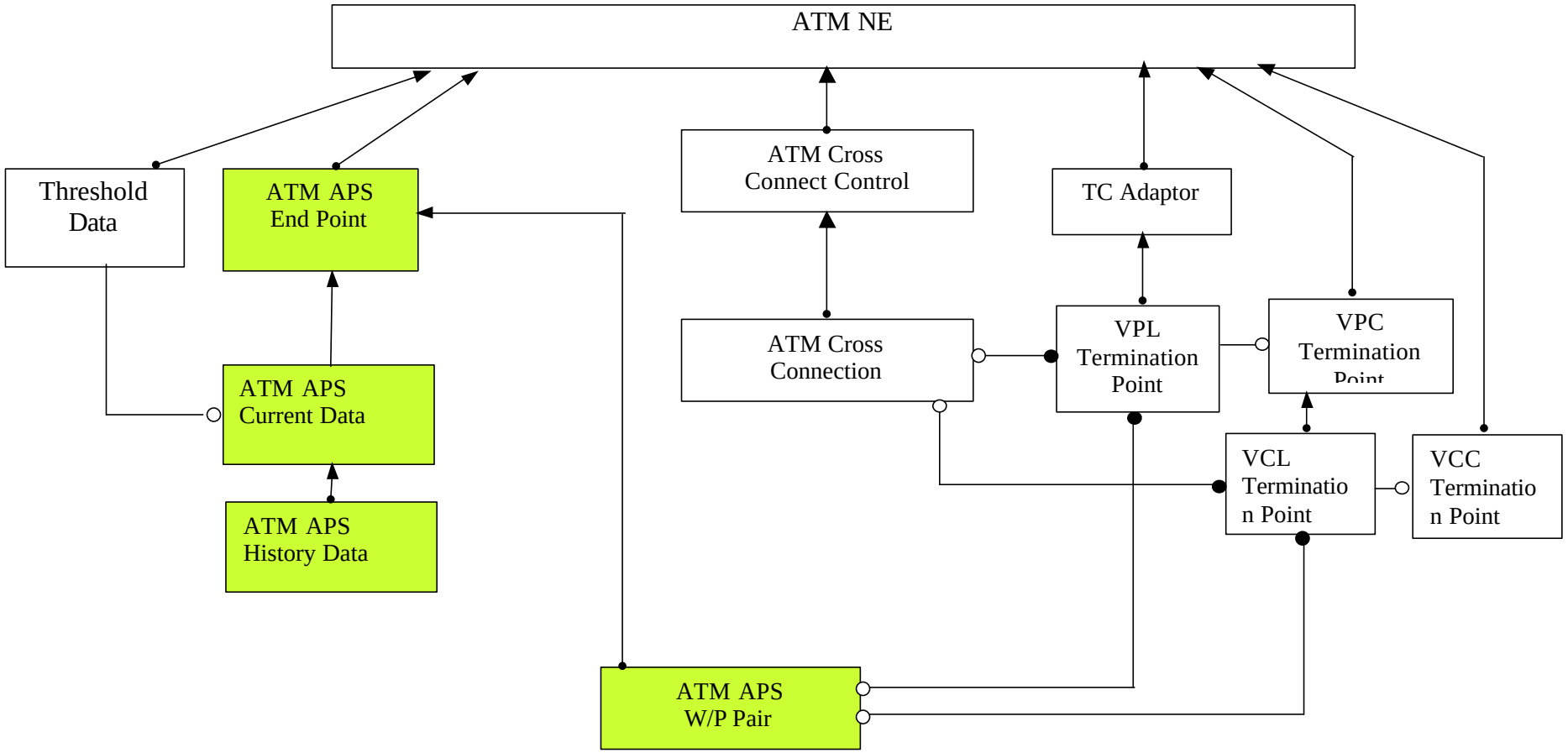
: Zero or More

: Zero or One

: Association

A ← B : A Contains B

Fig 2: Entity Relationship diagram APS – ATM Termination Point view



Legend:

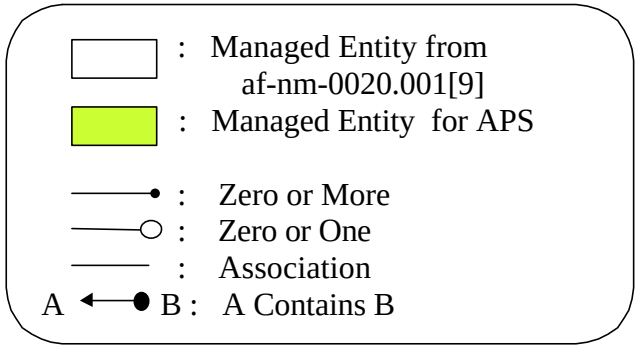
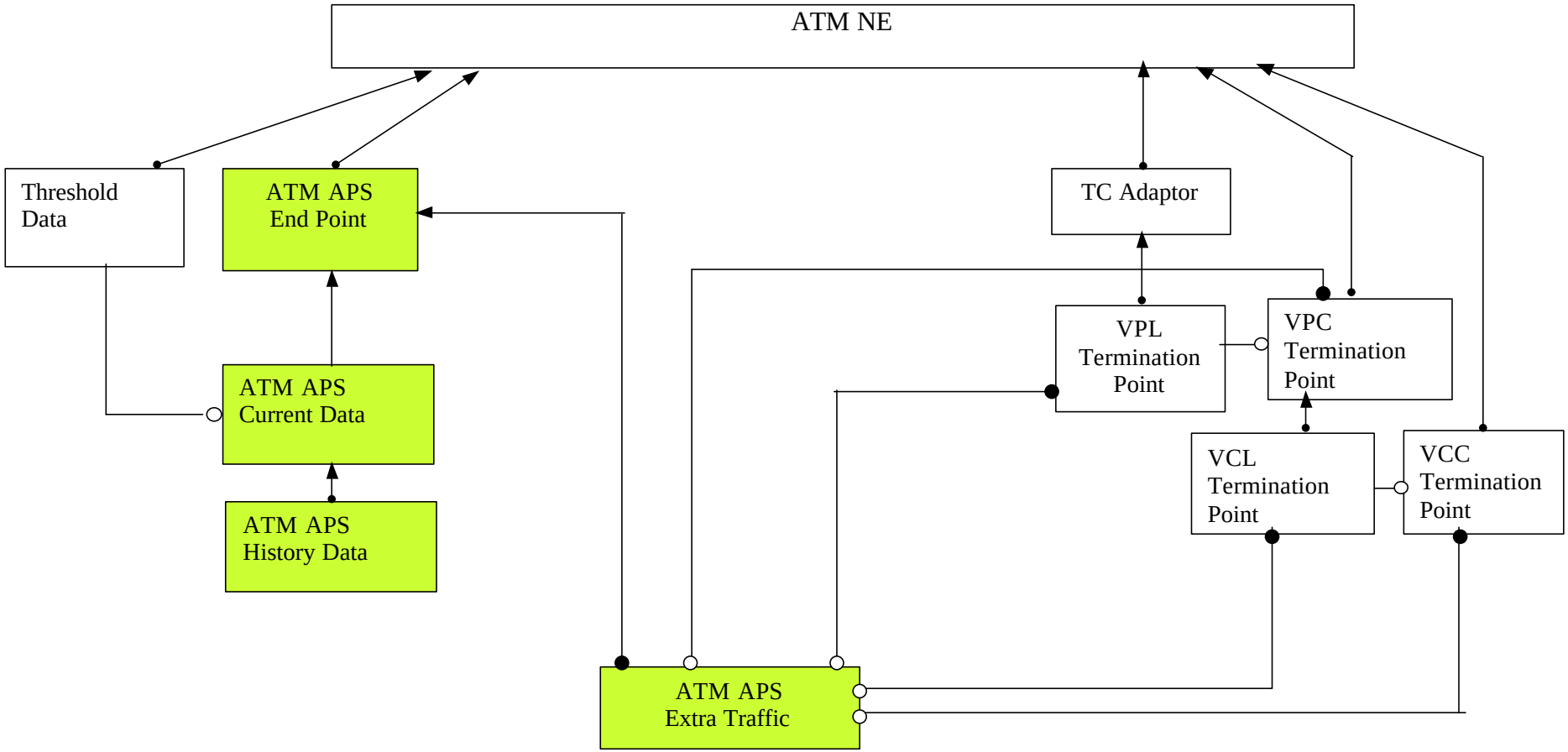


Fig 3: Entity Relationship diagram APS – ATM Cross Connection view



Legend:

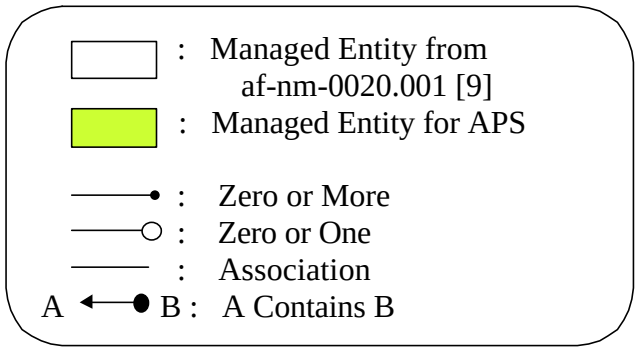
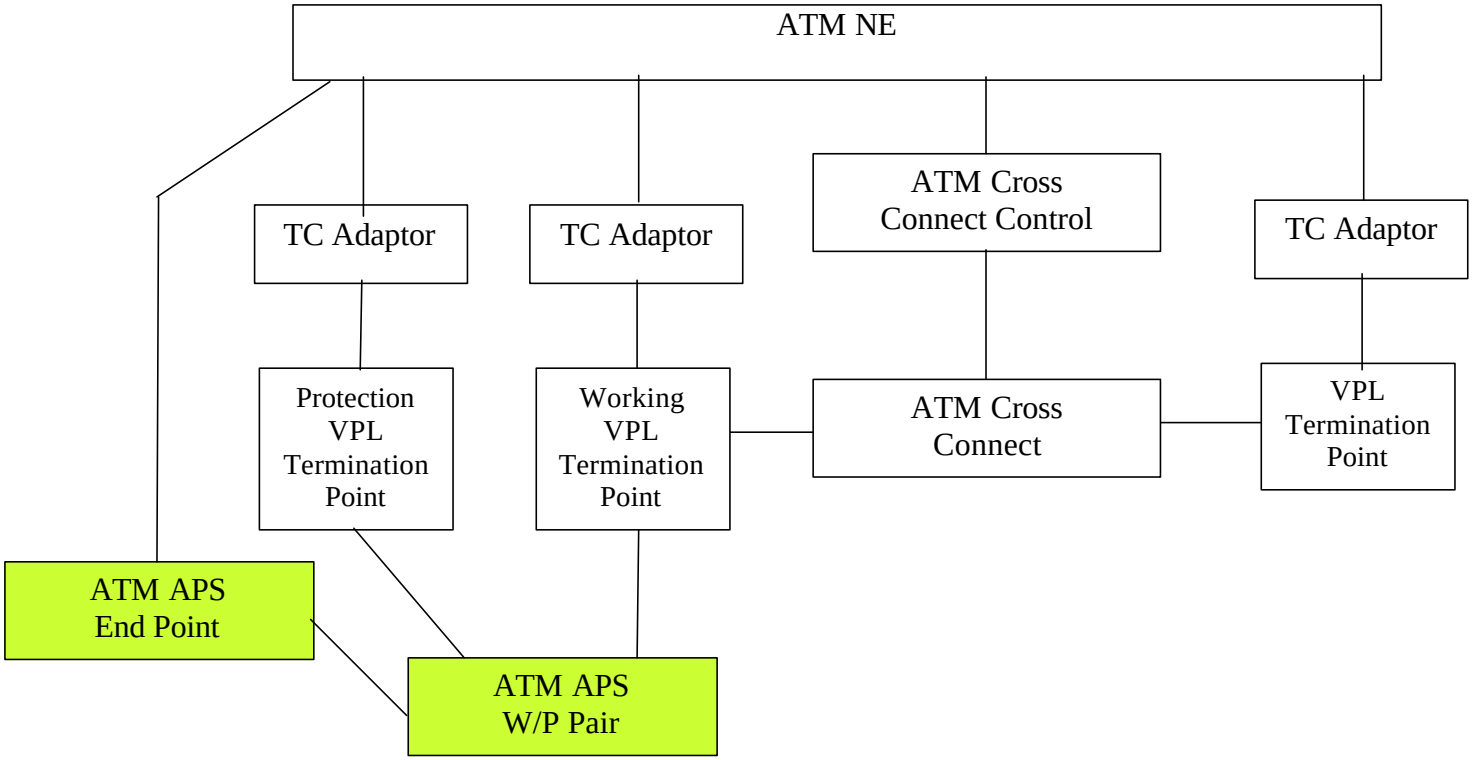


Fig 4: Entity Relationship diagram APS End Point with Extra Traffic



Legend:

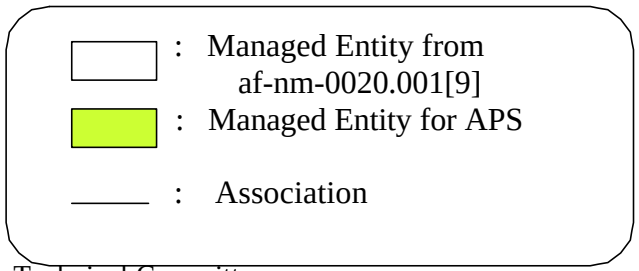


Fig 5: Example – Instance diagram,
Protected Sub-network Connection
(Protected VPL :one end of VP cross-connect)

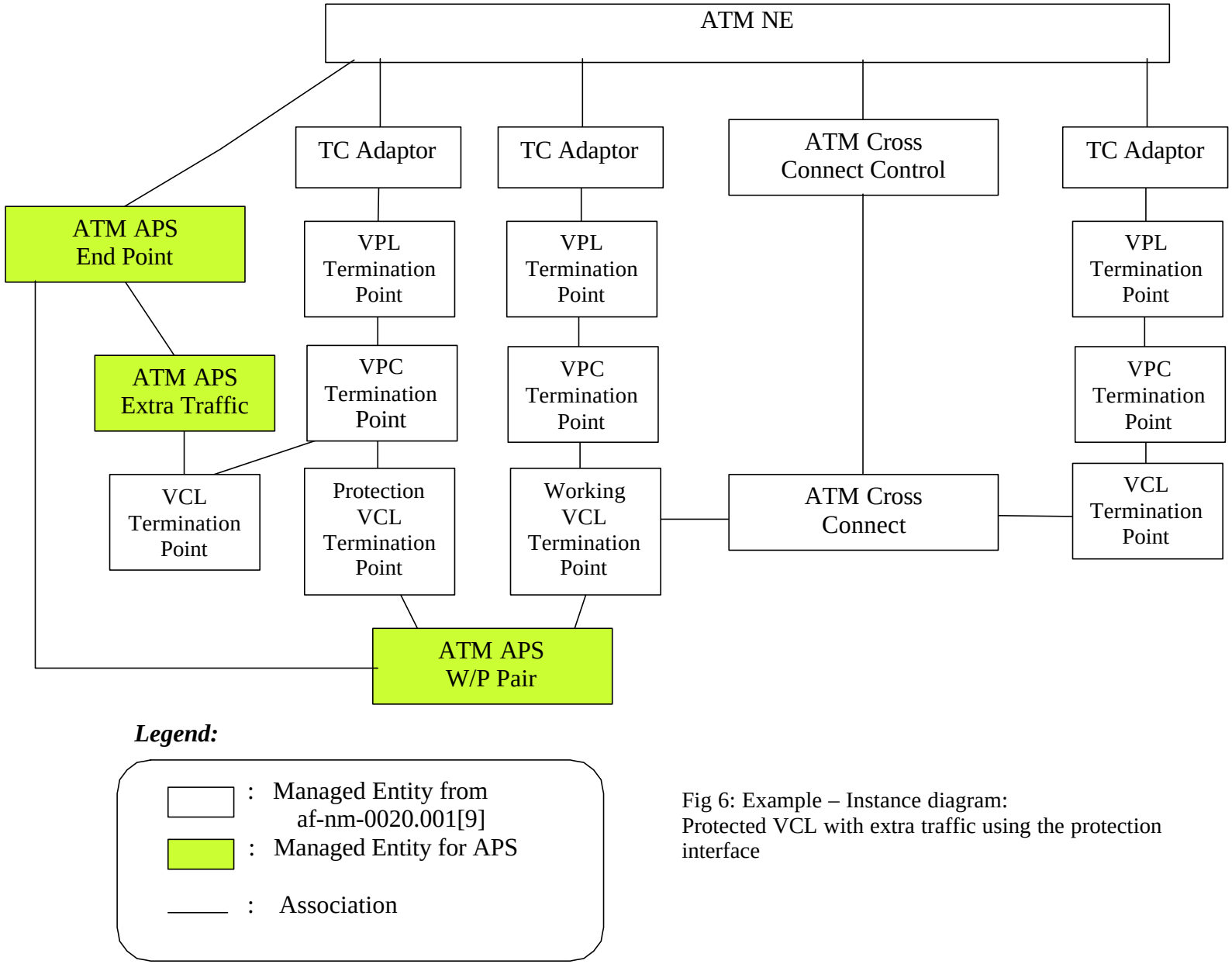
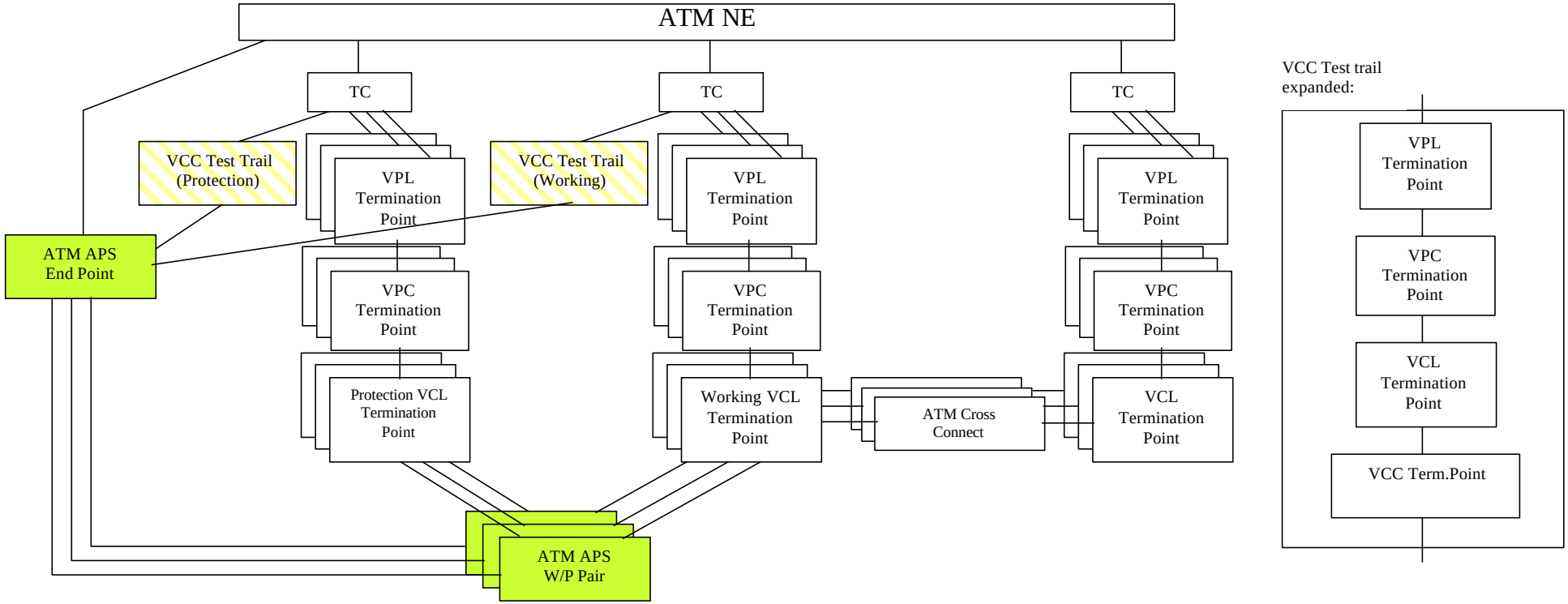


Fig 6: Example – Instance diagram:
Protected VCL with extra traffic using the protection interface



Legend:

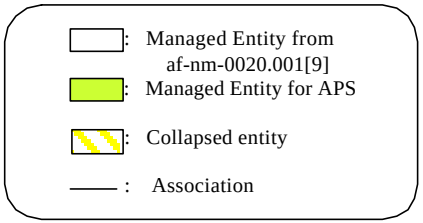
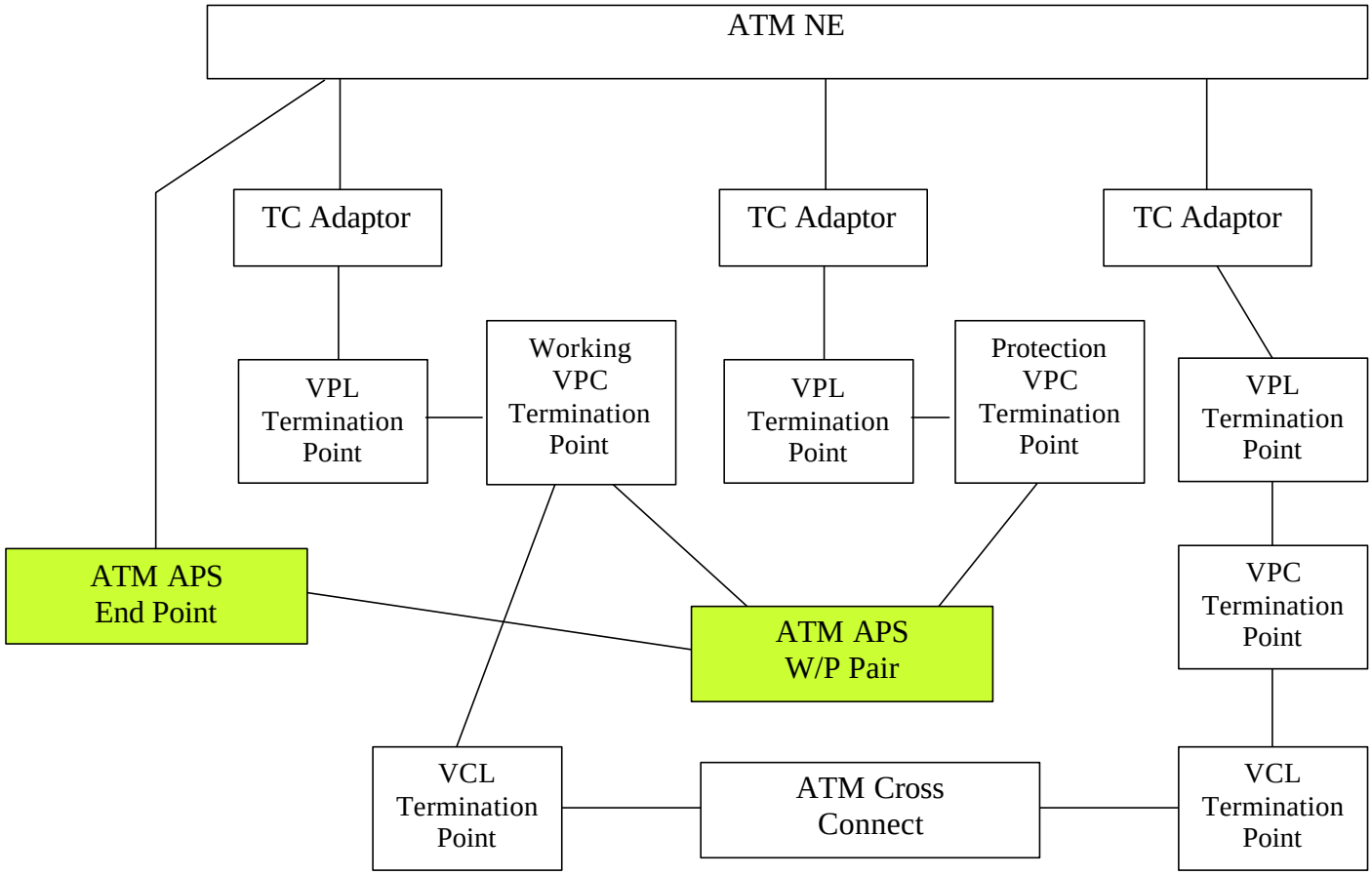


Fig 7: Example – Instance diagram:
Group protection of VCG type
Note: In the figure all protected VCLs are related to different VPC Term. Points. This is of course not a necessary condition. Several VCLs may instead belong to one VPC Term. Point. The VCLs at the non-protected side of the ATM cross-connects may also be located at different interfaces (TCs).



Legend:

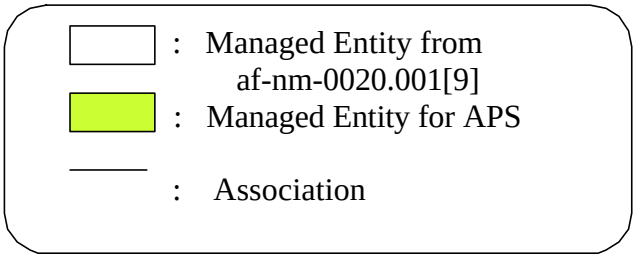


Fig 8: Example – Instance diagram, Protected VP trail (Protected VPC termination point) carrying a VCL of a ATM VC cross connection.

Note: The *ATM Cross Connect* has a relation to the *ATM Cross Connect Control* managed entity, but this is not shown in the figure.

8. References

ITU-T Recommendations

[1] ITU-T Recommendation I.630 : ATM Protection Switching, February 1999.

[2] ITU-T Recommendation I.610 : B-ISDN operation and maintenance principles and functions, February 1999.

[3] ITU-T Recommendation M.3100 : Generic Network Information Model, July 1995.

[4] ITU-T Recommendation X.731 : Open Systems Interconnection – Systems Management: State Management Function, January 1992.

[5] ITU-T Recommendation X.732 : Open Systems Interconnection – Systems Management: Attributes for Representing Relationships, January 1992.

[6] ITU Recommendation I.371 : Traffic control and congestion control in B-ISDN, August 1996.

ATM Forum Specifications

[8] af-cs-0141.000 : PNNI Addendum for Path and Connection Trace Version 1.0, July 2000.

[9] af-nm-0020.001 : M4 Interface Requirements and Logical MIB: ATM Network Element View, October 1998.

[10] af-tm-0121.000 : Traffic Management Specification Version 4.1, March 1999.

[11] af-nm-0184.000 : ATM APS SNMP MIB, March 2002

Telcordia Specifications

[12] GR-2980-CORE : Generic Criteria for ATM Layer Protection Switching Mechanism, Issue 2, December 1998.

[13] GR-1093-CORE : Generic State Requirements for Network Element, Issue 1, October 1994, Revision 1, December 1995.

Appendix A - State Transitions Tables for ATM APS Working and Protection Entities

Table A-1 shows the state transitions for ATM APS working and protection entities using the ISO State Model [3, 4].

Events /Commands	Working Entity				Protection Entity		
	operationalState = enabled			operationalState = disabled	operationalState = enabled		operationalState = disabled
	providingService	hotStandby		failed	providingService	hotStandby	failed
		WTR timer running	WTR timer not running				
Clear[1]	providingService	hotStandby (Stop WTR timer)	hotStandby	failed	providingService	hotStandby	failed
Freeze[2]	providingService	hotStandby (Stop WTR timer)	hotStandby	failed	providingService	hotStandby	failed
LoP[3]	providingService	providingService (Stop WTR timer)	providingService	failed	hotStandby	hotStandby	failed
SF-P[14]	providingService	providingService[13] (Stop WTR timer)	providingService[13]	failed	failed[13]	failed	failed
FS-W[14]	hotStandby[4]	hotStandby (Stop WTR timer)	hotStandby	failed	providingService	providingService[4]	failed
SF-W	failed[5]	failed	failed	failed	providingService	providingService[5]	failed
SD-P[12]	For further study	For further study	For further study	For further study	For further study	For further study	For further study
SD-W[12]	For further study	For further study	For further study	For further study	For further study	For further study	For further study
MS-P	providingService	providingService[9] (Stop WTR timer)	providingService[9]	failed	hotStandby[9]	hotStandby	failed
MS-W	hotStandby[6]	hotStandby (Stop WTR timer)	hotStandby	failed	providingService	providingService[6]	failed
Recovery-W	NA	NA	NA	hotStandby (Start WTR timer[7]) or providingService[10]	providingService	NA	failed
WTR Timer Expires	NA	providingService[8]	NA	NA	hotStandby[8]	NA	NA
Do Not Revert	NA	hotStandby (Stop WTR timer)	hotStandby	NA	providingService	NA	NA
No Request	providingService	hotStandby	hotStandby	failed	providingService	hotStandby	failed
Recovery-P	providingService	NA	NA	NA	NA	NA	hotStandby or protvidingService[11]

[1] An internally maintained Freeze flag (FZ) shall be set to FALSE(F), i.e., FZ=F. Similarly, All flags related to the APS entity LoP (Lockout of Protection), FS-W, MS-P, MS-W are set to FALSE if the Clear command does not specify a command type; or a specific flag is set to FALSE if a command type is specified.

[2] The Freeze flag (FZ) is set to TRUE(T) - all external commands except Clear are ignored if FZ=T. When FZ=T, current position of bridge/selector are maintained, and current K1/K2 values are maintained and transmitted.

[3] When LoP is detected the working entity shall take over the traffic from the protection entity when possible.

[4] If LoP=F, FZ=F, SF-P=F this transition will be performed.

[5] If FZ=F and LoP=F and SF-P=F, this transition will be performed after waiting a time period specified by the hold-off timer.

[6] If LoP=F, FZ=F, MS-P=F, SF-P=F this transition will be performed.

[7] If FS-W=F, SF-W=F, MS-W=F, 'Do Not Revert'=F (revertive mode), the WTR timer will be started, otherwise the state will only be changed to hotStandby.

[8] If 'Do Not Revert'=F (revertive mode), this transition will proceed

[9] If FZ=F, FS-W=F, SF-W=F this transition will be performed.

[10] If the protection entity is failed the working entity will go directly to state providingService.

[11] If the working entity is failed the protection entity will go directly to state providingService.

[12] Trigger on Signal Degrade is for further study according to [1].

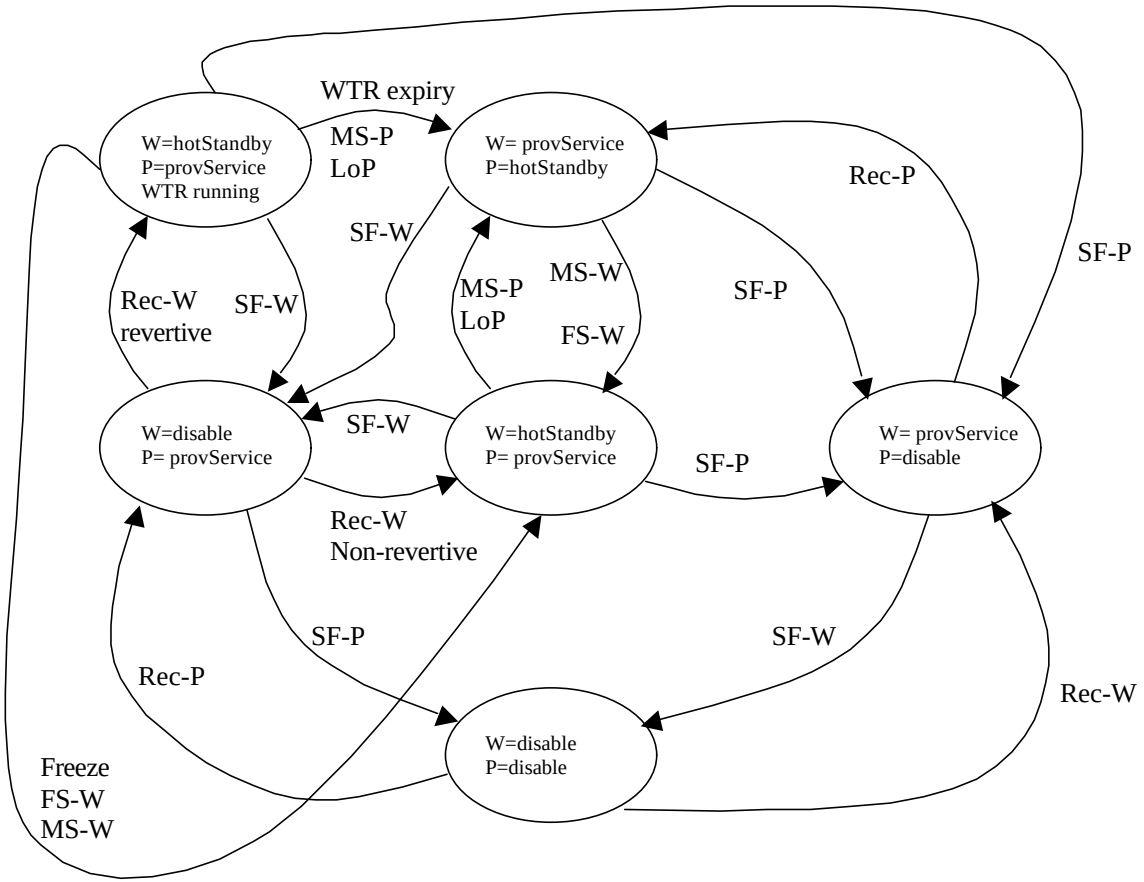
[13] This transition will be performed after waiting a time period specified by the hold-off timer.

[14] As noted in requirement (R-3.6.2)-2 the 'Forced switch for working' and 'Signal Fail for protection' have different priority order depending on if the protection switching is uni-directional (not using the APS coordination protocol) or bi-directional.

Note: Treatment of the events and commands described in the table and footnotes above are according to the priority order defined in [1]. The items in the table above are sorted according to this priority order from highest priority at the top to the lowest priority at the bottom. If several events are received at the same time only the one with the highest priority will affect the state changes. The table is intended to give a possible (but not the only) interpretation of how to implement state transitions for the ATM APS states described in [1].

Note: Using the 'Freeze' manual request will prevent any state transitions for the ATM APS End Point when new requests/events of lower priority are experienced.

Table A-1. State Transitions at Protection Domain Endpoints supporting the Working and the Protection Entity – using ISO State Model.



State diagram A-2. The diagram shows the allowed state combinations and examples of transition signals for the working and protection entity.

Note: The state transitions indicated above are dependent on the priority order of the APS events/commands received in a particular state. A higher priority command may thus force (or prevent) a certain state transition. The ‘Freeze’ manual request will for example prevent any state transitions when lower priority requests/events are experienced.

Appendix B – Requirements Mappings

Requirement	ITU Rec. I.630 section
(R-3.1)-1	5.1.2(1)
(R-3.1)-2	7.2.1, 7.2.2, 5.1.2(8)
(R-3.1)-3	5.1.2(8)
(O-3.1)-1	5.4
(R-3.1)-4	5.1.2(8)
(R-3.2)-1	5.1.2(9)
(R-3.2)-2	5, 7.2.3, A.1.1.1
(R-3.2)-3	5, A.1.1.1
(R-3.2)-4	5.1.2(9)
(R-3.2)-5	NA
(R-3.3)-1	5.1.1(1)
(R-3.3)-2	5.1.2(15)
(R-3.4)-1	5.2, 5.3, 5.1.2(2)
(R-3.4)-2	5.1.1(4), 5.3.4
(R-3.5)-1	A.2.1.2, B.3.2
(R-3.6)-1	5.1.2(13), 6.2.2
(R-3.6)-2	5.1.2(2), 6.2.2
(R-3.6)-3	6.2.2
(R-3.6)-4	7.3.2, A.1.1
(R-3.6)-5	5.1.2(4), 5.1.2(6), 6.2, 6.2.1, 6.2.2, A.2.1, B.3
(R-3.6)-6	A.2, A.2.3
(R-3.6.1)-1	5.7, 5.1.1(3), 5.1.2(12), 5.1.2(18)
(R-3.6.1)-2	5.7, 5.1.2(12), 5.1.2(18)
(R-3.6.1)-3	5.7, 5.1.2(12), 5.1.2(18)
(R-3.6.2)-1	A.2.1, A.2.1.1, B.3, B.3.1
(R-3.6.2)-2	5.1.2(6), Table A.1, Table B.1
(R-3.6.3)-1	7.2.1, 7.2.2, 7.2.3
(R-3.6.3)-2	7.2.1, 7.2.2, 7.2.3
(R-3.6.3)-3	NA
(R-3.6.4)-1	5.8, A
(R-3.6.4)-2	5.8, A
(R-3.6.4)-3	5.8
(R-3.6.4)-4	A.2.2, A.2.3.4
(R-3.6.4)-5	A.2.2, A.2.3.4
(R-3.6.4)-6	5.8, A.2.2
(R-3.6.4)-7	A.2.2
(R-3.6.4)-8	A.2.3.1, A.2.3.4

(R-3.6.4)-9	A.2.3.4, 5.1.2(19)
(O-3.7)-1	A.2.3.3, 5.1.2(16)
(O-3.7)-2	A.2.3.3, 5.1.2(16)
(R-3.7)-1	NA
(R-3.7)-2	A.2.3.2
(R-3.7)-3	A.2.1.3
(R-3.7)-4	B.3.3, A.2.1.3
(R-3.8)-1	A.1.1.2, 5.1.2(10)
(R-3.8)-2	A.1.1.2
(R-3.8)-3	A.1.1.2, 5.1.2(10)
(R-4.1)-cm-1	5.1.2(9), 5.1.2(16)
(R-4.1)-cm-2	5.7, 5.1.2(18)
(R-4.1)-cm-3	B.3.3, A.2.1.3
(R-4.1)-cm-4	6.2.2
(O-4.1)-cm-1	6.2
(R-4.1)-cm-5	NA
(R-4.1)-cm-6	NA
(R-4.1)-cm-7	5.1.2(16)
(R-4.1)-cm-8	5.1.2(9)
(R-4.1)-cm-9	5.1.2(9)
(R-4.2)-cm-1	5.1.1(1), 5.1.2(9), 5.1.2(16),7
(O-4.2)-cm-1	6.2
(R-4.2)-cm-2	7
(R-4.2)-cm-3	7
(R-4.2)-cm-4	7
(R-4.2)-cm-5	7
(R-4.2)-cm-6	7
(R-4.2)-cm-7	7
(R-4.2)-cm-8	5.1.2(16)
(R-4.2)-cm-9	5.1.2(9)
(R-4.2)-cm-10	5.1.2(9)
(R-4.3)-cm-1	Table A.1, Table B.1
(R-4.3)-cm-2	A.2.1, A.2.1.1, B.3, B.3.1, 5.1.2(17)
(O-4.3)-cm-2	A.2.2
(R-4.3)-cm-3	NA
(R-4.3)-cm-4	NA
(O-4.3)-cm-3	5.1.2(10)
(CR-4.3)-cm-1	NA
(CR-4.3)-cm-2	A.1.1.2
(R-5)-fm-1	A.2.3.1
(R-5)-fm-2	A.2.3.1
(R-6)-pm-1	NA
(R-6)-pm-2	NA
(R-6)-pm-3	NA