Alcatel·Lucent

AnyMedia® Access System

Applications and Planning Guide

IP-based services

Releases up to R1.38.1 and R3.6

363-211-587
CC109562769
Issue 10
September 2008

Notice

Every effort has been made to ensure that the information contained in this information product was accurate at the time of printing. However, information is subject to change.

Ordering information

See "How to order" (p. xiv).

Technical support

Technical support is available for *AnyMedia* Access System indoor/outdoor applications, for *AnyMedia* LAG System, and for *AnyMedia* Element Manager (*Navis AnyMedia* Element Manager).

AnyMedia service is complemented by a full range of services available to support planning, maintaining and operating your system. Applications testing, network integration, and upgrade conversion support is available.

Alcatel-Lucent service personnel will troubleshoot field problems 24 h a day over the phone and on site (if necessary) based on Alcatel-Lucent service contracts by Local/Regional Customer Support (LCS/RCS) and by Remote Technical Support (RTS).

Contacting your Alcatel-Lucent support: For Europe call the International Customer Management Center (ICMC): +353 1692 4579 or call the toll free number: 00 800 00 58 2368. For Asia Pacific, Caribbean and Latin America Region, Saudi Arabia, Middle East and Africa call the local Alcatel-Lucent Customer Technical Support Team. For north and south America (NAR and CALA) call the Customer Technical Assistance Management (CTAM): +1 866 Lucent8 (prompt#1) or +1 630 224 4672 from outside the United States.

Contents

2 Physical interfaces

3 OAM&P for IP-based services

Configuration management

IP fault management

About this information product

Purpose

This Applications and Planning Guide (APOG) applies to the international version and to the NAR version of the *AnyMedia*® Access System. It enhances the traditional APOGs with information about IP-based services.

Note that not all features described here, are supported by both system versions.

The APOG for the international version of the *AnyMedia*® Access System consists of three parts which are closely related to each other. They are *not* considered to be independent information products. For the titles of the three APOGs, see table below:

APOG titles for international regions	**CIC Ordering Number**
Applications and Planning Guide (APOG), *Overview*	363-211-585
Applications and Planning Guide (APOG), *Narrowband and ATM xDSL services*	363-211-586
Applications and Planning Guide (APOG), *IP-based services*	363-211-587
Note that the two APOG parts *Overview* and *Narrowband and ATM xDSL services* replace the former combined APOG with the ordering number 363-211-110.	

The APOG for the NAR version of the *AnyMedia*® Access System consists of two parts which are closely related to each other. They are *not* considered to be independent information products. The conventional APOG (363-211-101) has now been enhanced with a second part, “Application and Planning Guide for IP-based services”. For the titles of the two APOGs, see table below:

APOG titles for North America regions (NAR)	**CIC Ordering Number**
Applications and Planning Guide (APOG)	363-211-101
Applications and Planning Guide (APOG), *IP-based services*	363-211-587

The APOG part *IP-based services* focuses totally on the IP-based services in the *AnyMedia*® Access System. The following information is provided in this information product:

- An overview about IP-services
- A description of IP-related physical interfaces
- Operations, administration and performance management (OAM&P) for IP-based services
- System planning and engineering for IP-based services.

Reason for reissue

This is the first issue of this document. Information that is added, deleted, or changed in future releases will be summarized in this notice.

History

Issue	Date	Feature
8	July 07	Support of additional IP-AFM Layer 2 Features: • DHCP Option 82 • Enhanced VLAN stacking
7	March 07	• Access node aggregation for Alcatel-Lucent or other vendor V5 access nodes • Call statistics for H.284 (Megaco) protocol • Support of multiple H.248 backup media gateway controllers • Support of direct dialing in for MGCP • Support of ICAP faceplate Fast Ethernet uplink in controlled mode • Source IP policy routing • PayPhone support • Termination ID parameter structure for H.248 VoIP ports • Call traffic statistics for H.248 (Megaco) protocols • Pack audit and alarming within H.248 (Megaco) protocol • Configurable autonomous secondary dial tone (SDT) • Multiple IP addresses within the ICAP
6	November 06	• LPA633 in LAG200 • Support of additional features on ICAP and VoIP APs: – Media monitoring – Voice activity detection per port – Echo cancelation per port – Loopbacks per feeder • New VoIP AP LPZ602 (at the issue date of this document only supported for NAR markets) • LPA633 in stand-alone mode • ICAP in stand-alone mode • LPZ600 in stand-alone mode

Issue	Date	Feature
5	August 06	• New IP ADSL2+ 32 port AP, Annex A application pack IPADSL2_32p AP LPA633 in controlled and stand-alone mode • Remote Access to COMDAC via IP-AFM Inband Management Channel.
4	April 06	• Support of new IP pack IP COMDAC AP (ICAP) • Support of new IP pack IP-AFM • Migrating existing *AnyMedia*® Access Systems towards IP networks by aggregation of remote terminals via ICAPs • Support of several IP APs in stand-alone mode
3	January 06	• Support of LAG 200 Shelf (used in international regions) • Support of LAG 2300 Shelf (used in NAR) • ESIM as controller in LAG 200 Shelf • Support of IPFMs with extended memory • Support of new IP packs (IP-AFM, ICAP, IPADSL2_32p AP)
2	June 05	• Support of VDSL service • Quality of service • IP loopbacks • DHCP relay • Manual call restriction control • Improved software download capabilities for VoIP
1	February 05	first edition

Intended audience

Customers who use this APOG include the following:

- Standardization groups
- Product evaluators
- Network planners
- Engineers.

Conventions used

The following conventions are used throughout the *Applications and Planning Guide, IP-based services.*

Acronyms and abbreviations

In the text acronyms are expanded the first time they are used in the main text of a chapter (for example Fast Ethernet (FE)). If the acronym is a trademark, it will not be spelled out. A list of acronyms is provided at the end of this document.

Terms used (alphabetically ordered)

The following are terms used in this information product (IP) that may have a different meaning than the general or common use of the term.

- *a/b-cables* refer generically to the tip/ring pair cables that attach to the faceplate of application packs (APs).
- In the *AnyMedia*® Access System, the term *access* means that the system provides the primary service interface for the subscriber to enter the network.
- The term *AnyMedia LAG Shelf* is generally used for an *AnyMedia* shelf with IP spokes on the backplane, independently of the physical design of the shelf.
  In contrast to an *AnyMedia*® ETSI V5 Shelf or *FAST* Shelf the *AnyMedia LAG Shelves* are capable to support IP-based services also in controlled mode.
- The term *AnyMedia shelves* is used whenever the text does not need to distinguish between the shelf types. It is mostly used where services and service packs are described.
- The term *controlled mode* is generally used for a mode, in which the inter-worked traffic is handled by IP spokes on the shelf backplane which connect the pack to the IP controller. Therefore this mode requires the usage of a LAG Shelf equipped with an IP controller. The uplinks on the faceplates of the APs are not usable in this mode.
  Note that the IPFM controlled mode is supported in the LAG Shelves only.
- The term *stand-alone mode* is generally used for a mode, in which the inter-worked traffic is handled by the uplinks on the faceplate of the individual AP without using neither IP spokes on the backplane nor an IP controller. This mode is supported in all shelf types, but it is not supported by each IP AP type.
  A combination of APs in stand-alone mode and of APs in controlled mode is also allowed within one shelf. But note that every stand-alone pack is a separate NE from the management perspective, that means it reduces the NAM capacity in terms of managed shelves correspondingly.
- The term *IP controller* is a general term for an IP forwarding module (IPFM) or an ESIM that is used not as an AP but as an IP controller in a LAG 200 Shelf.

Trademarks

Trademarks of Alcatel-Lucent and other companies are in italics. They are identified with the registered mark (®) or trademark (™) symbol the first time the trademarks are used in the text (for example Alcatel-Lucent *AnyMedia*® Access System).

Related documentation for the international regions

The following is orderable documentation related to the *AnyMedia*® Access System and for additional components, especially for international regions. For the ordering address see “How to order” (p. xiv). Additionally, these information products are accessible from the Alcatel-Lucent internal web page:
http://access.de.lucent.com/ACCESS/cdoc/index.html

Manual Type	Comcode	CIC Ordering Number ([1])
Applications and Planning Guide (APOG), Overview	109 562 744	363-211-585
Applications and Planning Guide (APOG), Narrowband and ATM xDSL services	109 562 751	363-211-586
Applications and Planning Guide (APOG), IP-based services	109 562 769	363-211-587
Data Sheet Book	109 218 651	363-211-251
Ordering Guide	109 097 782	363-211-144
Commands and Procedures for Narrowband Services with TDM COMDAC	109 105 635	363-211-119
Commands and Procedures for ATM xDSL Services	109 024 737	363-211-133
Commands and Procedures for IP-based Services	109 562 736	363-211-555
Installation Manual for DC-Powered Racks for ETSI V5 and LAG 1900 Shelves	109 576 140	363-211-603 ([2])
Installation Manual for the Mainshelf and DC-powered racks	109 024 752	363-211-207 ([3])
Installation Manual for AC-powered racks	109 024 745	363-211-206
AnyMedia® LAG 4300 System, Installation Manual (IM)	109 461 939	363-211-256
Customer Documentation on CD-ROM	108 298 787	363-211-114

Notes:

1. For the ordering address see “How to order” (p. xiv).
2. Applicable for the new DC-powered racks based on CABI600 mechanics (J1C293B-1 L1 and J1C301B-1 L1)
3. Applicable for the established DC-powered racks J1C283B-1 L2 and J1C293A-1 L2.

Print copy (hard copy)

All listed documents are available in print and on CD-ROM.

Related documentation for the North America regions

The following is orderable documentation related to the *AnyMedia*® Access System and for additional components, especially for NAR. For the ordering address see “How to order” (p. xiv). Additionally, these information products are accessible from the Alcatel-Lucent’ internal web page:
http://access.de.lucent.com/ACCESS/cdoc/index.html

Manual Type	Comcode	CIC Ordering Number ([1])
Applications and Planning Guide (APOG)	108 298 639	363-211-101
Applications and Planning Guide (APOG), IP-based services	109 562 769	363-211-587

Manual Type	Comcode	CIC Ordering Number ([1])
AnyMedia® Access System Feature Supplement, Integrated Access Terminal (IAT)	N/A	363-211-127
AnyMedia® Access System Feature Supplement, MDS2 Shelf Configuration	108 864 521	363-211-106
AnyMedia® Access System Feature Supplement, Central Office Terminal	N/A	363-211-128
Ordering Guide	N/A	363-211-125
Commands and Procedures ([2])	N/A	363-211-100
Commands and Procedures for IP-based Services	109 562 736	363-211-555
Installation Manual	108 298 654	363-211-102
Engineering Guidelines	N/A	363-211-178
Data Sheet Book	N/A	363-211-254
AnyMedia® Access System Floor Plan Data Sheets	N/A	FPD 801-450-111-1
Customer Documentation on CD-ROM	108 361 155	363-211-104

Notes:

1. For the ordering address see "How to order" (p. xiv).
2. Available on CD-ROM only.

Print copy (hard copy)

If nor market otherwise, all listed documents are available in print and on CD-ROM.

How to order

These documents and drawings can be ordered at or downloaded from the Alcatel-Lucent Online Customer Support Site (OLCS) (https://support.lucent.com) or through your Local Customer Support.

How to comment

To comment on this information product, go to the Online Comment Form (http://www.lucent-info.com/comments/enus/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

Because customer satisfaction is extremely important to Alcatel-Lucent, every attempt is made to encourage feedback from customers about our information products.

1 IP-based services

Overview

Purpose

Alcatel-Lucent *AnyMedia*® Access System offers various applications to meet the telecommunications providers' needs. This chapter gives an overview of the IP-based services supported by the *AnyMedia*® Access System.

A subset of the IP-based services can be provided in two modes in the *AnyMedia*® Access System:

- Controlled mode
- Stand-alone mode

Contents

IP-based services – Overview

Supported services

The *AnyMedia*® Access System supports all IP-based services for triple play per priority:

- Voice over IP (VoIP) - supported by the VoIP APs LPZ600/LPZ602 and ICAP LPI600
- VDSL - supported by the VDSL AP or VSIM LPV417
- Fast Ethernet - supported by the ESIM LPE408
- ADSL2+ - supported by the IPADSL2_32p AP LPA633
- Traditional xDSL services - supported by the IP-AFM LPI960.

System architecture – Overview

The system architecture in IP subsystems depends on whether an IPFM will be used in the shelf (controlled mode) which is only possible in LAG Shelves, or whether an ESIM is used as controller which is possible in a LAG 200 Shelf only, or whether IP APs are used in stand-alone mode in any *AnyMedia* Shelf. Note that not all IP APs are capable to work in stand-alone mode.

IP subsystems in controlled mode (IPFM controlled)

This mode requires an IPFM as IP controller in the same LAG shelf (note that in a LAG 200 Shelf the IP controller will be an ESIM). In controlled mode, the IPFM aggregates the user traffic from all IP APs (via the backplane spokes) into its uplinks and serves as the interface into the network. IP APs do not make any use of their faceplate uplink in the controlled mode.

From the IPFM point of view no pre-provisioning and no system view other than the actual pack type and alarm logging is supported.

Each IP AP has its own service IP address but no OAM&P address. In IPFM controlled mode all management traffic is handled by the IPFM. Provisioning data is stored on the IPFM when a *Save to NVDS* is done. Program images, auxiliary files and database are stored non-volatile on the IPFM.

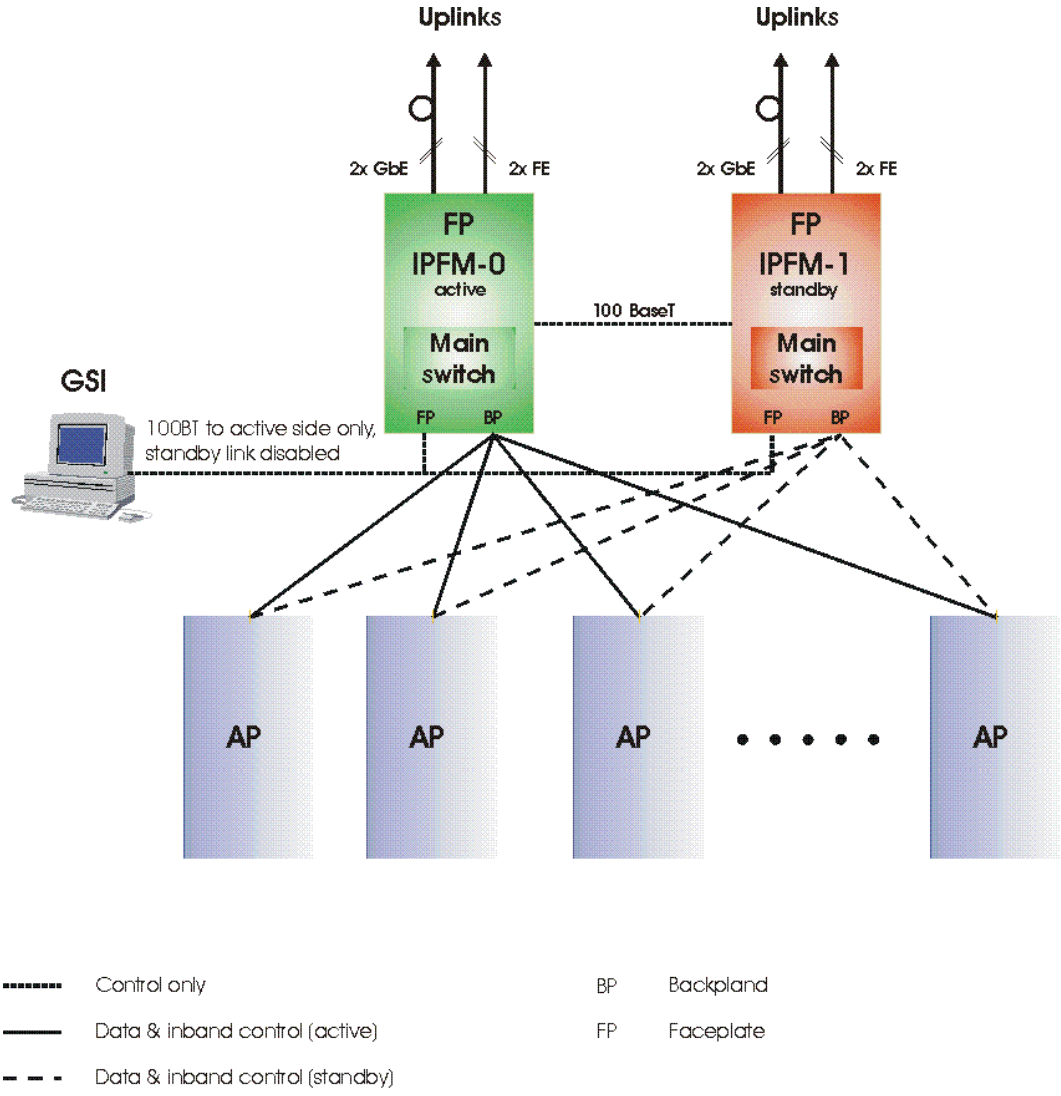
At delivery, IP APs are configured for controlled mode by default. That configuration, however, can be changed by provisioning and is stored non-volatile on the IP AP itself.

In controlled mode the system architecture is characterized by the following features:

- A LAG Shelf with IP spokes on the backplane is required
- The IPFMs are the controllers of the application packs (APs) in the IP subsystem.
- The traffic is handled by IP spokes on the shelf backplane which connect the APs to the IPFM.
- The uplinks on the faceplates of the IP APs are not usable in this mode.
- The IP AP configurations are stored on the IPFM.
- Two GbE uplinks per IPFM employing GBIC modules

- Two FE uplinks per IPFM
  All uplinks on the standby IPFM are disabled.
- FE downlinks to each AP slot
- FE inter-IPFM link for data synchronization purposes in duplex mode
- FE socket at the faceplate of each IPFM for connecting a management system in outband mode.
  In duplex mode, the management system is connected to a single IPFM at a time via a Y-cable. The interface on the standby IPFM is disabled.
- For some functions (LED test, metallic line testing) a COMDAC and a CIU/CTU are required in the shelf.

The figure below shows the principle of the system architecture for the IP subsystem in IPFM controlled mode. Not shown in the figure is the UART interface towards the COMDAC.

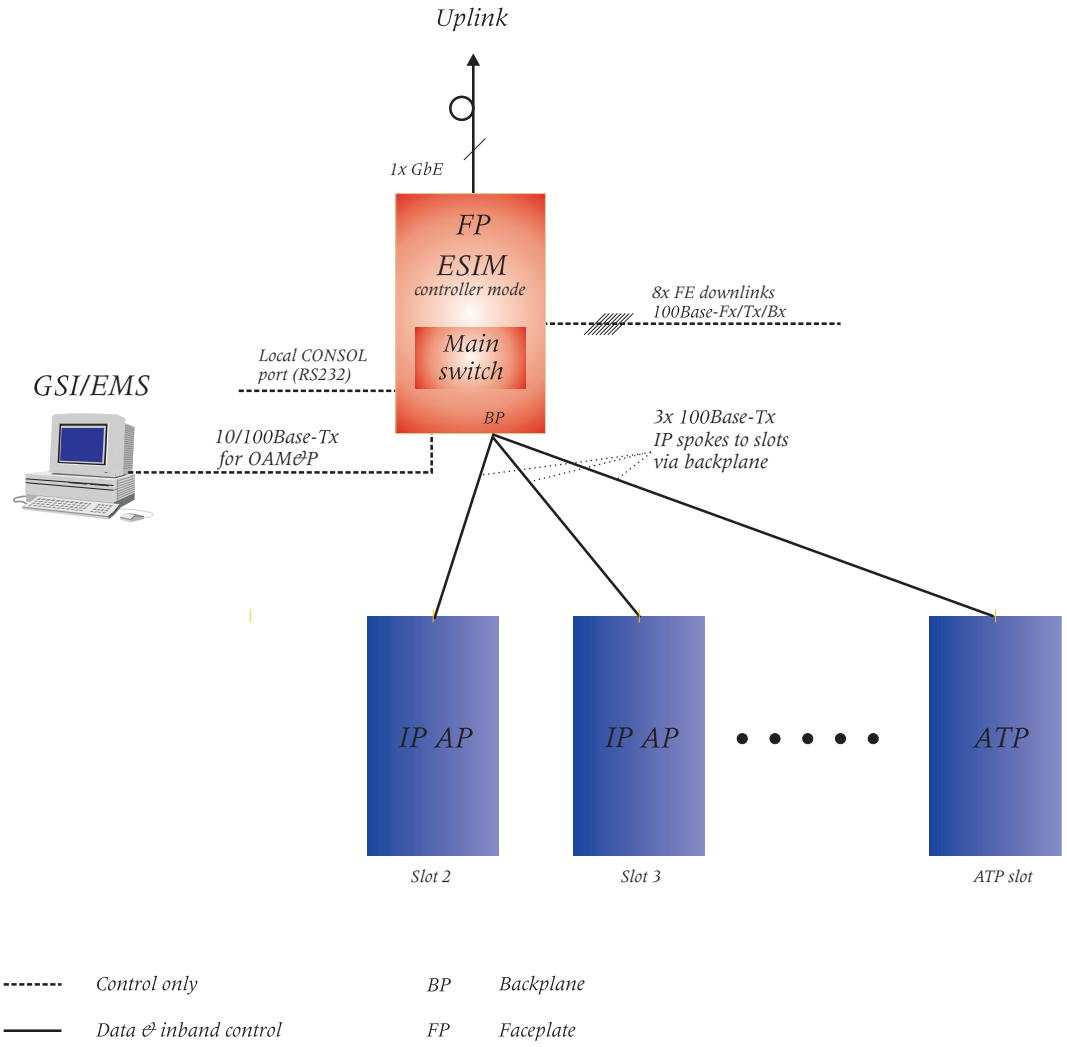


System architecture for ESIM controller mode

In this mode the system architecture is characterized by the following features:

- Applies only to LAG 200 Shelves.
- An ESIM is used as controller of the other application packs (APs) in the shelf.
- The traffic is handled by IP spokes on the shelf backplane which connect the APs to the ESIM.
  Two 100Base-Tx spokes to slots 2-3 for IP-APs
  Note that the uplinks on the faceplates of the IP APs are not usable in the ESIM controller mode.
- The IP AP configurations are stored on the ESIM.
- Eight Fast Ethernet (SFP, small form-factor pluggable module) downlinks.
- One GbE (SFP) uplink.
- FE socket (MGMT) at the faceplate of the ESIM for connecting a management system in outband mode.
- Serial RS232 interface with USB-A connector (CONSOLE) for command line interface (CLI)

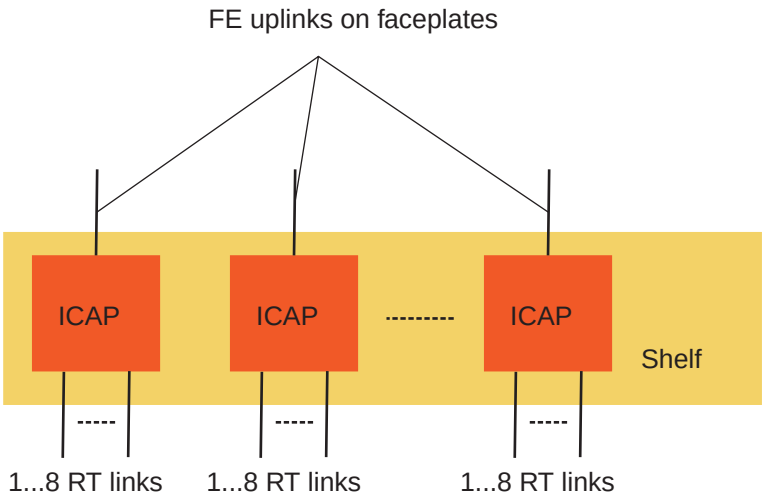
The figure below shows the principle of the system architecture for the ESIM as controller in a LAG 200 Shelf configuration.



IP APs in stand-alone mode

A stand-alone IP AP is a self managed pack which can be housed by any *AnyMedia* shelf . The faceplate connections are used for all IP traffic and on some IP APs for OAM&P. Although when operating as a stand-alone pack an IP AP remains an AP to the COMDAC, if present. It does not try to talk to an IPFM even if plugged into a LAG shelf. The management is via SNMP.

The next figure shows as an example ICAPs in a stand-alone mode configuration.



In contrast to the IPFM controlled mode, the management system has to treat each IP AP (or a pair of ICAPs in duplex mode) as a completely independent system.

A stand-alone IP AP has its own service IP address and OAM&P address. Program images, auxiliary files and database are stored non-volatile in NVDS on each individual stand-alone IP AP.

In stand-alone mode the system architecture is characterized by the following features:

- From a management perspective, each stand-alone IP AP is an individual independent network element, that means it reduces the NAM capacity in terms of managed shelves correspondingly.
- No controller is required for the stand-alone IP AP (with the exception of the COMDAC which is required for certain functionality such as LED test or metallic line testing).
- The software images and the database are stored on the APs.
- The inter-worked traffic is handled by the uplinks on the faceplate without using either IP spokes on the backplane or an IP controller.
- The uplink port(s) to the IP network as well as OAM&P ports for outband management (if existing) are located on the faceplate of the IP APs. The connection to the IP spoke on the backplane (if in a LAG Shelf) is disabled.
- Any *AnyMedia* shelf can be used.
- Any combination of IP APs capable of stand-alone operation is possible in the shelf and any number of stand-alone packs is allowed.

This mode is currently not yet supported by each IP AP type.

By default, IP APs come configured in controlled mode. When required, the controlled mode has to be changed to stand-alone mode during system turn-up.

An AP configured for stand-alone mode remains stand-alone even after it has been removed and inserted into another shelf.

IP AP types

For the different IP-based services several IP APs are used

- VoIP APs (LPZ600/LPZ602) in controlled mode for POTS to voice over IP and in stand-alone mode (LPZ600 only).
- IP COMDAC AP (ICAP) for voice over IP applications.
  The ICAP is usable to aggregate voice traffic from the same shelf, or from subtending remote terminals either running in controlled mode or in stand-alone mode in a simplex or duplex configuration.
- VDSL subscriber interface module (VSIM) APs for VDSL applications
- Ethernet subscriber interface module (ESIM) APs which includes 8 Fast Ethernet downlinks to subscribers.
  The ESIM is usable in IPFM controlled mode or can be also used as controller for other IP APs when running in the LAG 200 shelf configuration.
- IPADSL2_32p AP provisionable for
  – Full-rate ADSL (ITU-T G992.1 Annex A and T1.413)
  – ADSL lite (ITU-T G992.2)
  – ADSL2 ((ITU-T G992.3 Annex A)
  – ADSL2+ (ITU-T G992.5 Annex A, M)
  These services may be combined with POTS from another AP. Internal splitter function for each line is included.
  The IPADSL2_32p AP is usable in controlled mode or in stand-alone mode.

For more details on the APs refer to the *Data Sheet Book*.

The following table shows in which mode the individual IP packs are supported in the different shelf types.

Pack type		Mode type	Shelf types for International regions				Shelves for NAR regions	
			ETSI V5	LAG 1900	LAG 4300	LAG 200	FAST	LAG 2300
IPFM	LPI903	Controller	-	-	x	-	-	-
	LPI904	Controller	-	x	-	-	-	x
	LPI905	Controller	-	-	x	-	-	-
	LPI906	Controller	-	x	-	-	-	-
ESIM	LPE408	Controller	-	-	-	x	-	-
		Controlled	-	x	x	x	-	x
		Stand-alone	x	x	x	x	-	x
VSIM	LPV417	Controlled	-	x	x	x	-	x
VoIP AP	LPZ600	Controlled	-	x	x	x	-	-
		Stand-alone	x	x	x	x	-	-
	LPZ602	Controlled	-	x	x	x	-	-
		Stand-alone	-	-	-	-	-	-

Pack type		Mode type	Shelf types for International regions				Shelves for NAR regions	
			ETSI V5	LAG 1900	LAG 4300	LAG 200	FAST	LAG 2300
ICAP	LPI600	Controlled	-	x	x	-	-	x
		Stand-alone	x	x	x	-	x	x
IPADSL2_32pAP	LPA633	Controlled	-	x	x	x	-	x
		Stand-alone	x	x	x	x	x	x
IP-AFM	LPI960	Controller	x	x	x	-	x	x

IP forwarding module types

The IP forwarding module (IPFM) is the central controller of the IP subsystem (except the ESIM in a LAG 200 Shelf). Depending on the LAG shelf type used, different IP forwarding modules (IPFMs) are available:

- LPI903 and LPI905 for use in the *AnyMedia*® LAG 4300 Shelf
- LPI904 for use in the *AnyMedia*® LAG 1900 Shelf and LAG 2300 Shelf. LPI906 is only used in the LAG 1900 Shelf.

The IPFM supports the following features:

- Pack protection
- VLANs (up to 257)
- VLAN Swapping
- IGMP snooping
- IGMP fast leave
- MAC learning per port (uplinks and downlinks)
- Flow control per 802.3x on GbE uplinks
- Broadcast storm control per VLAN - up to 64 instances
- Link aggregation per 802.3ad Section 3 on uplinks
- Link aggregation control protocol (LACP) can be enabled/disabled
- Uplink protection via spanning tree protocol (STP) per 802.1d and Rapid spanning tree protocol (RSTP) per 802.1w are supported via a single group on uplinks.

L2, L3 and L4 functionality is supported at wire speed.

□

IP-based services – Voice

VoIP technology — Overview

The *AnyMedia*® Access System supports VoIP services in two ways:

- Voice is packetized on individual VoIP APs.
- The voice traffic and subscriber signaling provided via legacy TDM systems (international remote terminals or NAR GR-303 RTs) is transported by means of E1/DS1 feeders connected to IP COMDAC APs (ICAPs). The packetization of the voice traffic and the VoIP subscriber signaling is provided by the ICAP.
  The voice traffic of the same shelf or of several remote terminals in a central location may be aggregated by an ICAP.
  The ICAP may be located in one of the remote terminals or in a separate stand-alone shelf which does not provide legacy TDM subscriber interfaces.

For VoIP the following features are supported:

- Call features
  - Calling number display
  - Call waiting
  - Call waiting number display
  - 3-way calling
  - Configurable autonomous secondary dial ton (SDT)
  - Message waiting indication (audible/visual MWI)
- Direct dial-in
  - DTMF (push button) dialing
  - Dial pulse up to 25 pps
- Multi-line hunt group
- Emergency communication function
- Media monitoring
- Automatic answering tones (AAT)
- Talk to subscriber (TTS)
- Manual restriction control
- Software patch capability
- Music on hold.

VoIP technology using VoIP APs

In the upstream direction the telephone sends an analog audio signal to the POTS interface of the VoIP AP. There it is digitized, encoded and sent as RTP packet.

The VoIP APs are built based on the existing POTS technology and provide the following features and functionalities:

- 32/64 POTS ports (SIP or H.248 or MGCP signaling)
- Metallic test access

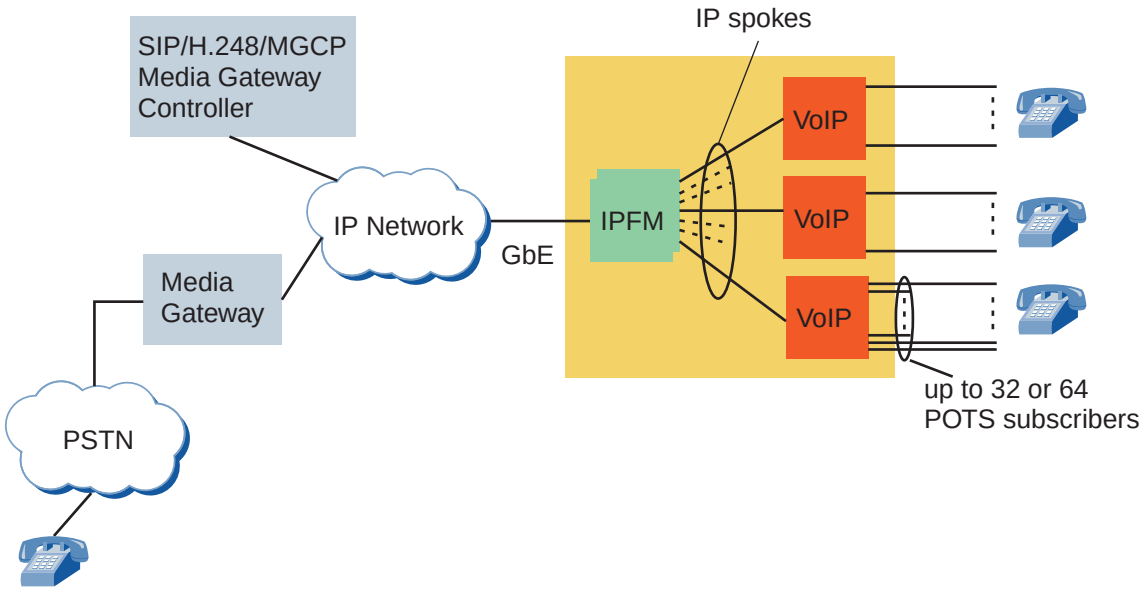
- 1:N port protection (per shelf)
- Support of up to 700 BHCC per pack
- Pre-blocking for subscriber calls on all user ports for replacing VoIP AP. Calls provided by this pack are preserved, but new calls are not established (shutdown mode).
- Customer-specific adaptations.

In controlled mode the IP voice and signaling packets are transferred from the VoIP AP towards the network via the 100Base-Tx uplink (IP spoke on the backplane) to the active IP controller.

In stand-alone mode the VoIP AP (LPZ600 only) may be used in any international shelf type. In this mode, the VoIP AP uses one FE port on the faceplate to directly connect to the IP network without using either IP spokes on the backplane or an IP controller.

In controlled mode downstream direction, the VoIP AP receives the VoIP packets from the IP controller and recovers the encoded voice data from the IP stream. In stand-alone mode the VoIP AP receive the VoIP packets form the IP network directly. Then the voice data is converted into a POTS analog signal.

The following figure shows as an example for VoIP technology a network configuration with VoIP APs in IPFM controlled mode.



When using VoIP APs, support for VoIP is added to the *AnyMedia*® Access System in a modular fashion. The VoIP APs provide all functionality necessary to support VoIP POTS telephony, including the call control stack (SIP or MGCP or H.248 version 2) and voice processing (RTP stream termination, tone detection/generation, echo cancellation, voice coding, etc.). Each VoIP AP essentially serves as an independent line access gateway for its 32 or 64 lines. There is no separate central controller for the call processing.

The VoIP APs are optimized for Greenfield NGN deployments. They allow growth of POTS over IP incrementally from a small configuration to thousands of lines and much more, without any constraints from TDM cross-connect capacity The distributed architecture allows service providers to incrementally add VoIP capability to *AnyMedia*® Access Systems without incurring a high initial cost. It provides best scalability in terms of CPU power at virtually unlimited processing power. The LPZ600/LPZ602 can support 32/64 VoIP simultaneous calls per pack, i.e., ALL POTS lines in the *AnyMedia*® LAG Shelf may be active in worst case conditions, battery and ringing capacity permitting.

The pack requires a single public IP address shared for signaling and voice (RTP).

The RTP streams may take the shortest path

- Intra-pack call
  If originating subscriber and terminating subscriber reside on the same VoIP AP then the RTP stream stays on the pack
- Intra-shelf call
  If originating subscriber and terminating subscriber reside on different VoIP APs then the RTP stream stays within the LAG but is routed through the IP controller
- Inter-shelf call
  If originating subscriber and terminating subscriber reside on different LAGs then the RTP stream is routed via the IPFMs of either shelf through the network.

VoIP technology using ICAP

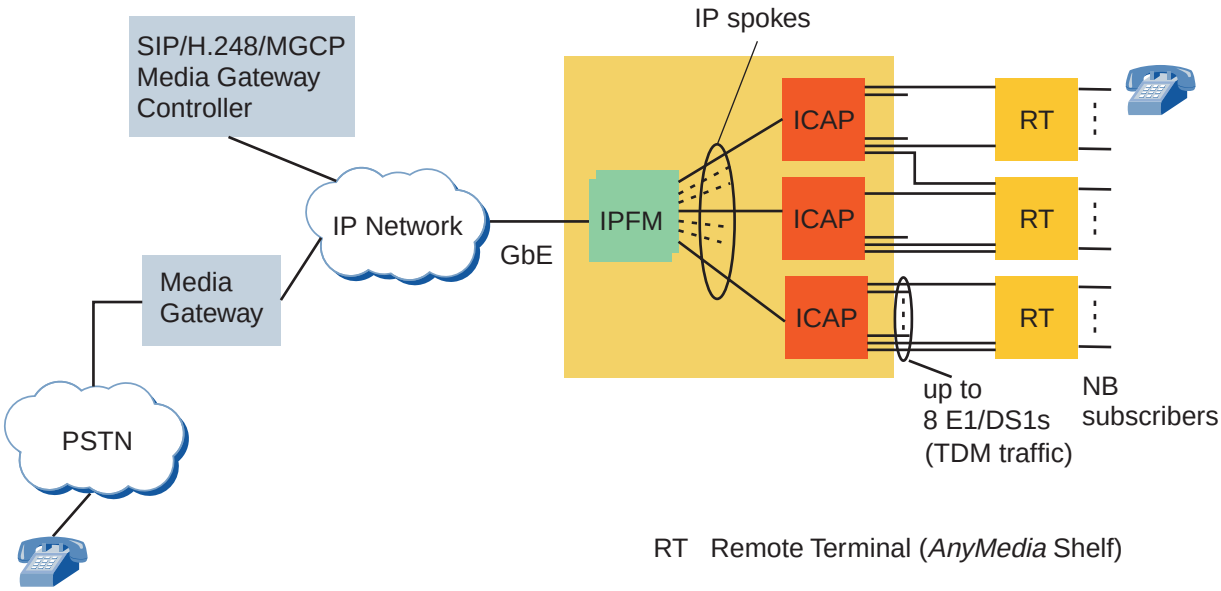
The ICAP enables network providers to upgrade existing *AnyMedia*® Access Systems for offering additionally VoIP services while keeping existing legacy *AnyMedia* Shelves and APs without using new VoIP packs. The subtending shelves connected to the ICAP operate in RT mode (apply to international regions) respectively GR-303 mode (apply to NAR).

An ICAP may reside in any AP slot and can operate in simplex mode or in duplex mode.

- In stand-alone mode the ICAP may be used in any shelf type (not yet supported in LAG 200 Shelf).
  In this mode, the ICAP uses one FE port on the faceplate to directly connect to the IP network without using an IPFM.
- In the LAG shelves it may be used in controlled mode (not yet supported in LAG 200 Shelf).
  In controlled mode the ICAP sends the IP packets via its uplink provided by an IP spoke on the backplane towards the IP controller. The IP controller aggregates the traffic of the uplinks of multiple ICAPs or other IP data packs into one central IP feeder.

Each ICAP terminates up to eight E1/DS1s. Packets are forwarded either to a Fast Ethernet (FE) faceplate connector (in stand-alone mode) or via an IP spoke on the backplane to the IPFM.

The following figure shows as an example a network configuration with the ICAP in IPFM controlled mode (in a LAG Shelf only) that will be described in more detail in the next section.

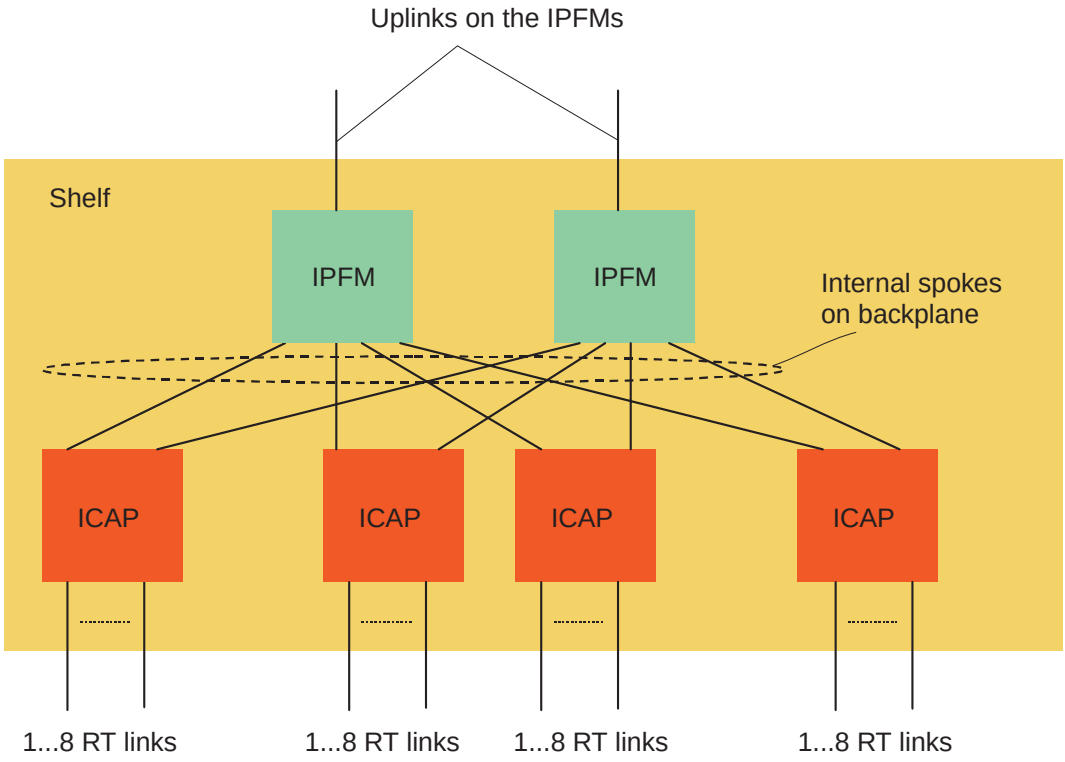


The ICAP provides the following features and functions:

- VoIP signaling protocols
  - SIP
  - H.248
  - MGCP
- Voice codecs
  - G.711
  - G.726
  - G.729AB
  - G.723.1A
  - Clear-channel
- Other features
  - G.168 near-end echo cancellation (up to 128 ms tail)
  - T.38 FAX relay
  - FAX/VGD pass through
  - 3-way conferencing
  - PayPhone support
  - Support of multiple H.248 backup media gateway controllers.
- Downstream feeders
  - 8 E1 feeders for remote terminal hosting (international regions) **or**
  - 8 DS1 feeders for GR-303 remote terminal hosting (NAR)

- Uplink
  - Stand-alone mode: One Fast Ethernet port on faceplate.
  - Controlled mode: One Fast Ethernet port on backplane compatible with IPFM high-speed links and/or one Fast Ethernet port on faceplate.
- Capacity
  - 2048 subtending lines
  - Maximum 15000 BHCA
  - The E1 ICAP supports 240 simultaneous active calls (8 feeders x 30 channels)
  - The DS1 ICAP supports 192 (minus datalinks) simultaneous active calls (8 feeders x 24 channels)
  - Provides up to 8 E1/DS1 ports for hosting remote terminals or E1/DS1s from the same shelf
  - Supports up to 8 *AnyMedia* E1 remote terminals for international regions
  - Supports up to 4 GR-303 remote terminals for NAR
- Pack protection
  - Either simplex operation mode or
  - 1:1 pack protection in protection groups (more than one protection group can be populated in a shelf)

The following figure shows ICAPs in controlled mode in a configuration with two IPFMs.



ICAPs in duplex mode

ICAPs can operate in simplex mode or in duplex mode as a protected pair, that means one ICAP is protected 1:1 by a standby ICAP in a neighbored slot. In case of a failure on the active ICAP, automatically a side switch will occur to the standby ICAP. The side switch can also be triggered manually by the operator.

Protection switching on the ICAP is not service-affecting. Stable calls will be saved during the side switch.

For an ICAP duplex configuration consider the following:

- The preferred ICAP resides in an odd numbered slot (for example slot 1) and the non-preferred ICAP resides in the even numbered slot to the right (for example slot 2).
- As one of the provisioning activities, the configuration mode has to be set to duplex.
- Provisioning is always done for the ICAP pair (the provisioning data of the ICAP pair is automatically effective for both ICAPs).
- For the E1/DS1 cabling a Y-cable is used.
- In stand-alone mode the FE2 ports on the faceplate of both ICAPs have to be connected via a special LAN crossover cable.

From the system point of view, both ICAPs of a protection group are considered as a single entity. That means they have one IP address assigned, the alarms on system level refer to the protected ICAP pair, and the alarms are raised by making use of the preferred slot id. Hardware-related alarms, for example pack alarms, refer to the ICAP that is actually impacted.

At delivery, ICAPs are configured for simplex mode

□

IP-based services – Voice over access node aggregation

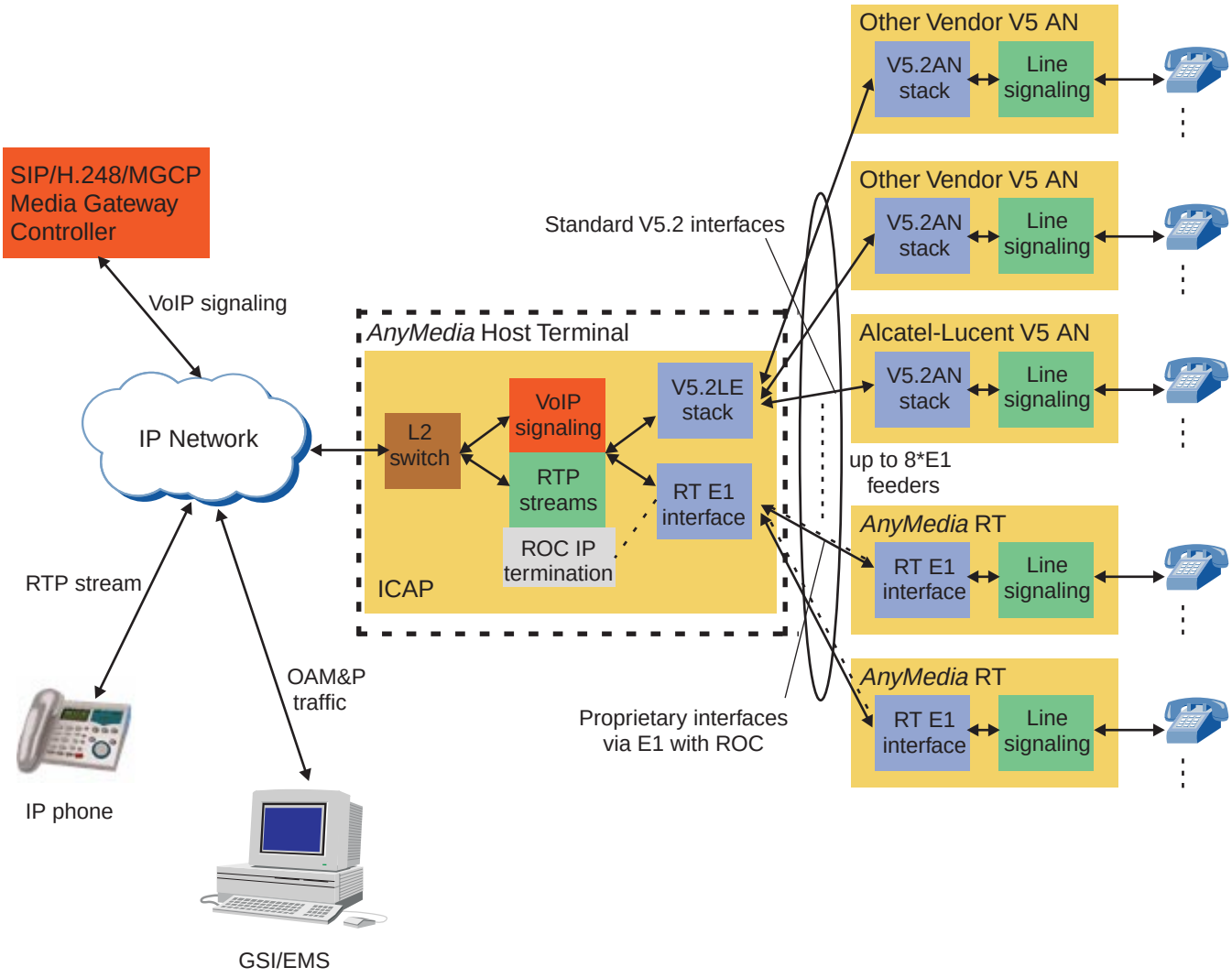
Overview

The ICAP in the *AnyMedia*® Access System supports TDM traffic aggregation from multiple access nodes (ANs) with the following interfaces:

- Standard V5.2 interfaces
  In V5.2 aggregation scenarios, which use the standard V5.2 protocol from any vendor, the ANs are connected to an ICAP in an *AnyMedia* host terminal. These scenarios provide conversion of TDM voice traffic to IP-based voice as well as conversion of V5.2 protocol-based signaling to IP-based network signaling (SIP, H.248 or MGCP).
- Proprietary remote terminal signaling and control interface via E1
  In *AnyMedia* remote terminal (RT) aggregation scenarios, which use a proprietary signaling and control protocol instead of the standard V5 protocol, only *AnyMedia* RTs are connected via the E1 interfaces to the ICAP. This scenario is also known as remote hosting, that means the host terminal provides some more functionality to the connected RT than pure aggregation.
- Standard GR-303 interface
  This scenario is similar to the standard V5.2 scenario. ANs with standard GR-303 interfaces from any vendor are connected to an ICAP in an *AnyMedia* host terminal which aggregates the traffic and provides conversion of TDM voice traffic to IP-based voice as well as conversion of GR-303 protocol-based signaling to IP-based network signaling (SIP).

For AN aggregation, the *AnyMedia* host terminal is either configured with ICAPs in stand-alone mode or with ICAPs in IPFM controlled mode. Each ICAP (or duplex ICAP pair) supports up to 2000 subscribers with up to 240 calls simultaneously.

The following figure shows as an example an AN aggregation scenario with V5.2 interfaces and with proprietary remote terminal signal and control interfaces via ICAP in stand-alone mode. The principle of GR-303 aggregation is the same, but it cannot be combined with the other aggregation types in one ICAP.



The standard V5.2 aggregation and remote terminal (RT) aggregation via the proprietary remote terminal signaling and control interface are supported within one image (mixed aggregation-share of the E1 feeder) and are different in the following aspects:

Standard V5.2 aggregation

Standard V5.2 access nodes can be connected over up to 8 E1 feeders to the ICAP as shown in the see figure above (connection via standard V5.2 interface to the V5.2LE stack in the ICAP). The protocol between the V5.2 access nodes and the ICAP is the standard V5.2 protocol. The ICAP provides a translation between TDM and VoIP, and all the POTS subscriber lines in the V5.2 access network are thus connected to an IP network.

The V5.2 aggregation supports the following protocols in accordance with the V5 standards:

- Common control protocol
- Port control protocol for PSTN

- PSTN signaling protocol
- Bearer channel connection protocol
- Link control protocol
- Protection protocol

These protocols are different depending on whether they are running at the LE site or at the AN site.

AnyMedia RT aggregation via proprietary RT signaling and control interface

In *AnyMedia* RT aggregation the 8 E1 feeders are shared for connecting *AnyMedia* remote terminals (RTs) only to the RT E1 interface in the ICAP. A protocol for the remote subscriber signaling and control functionality is used, which includes functions as offered also by a V5 standard protocol.

In *AnyMedia* RT aggregation scenarios the ROC channels are passed to the host terminal (ROC IP termination on ICAP) in a dedicated separate 64-kbps timeslot across all E1 links in order to implement ROC channel protection in case of “RT Link” failures.

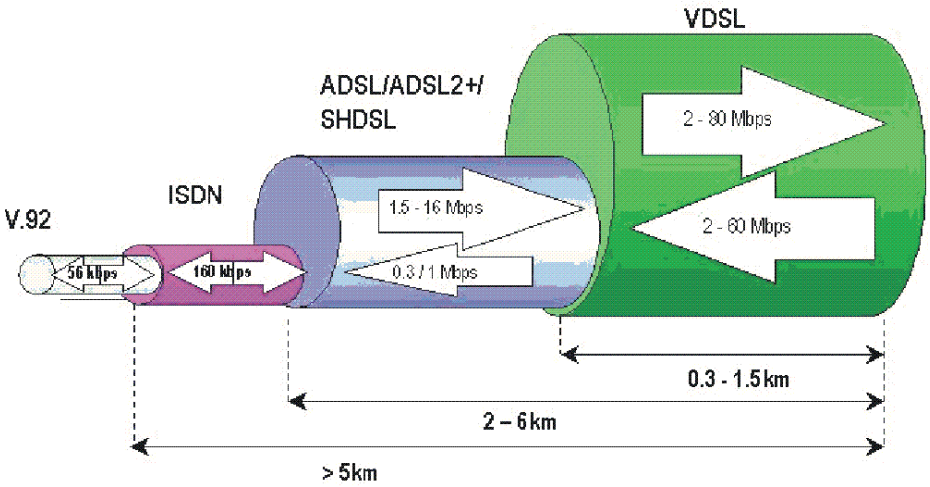
□

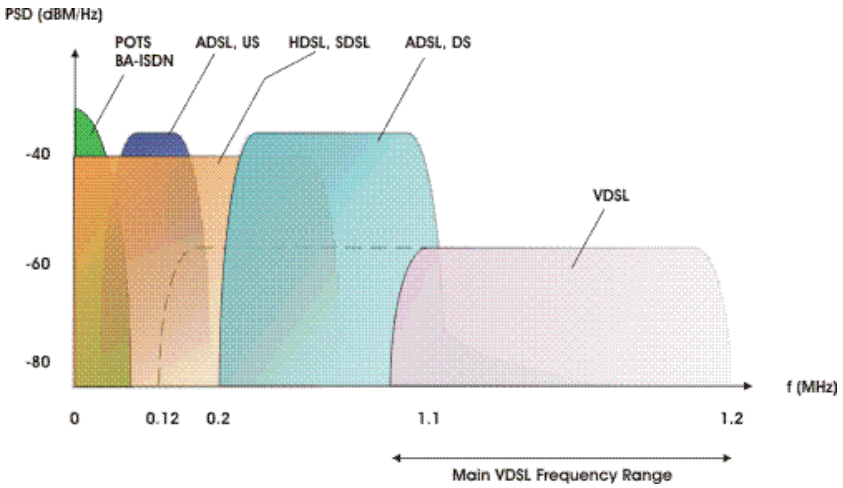
IP-based services – VDSL service

VDSL technology

The IP subsystem supports very high speed digital subscriber line (VDSL) service. VDSL is the highest-rate form of DSL technology available on shorter loops for both, symmetric and asymmetric modes.

Subscriber loop ranges may vary between 0.3 and 1.5 Km. Typical services provided on top of VDSL are very high speed internet access or video on demand. The next figure depicts a comparison between typical maximum bandwidths provided by some commonly used services.





The *AnyMedia*® Access System uses QAM (a single carrier modulation type) for line modulation..

Support of VDSL service implies the following capabilities:

- Up to 253 VLANs (VSIM AP)
- IGMP snooping

- IGMP fast leave
- MAC learning per VDSL port
- Flow control per 802.3x on VDSL downlinks (between VSIM and modem)
- Broadcast storm control per pack
- DHCP filtering (via classifier)
- NetBIOS/NBT filtering (via classifier)
- On-board POTS splitters
- QAM line modulation
- Bandplan 998 including Long Reach (LR) VDSL according to ITU-T G.993.1 Annex A involving US0 (25- 138 kHz) and bandwidth between 138 kHz and 1100 kHz for DS via programmable filters
  - Provisionable power back off function
  - Rate adaptive mode
  - Provisionable ADSL band use
- Metallic line testing
- VDSL performance monitoring.

□

IP-based services – Ethernet service

Technology used for ESIM

Support of Ethernet service implies the following capabilities:

- Accepts up to 8 SFP modules on downlinks
  - 100Base-BX
  - 100Base-FX and/or
  - 100Base-Tx
- Up to 257 VLANs
- VLAN Swapping
- IGMP snooping
- IGMP fast leave
- MAC learning per port (uplink and downlinks)
- Flow control per 802.3x on Ethernet downlinks and on GbE uplink on the faceplate in stand-alone mode
- Broadcast storm control per VLAN - up to 64 instances
- Link aggregation per 802.3ad Section 3 on downlinks
- Link aggregation control protocol (LACP) can be enabled/disabled
- Spanning tree protocol (STP) per 802.1d and Rapid spanning tree protocol (RSTP) per 802.1w are supported via a single group
- DHCP filtering
- DHCP Server
- NetBIOS/NBT filtering
- OSPF
- PIM
- 1 GbE uplink for applications with the ESIM used as controller in a LAG 200 Shelf. The following SFP modules are supported:
  - 1000Base-SX
  - 1000Base-LX
  - 1000Base-Tx

  The ESIM may also act as controller pack when inserted in slot 1 of a LAG 200 Shelf. In this special case, the ESIM will detect that it is inserted in the controlling slot and it will configure itself in a “shelf-control” control mode. In this mode the ESIM can control up to 2 APs (VSIM, VoIP AP, IPADSL2_32p AP).

L2, L3 and L4 functionality is supported at wire speed.

□

IP-based services – ADSL services

xDSL over IP — Overview

The *AnyMedia*® Access System supports xDSL services over IP in different ways:

- xDSL over IP using IP-AFM
- xDSL over IP using IP APs.

xDSL over IP using IP-AFM

The IP-AFM enables network providers to upgrade existing *AnyMedia*® Access Systems for offering xDSL services via IP while keeping existing shelves and xDSL APs.

In this configuration the AFM is replaced by an IP-AFM in the same slot. In upstream direction the IP-AFM packetizes the ATM cells from the subscriber lines into Ethernet frames and sends them via one of its uplinks towards the IP network. In downstream direction the Ethernet frames from the IP network are unpacked and the ATM cells are forwarded towards the subscribers. This way the IP-AFM acts as a multiplexer between an uplink on the network side and xDSL APs, converting ATM cells into Ethernet packets and vice-versa.

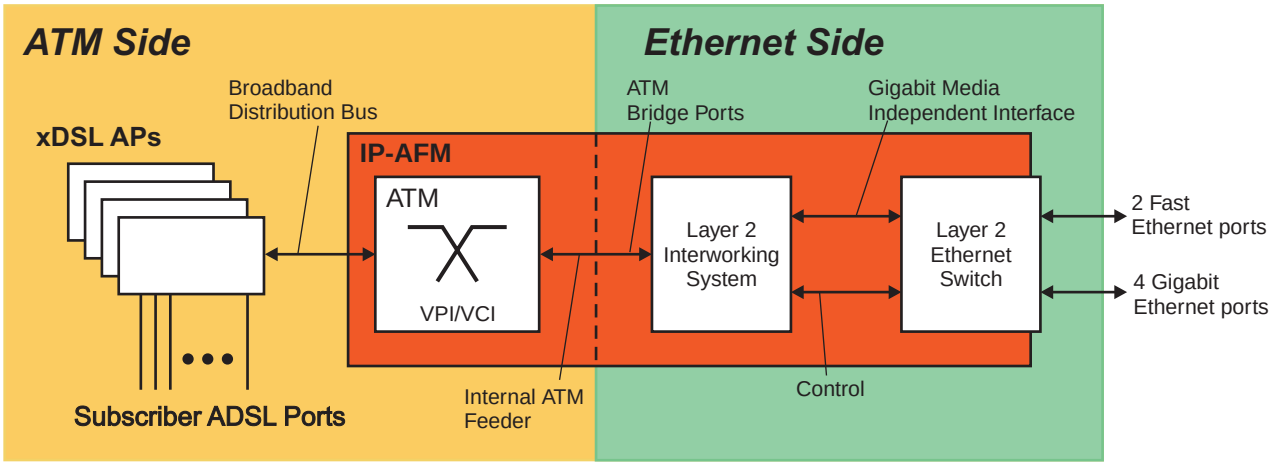
This IP configuration is favorably used for applications where already installed xDSL APs shall be preserved and a connection to an IP network is required.

For connecting multiple broadband subsystems to the IP network, IP-AFMs can be daisy-chained.

The IP-AFM uses ports on the faceplate for directly connecting to the IP network and for OAM&P. It does not require IP spokes on the backplane, and therefore it can be equipped in any *AnyMedia* shelf (except LAG 200). The management functions are initiated via SNMP.

The subscriber ADSL ports are cross connected via VPI/VCIs to an internal ATM feeder. These cross-connections correspond to the ATM bridge ports which allow subscriber traffic to ingress / egress the Layer 2 interworking system where the ATM cells are interworked into Ethernet frames.

The IP-AFM functionality view is shown from a high-level view in the following figure:



The IP-AFM provides the following features and functions:

- Acts as a multiplexer between a Gigabit Ethernet (GbE) or Fast Ethernet (FE) uplink and xDSL APs, converting ATM cells into Ethernet packets and vice-versa.
- Supports simplex or duplex operation
- Supports four GbE ports on the faceplate:
  - one port is used as uplink to the IP network or in case of a daisy-chain to the previous IP-AFM in a preceding shelf in the daisy-chain
  - one port is used to connect two IP-AFMs in duplex operation
  - one port is used as downlink to the next IP-AFM in a succeeding shelf in case of a daisy-chain
  - one port is reserved for future use.
- Supports two FE ports on the faceplate which can be used as uplink to the IP network
- One FE port can be used to aggregate traffic from an ICAP (simplex or duplex) to the GbE uplink on the IP-AFM via 100Base-T connection between the faceplate of the IP-AFM and the ICAP
- Supports daisy chaining between *AnyMedia*® Access Systems populated with IP-AFMs over one of the Gigabit Ethernet ports to increase the utilization of the ATM traffic to the IP network

Support of ADSL service via the IP-AFM implies the following capabilities:

- VLAN stacking
- 1 PVC to 1 VLAN mapping
  Note that the maximum number of 1 PVC to 1 VLAN mapping is 1024.
- n PVCs to 1 VLAN mapping
  Multiple PVCs from xDSL ports and/or trunk ports can be mapped into a single VLAN.
  Up to 32 VLANs as well as tag-based and port-based VLANs are supported.
- Broadcast storm control per pack
- IGMP snooping

- IGMP fast leave
- MACs can be learned or provisioned per ATM bridge port
- Flow Control on GbE uplinks per 802.3x
- Spanning Tree Protocol STP 802.1D
- Rapid Spanning Tree Protocol RSTP 802.1W
- ATM functionality as in existing AFMs;
  - ATM service categories
  - Connection admission control (CAC)
  - Overbooking factor per service category, except for UBR
  - Priority
  - Traffic shaping
  - Partial packet discard
  - Early packet discard (EPD)
  - Responds to F4/F5 loopback cells from modem

IP-AFM daisy-chain configurations

To increase the fill of the Gigabit Ethernet (GbE) interface that connects to the IP network, several IP-AFMs can be daisy-chained. These configurations provide transfer of Ethernet frames from each *AnyMedia*® Shelf onto a common connection to the IP network. All the GbE uplink ports used for daisy chaining need to be enabled by the operator.

Following daisy-chain configurations are provided:

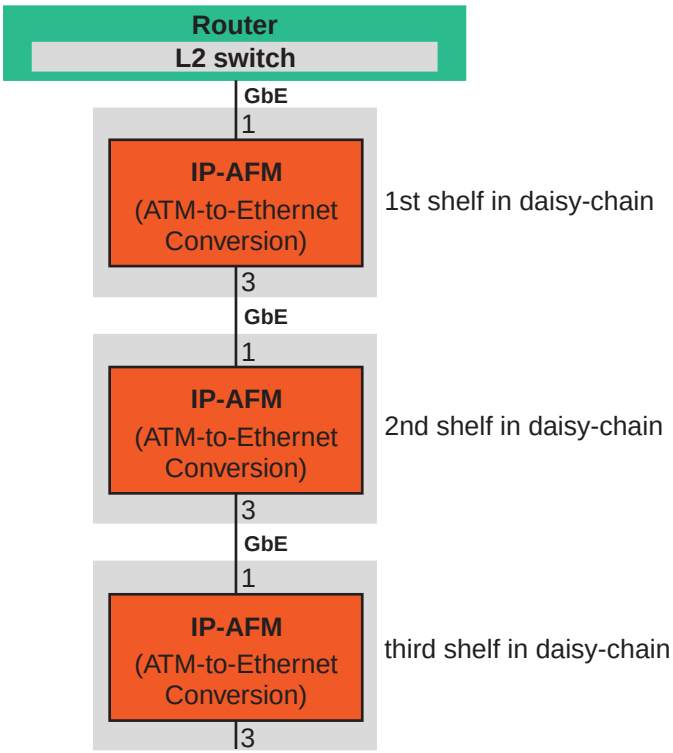
- Daisy chaining in simplex mode
- Daisy chaining in duplex mode

Daisy chaining in simplex mode

For connecting several shelves in a daisy chain, port GbE1 of the subtending shelf is always connected to port GbE3 of the previous shelf in a daisy-chain.

In the example shown in the figure below, three shelves share the same connection to the IP network.

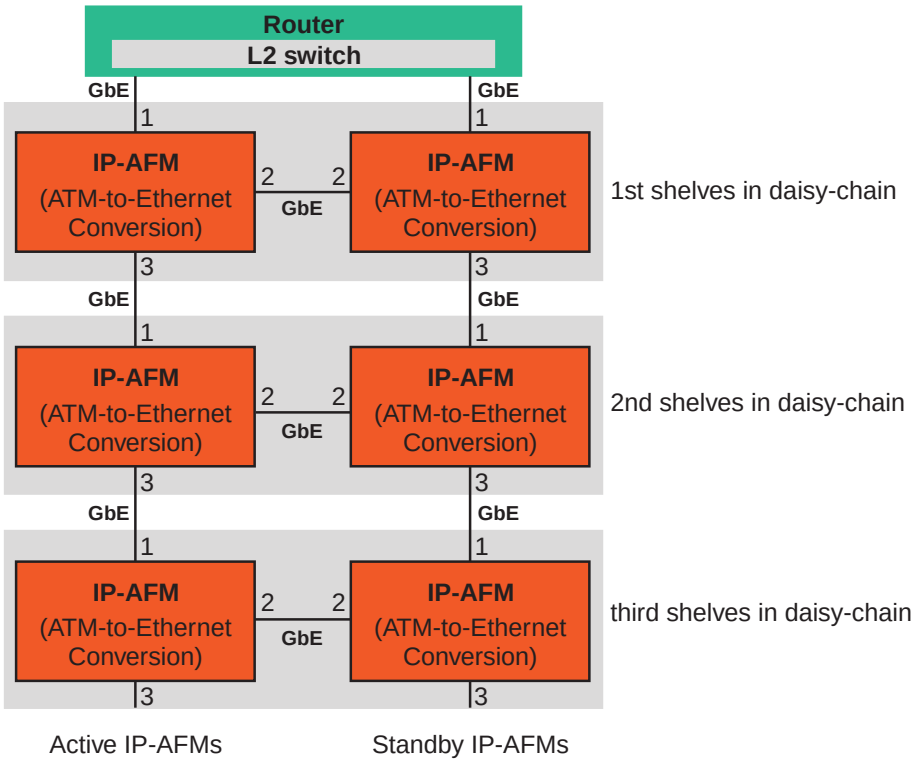
Daisy chaining in simplex mode (example) is shown in the following figure:



Daisy chaining in duplex mode

For daisy chaining in duplex mode each shelf in the daisy-chain is equipped with two IP-AFMs and the neighbored IP-AFMs are connected via the GbE 2 ports (Mate to IP-AFM).

Daisy chaining in duplex mode (example) is shown in the following figure:



xDSL over IP using IP APs

xDSL services over IP may also be provided on individual IP APs. Currently the system supports ADSL2 and ADSL2+ service by the IPADSL2_32p AP. These packs, autonomously convert ATM xDSL traffic from the subscribers into Ethernet frames and sent them towards the IP network. In downstream direction, the Ethernet frames are segmented in ATM cells and transmitted to the subscriber side.

The IPADSL2_32p AP may reside in any AP slot and can operate in stand-alone mode or in controlled mode. xDSL over IP using IP APs is preferably used for new installations (greenfield applications).

The technology used on IP APs for xDSL supports ATM cell transfer between customer premises equipment (CPE) xDSL modems and an Ethernet Layer 2 switch implemented on the pack. There, the ATM VCs are switched to Ethernet frames and forwarded towards the IP network.

An IPADSL2 AP can be viewed as Layer 2 bridge system composed by:

- Provisioned ATM VCs over the subscriber ports.
  These ATM VCs are named ATM bridge ports.
- Ethernet frames via Ethernet ports on the network side

The IPADSL2_32p AP can operate in stand-alone mode or in controlled mode. It may reside in any AP slot.

- For controlled mode an LAG Shelf is required.
  In controlled mode the AP sends the IP packets via an IP spoke on the backplane towards the IPFM.
- In stand-alone mode the AP may be used in any shelf type.
  In this mode, the AP uses one or both 100/1000Base-T uplink ports (on the faceplate) to directly connect to the IP network without using an IP controller.

Support of ADSL service implies the following capabilities:

- Up to 256 VLANs
- IGMP snooping
- IGMP fast leave
- MAC learning per ADSL port
- Flow control per 802.3x on GbE uplinks on faceplate in stand-alone mode
- Broadcast storm control per pack
- DHCP filtering
- NetBIOS/NBT filtering.

□

IP-DSLAM features – Overview

Overview

The IP subsystem provides the following IP-DSLAM features:

- VLAN
  - Tag-based
  - Port-based
  - L3 VLAN (IPFM and ESIM only)
  - VLAN stacking (IPFM and ESIM only)
  - Enhanced VLAN stacking (IP-AFM)
  - DHCP Option 82 (IP-AFM)
  - VLAN swapping (IPFM and ESIM only)
- Broadcast storm
  - per VLAN (except on VSIM and on IP-AFM)
  - per pack on VSIM and on IP-AFM
- IGMP snooping
  - IGMP fast leave
- IP trace route
- Static route defaults
- MAC learning
  - Provisioning of static MAC addresses per VLAN
  - Display of dynamic MAC addresses
- Quality of service
- DHCP and NetBIOS/NBT filtering
- DHCP Server (ESIM only)
- OSPF (ESIM only)
- PIM (ESIM only).

Some of these features are described in more detail in the following sections.

□

Virtual local area networks (VLANs)

Overview

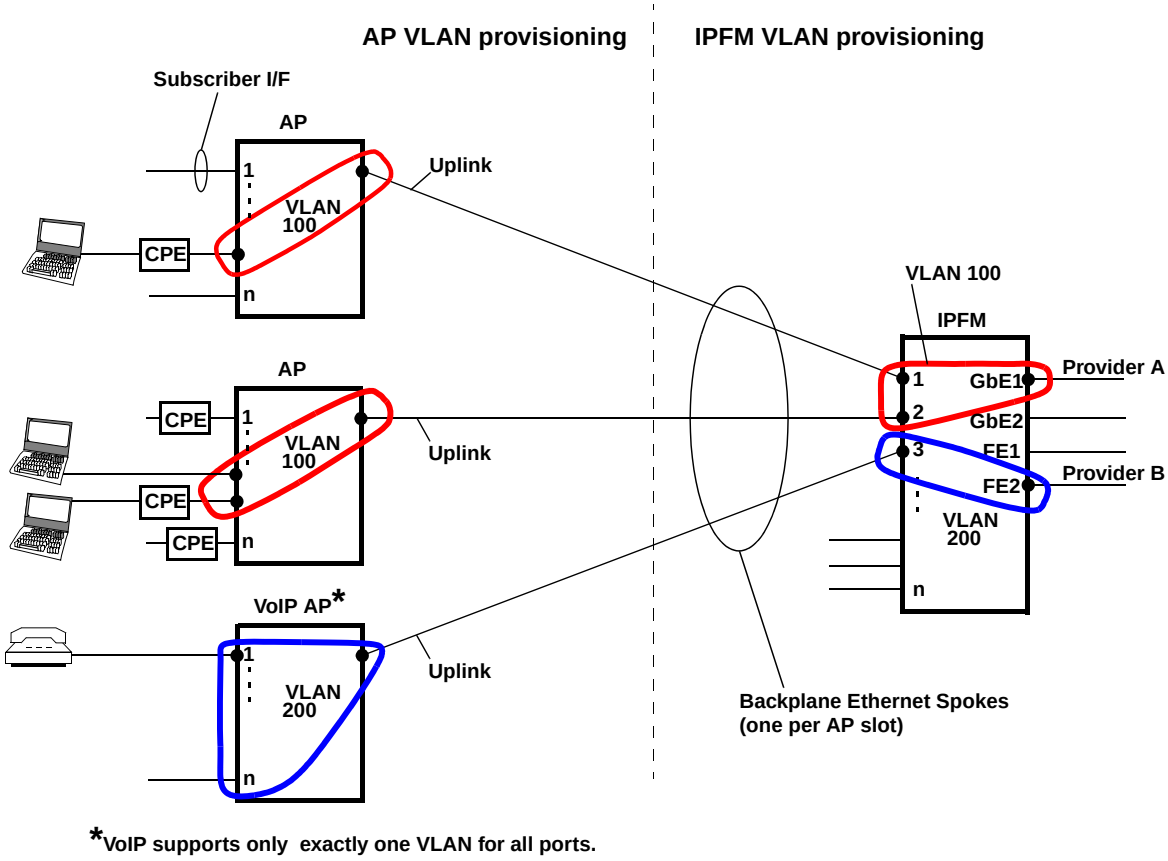
This section describes the overall idea of VLANs and how they are supported and used by the IP packs.

To provision VLANs at the IP subsystem the following assignments have to be considered:

- VLAN settings towards the network (IPFM uplink ports or uplink ports on stand-alone APs)
- VLAN settings on the system internal IP controller backplane ports (towards the APs)
- VLAN settings on the system internal AP backplane ports (towards IPFM/ESIM or IP-AFM)
- VLAN settings towards subscriber (AP subscriber/xDSL ports)
- VLAN settings on ATM bridge ports of IP-AFM controller:
  - In an IP-AFM configuration, the ATM bridge ports represent the subscriber ingress/egress points of the bridge system. They are defined by VCC (VPI/VCI) cross-connections as provisioned in legacy AFMs.
  - Each VLAN can accommodate up to 736 cross-connections bridge ports.

That means, that although VLANs are effective across the system, they are provisioned on a per pack basis. The operator has to ensure consistent provisioning among the packs

The following figure shows the principal concept of VLAN provisioning.



VLAN Basics

A VLAN allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group called VLAN group. A station can belong to more than one VLAN group. The stations on the same VLAN group can communicate with each other, but a station cannot directly communicate with a station that doesn't belong to the same VLAN group.

To communicate with stations in other VLAN groups the traffic must first go through a router which is configured to support Layer 3 VLAN routing. VLANs also increase network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. A VLAN group is a broadcast domain. In traditional Layer 2 switched environments, all broadcast packets go to each individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

There are three commonly used Layer 2 VLAN implementations:

- Port-based VLAN
- IEEE 802.1q tagged VLAN
- PVC-based VLAN (applicable to IP-AFMs only)

The most significant difference between the VLAN implementations is that tag-based VLAN can operate across Layer-2 switches of the same network, whereas a port-based VLAN only operates at a single switch level. The VoIP AP supports tag-based VLAN. The other IP packs support a combination of both modes.

The number of supported VLANs depends on the pack type:

- The IPFM supports 257 VLANs (note that internal VLANs cannot be provisioned).
- The ESIM supports 257 VLANs (note that internal VLANs cannot be provisioned).
- The VSIM AP supports 253 VLANs.
- The IP-AFM supports 32 VLANs for n PVCs to 1 VLAN mapping (VLAN aggregation mode) and 1024 VLANs for 1 PVC to 1 VLAN mapping.
- The IPADSL2 AP supports 256 VLANs.
- The VoIP AP and the ICAP support exactly 1 VLAN each.

The VLAN identifiers are supported in the range of 1 through 4092. The VLAN ID 1 is the default VLAN and the VLAN IDs 4093 and 4094 are reserved for internal use.

The IEEE 802.1q VLAN specification comprises three tasks:

- Ingress process
- Forwarding process
- Egress process

Ingress rules

The ingress process identifies whether the incoming frames contain a tag, and classifies the incoming frames belonging to a VLAN. Each port has its own ingress rules.

Forwarding process

The forwarding process decides whether or not to forward the received frames according to its filtering database. The filtering database stores and organizes VLAN registration information used to take the forwarding decision for frames to and from switch ports.

Egress rules

The Egress Process decides whether the outgoing frames will be sent tagged or untagged. In the IP subsystem VLAN is provisioned on each pack. For an AP this means that the VLAN has to be provisioned also for the uplinks of the individual APs (actually the backplane spokes) to the IPFMs. Vice versa, the IPFMs have to define a VLAN on the appropriate downstream port (backplane spokes).

Broadcast storm control function

The broadcast storm control function monitors the incoming traffic per pack (IP-AFM, VSIM AP) or per VLAN (IPFM, ESIM, IPADSL2 AP). If the broadcast traffic (frames per second) crosses a provisionable threshold (frames per second), then the broadcast traffic on the VLAN is blocked until the broadcast traffic drops below the provisioned threshold.

In case of broadcast storm control per VLAN the traffic level where the traffic is blocked for the dedicated VLAN can be set in a range from 16 up to 1048560 pps. A value of 0 means that the broadcast storm control is disabled for this VLAN, independent of whether the global enable/disable function is set to ″enabled″. Up to 64 ″storm control groups″ are supported.

Tunnel VLAN

VLAN tunneling (or stacking) refers to the mechanism where one VLAN may be encapsulated within another backbone VLAN (also known as tunnel VLAN). In this way a carrier can partition the network among several Internet service providers (ISPs), while allowing each ISP to still utilize VLANs to their full extent.

VLAN swapping

VLAN swapping is a method of VLAN translation to allow more flexibility in VLAN allocation.

□

Additional L2 and L3 functions

Overview

Besides VLAN provisioning, the IP subsystem provides a couple of additional Layer 2 and Layer 3 functions:

- IPFM L3 VLAN data
- Flow control according to 802.3x
- MAC learning
- Spanning tree
- Link aggregation
- Static routes
- IGMP snooping/IGMP fast leave
- DHCP relay
- VLAN Swapping (IPFM and ESIM only)
- DHCP Server (ESIM only)
- OSPF (ESIM only)
- PIM (ESIM only)
- PPPoE insertion tag (IP-AFM)
- DHCP Option 82 IP-AFM (IP-AFM)
- Enhanced VLAN stacking (IP-AFM).

IPFM L3 VLAN data

VLANs use bridging and broadcast functionality (L2 data). Additionally, IP routing functionality is optionally performed based on one IP address assigned to the VLAN.

The IPFM and the ESIM in stand-alone mode allows the user to define up to 62 L3 VLANs.

If a L3 VLAN is set up, the IPFM/ESIM analyzes all packets within that VLAN and performs the appropriate routing.

L3 VLANs are useful to route packets between different VLANs which are otherwise separated from each other.

Flow control

Flow control ensures that a receiving device can handle all of the incoming data. So, flow control can improve the overall performance of a network and increase the efficiency of bandwidth utilization. Special frames, called “pause frames” are sent from the receiver to the sender to indicate that the receiving device is not able to handle all incoming data and to request a defined pause time. Flow control is only used between adjacent hosts and not from hosts that are not physically attached. Depending on the network equipment, flow control can be enabled on both transmission and reception, or on either the transmission or the reception, or can be disabled on both ends.

On the uplinks, flow control per 802.3x (included in IEEE 802.3-2003) /802.3z can be disabled or enabled.

MAC address learning

The IP packs (except the VoIP APs) internally maintain a table with the MAC addresses that are learned from the network (dynamic MAC addresses). When an incoming Ethernet frame is received, the IP pack examines its destination MAC address and looks up for this entry in the MAC table, to determine the outgoing port where the frame must be forwarded. These MAC addresses are kept in the table for a provisionable period of time and then they will be removed. The next time a frame is received from that destination, the IP pack needs to re-learn the MAC address again. If a frame is received with a source MAC address for which an entry exists in the table, then its associated timer is reset.

It is also possible to provision MAC addresses in the table directly by the operator (static MAC addresses).

For IP-AFM the MAC addresses can be learned or provisioned per ATM bridge port.

Spanning tree

The IP subsystem provides link protection via spanning tree according to the following standards:

- Spanning tree protocol (STP) defined by IEEE 802.1d standard or
- Rapid spanning tree protocol (RSTP) defined by IEEE 802.1w standard.

When links are configured using STP or RSTP, one of the links is the active one, the others are considered to be standby connections. They are placed in the blocked state by one of the nodes, that means, no traffic is forwarded to them.

Currently STP and RSTP are differently supported:

- By the IPFM on the uplinks.
- By the ESIM on the downlinks to the Ethernet subscribers.
- By the IP-AFM on uplinks and on daisy-chain ports (RSTP also on the link to the mate IP-AFM).

Link aggregation

Link aggregation as defined by IEEE 802.3ad standard is supported on the IPFM on the uplinks, on the ESIM on the ports for the downlinks to the subscribers on the uplinks and on the daisy-chain ports.

When links are aggregated into a single logical link, maximum usable bandwidth is available to the system when both links are operational. When one link fails, the bandwidth degrades to 50% of maximum, but transmission is maintained. Active connections (including VoIP calls) will be maintained. When the link recovers, bandwidth is increased to 100%, again without impact on active connections.

Link aggregation is limited to links using the same bandwidth, that terminate on the same pack.

Static routes

Routers forward packets to the destination addresses based on information from static routes or dynamic routing protocols. In the *AnyMedia*® Access System the IPFM supports up to 256 static route entries. Destination IP address, the subnet mask and one default gateway are provisionable.

IGMP snooping

The IP subsystem supports Internet group management protocol (IGMP) snooping as defined in RFC2236 for IGMP V2.

The purpose of IGMP is to restrain multicast traffic in a switched network, since by default, a LAN switch floods multicast traffic within the broadcast domain. This can cause a huge waste of bandwidth. When IGMP snooping is enabled on a VLAN, the system discards all unknown multicast traffic. The IGMP provides the means by which traffic is forwarded to switch ports at which subscribers receiving a certain multicast are connected.

IGMP snooping allows Layer 2 switches to ″listen in″ on the IGMP conversation between hosts and routers. When a Layer 2 switch hears an ″IGMP report″ (that is the request from a client to join a given multicast group), the switch adds the host's (switch) port number to the group destination address – Multicast IP address list for that group. When the switch hears an ″IGMP leave″, it removes the host's port from the table.

The IP subsystem supports IGMP Fast Leave. IGMP Fast Leave can be enabled/disabled per pack.

DHCP relay

DHCP servers can be used to distribute dynamic IP addresses to the APs. As the DHCP servers may be located outside the subnet of the APs, the IPFM and the ESIM are provisionable to act as a DHCP relay between the DHCP requests of the APs and the DHCP servers and their responses.

DHCP filtering

DHCP filtering is provisionable. When enabled, the DHCP responses are accepted from the uplinks, while DHCP responses from downlinks are dropped.

NetBIOS/NBT filtering

When NetBIOS/NBT filtering is enabled, all NetBIOS/NBT packets are filtered on both the uplinks and downlinks.

PPPoE insertion tag IP-AFM Layer 2 function

PPPoE is PPP variation where the PPP protocol data units are transmitted via an Ethernet based medium.

When PPPoE Line Id Tag Insertion is enabled the ATM Bridge Ports is provisioned with the option for inserting a line identification tag in the PPPoE discovery and request PDUs sent by the PPPoE client running on the subscriber's machine.

PPPoE Tag Insertion Mode: Specifies how the agent circuit Id tag will be generated by the PPPoE function. If set to **Auto**, the tag will be generated as specified in the corresponding work order. If set to **Explicit**, this field will be set to the cross-connection name of the associated VCC.

DHCP Option 82 IP-AFM Layer 2 function

DHCP is an IP protocol which is used to dynamically assign the IP address and other configuration parameters, such as default gateway, subnet mask, DNS server address etc., from DHCP server to a client. Since the client is usually working in a distrustful environment, it is very important to identify the real DHCP request client by a trusted access node.

The main purpose of DHCP Option 82 is to insert the subscribers identification information to the DHCP packets by a trusted access node (DHCP relay agent). The DHCP option 82 feature is used to provide line identification for the authentication services.

The ATM Bridge Ports on the IP-AFM can be provisioned to:

- Insert a DHCP Option 82 in the (DHCP Discover/Request/Decline/Release/Inform) PDUs that are sent by the client that is running on the subscriber's machine.
- For the downstream direction, the DHCP option 82 in the (DHCP Offer/Ack/Nack) PDUs is always be removed without caring the ATM Bridge Port provisioning.

If DHCP Option 82 is enabled, the IP-AFM will activate the L2 DHCP relay agent function for the specified ATM Bridge Port. In this situation, all (DHCP Discover/Request/Decline/Release/Inform) PDUs are intercepted by the IP-AFM and have the DHCP option 82 tag inserted.

The **DHCP Option 82 Insertion Mode**: Define how the DHCP Option 82 tag will be generated automatically (auto) by the L2 DHCP Relay Agent function or will be explicitly configured by the user on a per bridge port basis (explicit).

Enhanced VLAN stacking

VLAN stacking is used to uniquely identify Subscribers and Network Service Providers (NSPs). This is done by using two levels of VLAN tagging.

The IP-AFM support the insertion of two VLAN tags into an upstream frame and remove those two VLANs in the downstream frame:

- The Outer VLAN (NSP-VLAN) uniquely identify Network Service Providers (NSPs)
- The Inner VLAN (User-VLAN) identifies the user serviced by that NSP.

The User-VLAN-id value is unique within the NSP VLAN.

To keep the current single VLAN inserting function, current VLAN ID provisioned in the VLAN Table is kept and used by the single VLAN insertion function only. It means that all VLAN IDs in the VLAN Table are used by the single VLAN insertion function and are not used as an NSP-VLAN or User-VLAN by the double VLAN insertion function.

To support the double VLAN insertion function, a new VLAN Group Table is created. In this new table, there are two fields, one for the VLAN Group ID and another for the NSP-VLAN ID.

VLANs are grouped into 64 groups as follows:

- VLAN Group 1 includes VLAN Id from 2 to 63
- VLAN Group 2 includes VLAN Id from 64 to 127 . . .
- VLAN Group 64 includes VLAN Id from 4032 to 4092.

If an NSP-VLAN Id is assigned to a VLAN Group, all VLAN IDs in this group can only be used as a User-VLAN ID. If no NSP-VLAN ID is assigned to a VLAN Group, all VLAN IDs in this group can only be used by an existing VLAN table for the single VLAN Insertion function only. It is possible to assign to an ATM Bridge Port a User-VLAN with the same Id than an NSP-VLAN.

□

2 Physical interfaces

Overview

Purpose

This chapter describes the physical interfaces of the *AnyMedia*® Access System related to IP-based services.

The following table shows as an overview the subscriber interfaces, the network interfaces (for stand-alone mode and for IPFM controlled mode) and the OAM&P interfaces used in each of these modes.

Interface	Pack Type						
	IPFM	ICAP	VoIP AP	VSIM AP	ESIM	IP-AFM	IPADSL2_ 32 AP
Subscriber	-	8 E1/DS1 interfaces with 36-pin AMP champ ribbon style connectors	32 Z or 64 Z interfaces with 64-pin AMP a/b connector	16 VDSL interfaces with 64-pin AMP a/b connector	8 Fast Ethernet downlinks with SFPs	Broadband distribution bus to ATM xDSL APs (up to 736 xDSL subscribers on controlled APs)	The connector on the AP side includes two connectors: POTS connector with 32 pin and POTS-ADSL connector with 32 pin

Interface		Pack Type						
		IPFM	**ICAP**	**VoIP AP**	**VSIM AP**	**ESIM**	**IP-AFM**	**IPADSL2_ 32 AP**
Network	In IPFM controlled mode	2 GbE uplinks with GBICs 2 FE uplinks 100Base-T port with RJ-45 connectors	IP spoke to IPFM				N/A	IP spoke to IPFM
	In stand-alone mode	-	1 10/100 Base-T uplink with RJ-45 connector (FE1)	1 10/100 Base-T uplink with RJ-45 connector[1]	-	1 GbE uplink with SFP	4 GbE with SFP 2 FE uplinks 100Base-T ports with RJ-45 connectors	Two 100/1000Base-T uplinks[2] with RJ-45 connectors
	In ESIM controller mode	-	-	-	-	1 GbE uplink with SFP[3]	-	-
OAM&P	In controlled mode	100Base-T port with RJ-45 connector Inband management channel CONSOLE port with 9-pin D-sub connector[5]	-	-	-	[4]	N/A	-
	In stand-alone mode	-	RS232 port with USB-A physical connector[5] Inband management channel	RS232 local console port with RJ-45 connector[1],[5] Inband management channel	N/A[6]	RS232 port with USB-A physical connector[5] 10/100Base-T port with RJ-45 connector	RS232 local console port with RJ-45 connector 10Base-T port or remote link with RJ-45 connector Inband management channel	RS232 port with USB-A physical connector[5] 10/100Base-T port with RJ-45 connector Inband management channel

Notes:

1. Only the VoIP AP LPZ600 supports stand-alone mode.
2. One for future use.

3. Applicable in LAG 200 Shelves only.
4. If the ESIM is used in controller mode in a LAG 200 Shelf, then it provides the same management interfaces as in stand-alone mode.
5. For initial system turn-up.
6. Pack is not yet used in stand-alone mode.

Contents

Subscriber interfaces/Downstream feeders

Overview

Currently the following subscriber interfaces are supported in the IP subsystem:

- E1/DS1 interfaces on the ICAP used as downstream feeders to *AnyMedia*® remote terminals (RTs)
- Z interfaces on the VoIP AP
- VDSL interfaces on the VSIM AP
- Fast Ethernet ports on the ESIM
- IP-AFM indirectly supports up to 736 ADSL interfaces on ATM xDSL APs it controls
- ADSL ports on the IPADSL2_32p AP.

Note that the VoIP AP (LPZ600), the VSIM AP and ESIM is currently supported only for international regions.

E1/DS1 interface on ICAP

Two E1/DS1 interfaces (one for protection as buddy feeder) for up to 8 E1/DS1 downstream feeders to *AnyMedia*® RTs are located on the ICAP (LPI600).

In E1 mode the downstream feeders are HDB3-coded interfaces with separate pairs for transmit and receive direction. The bit rate is 2048 kbps. The electrical and physical characteristics correspond to ITU-T Recommendations G.703 and G.823 (for jitter aspects). Via this interface, digital signals are transmitted in frames, according to ITU-T Recommendation G.704 and G.706.

In DS1 mode the bit rate is 1544 kbps. The feeders use a GR303-like proprietary format.

Two connectors are provided, each serving 8 Tx/Rx feeders. The main input (M DS1/E1) is used for simplex configurations. In 1:1 protected configurations, a Y-cable connects to the main input of both ICAPs. The active pack terminates the signals and the standby pack opens relays to disconnect its input. The “buddy” connector (B DS1/E1) is for future use in 1:N protected configurations.

The connectors used are 36 pin AMP champ ribbon style.

Z interface

The Z interface is identical to those in the narrowband subsystem. For a description refer to the *Application and Planning Guide, Narrowband and ATM xDSL Services (363-211-586)*.

The Z interfaces on a VoIP AP are provided by the LPZ600 or LPZ602. The connector used is a 64 pin AMP a/b connector.

VDSL interface

The VDSL interface is a twisted 2-wire subscriber interface.

In the *AnyMedia*® Access System it supports:

- Bandplan 998 including Long Reach VDSL according to ITU-T G.993.1 Annex A involving US0 (25- 138 kHz) and bandwidth between 138 and 1100 kHz for DS via programmable filters

VDSL interfaces are provided by the VSIM AP (LPV417). The connector used is a 64 pin AMP a/b connector.

Ethernet interface on ESIM

The ESIM accommodates eight Fast Ethernet downlinks to subscribers. The following small form factor pluggable (SFP) module types are used:

- 100Base-Tx (RJ45 connector for electrical connection)
- 100Base-FX (LC connector for optical connection).
- 100Base-BX (LC connector for optical connection).

These Ethernet ports to the subscribers are provided by the ESIM (LPE408).

ADSL interface

The ADSL interface is a twisted 2-wire subscriber interface. It provides voice and data transmission using discrete multitone (DMT) technology. All ADSL standards are supported.

In the IP subsystem ADSL interfaces are provided by the IPADSL2_32p AP (LPA633). The connector used on the AP side includes two connectors one POTS connector with 32 pin and one POTS-ADSL connector with 32 pin.

□

Network interfaces

Overview

The IP subsystem provides the following network interfaces according to IEEE 802.3. These network interfaces are accessible from the faceplates of the individual packs.

- 2 Gigabit Ethernet (GbE) uplinks per IPFM
- 2 Fast Ethernet (FE) uplinks per IPFM
- 2 Fast Ethernet (FE) uplinks per ICAP; one FE is used as uplink, the second one is used only as stand-alone duplex for the cross-couple
- 1 Gigabit Ethernet (GbE) uplink per ESIM for stand-alone mode and ESIM controller mode
- 4 Gigabit Ethernet (GbE) uplinks and 2 Fast Ethernet (FE) uplinks per IP-AFM controller mode
- Two 10/100/1000Base-T uplinks per IPADSL2_32p AP for stand-alone mode.

In IPFM controlled mode, the IP APs are connected to the IPFM via an IP spoke on the backplane.

GbE uplinks on IPFM

The GbE uplinks are designed as 1000Base-SX/LX uplink interfaces. They use Gigabit Interface Converter (GBIC) modules which are attached to the faceplate of the IPFM(s). The GBIC modules are industry-standard hot-swappable devices.

The maximum distances for the currently used GBIC types are

- For the SX range
  - 220 m with 62.5 µm multi-mode fiber
  - 500 m with 50 µm multi-mode fiber
- For the LX range
  - 275 m with 62.5 µm multi-mode fiber
  - 550 m with 50 µm multi-mode fiber
  - 10 km with single-mode fiber.

FE uplinks on IPFM

The FE uplinks are implemented as 100Base-Tx uplink interfaces which are accessible via RJ-45 connectors on the faceplate of the IPFM(s).

Uplinks on ICAP

For stand-alone mode the ICAP provides two FE uplinks which are implemented as 10/100Base-Tx uplink interfaces. One FE is used as uplink, the second one is used only as stand-alone duplex for the cross-couple. They are accessible via RJ-45 connectors on the faceplate of the ICAP.

In 1:1 protected configurations, each ICAP uses one uplink towards the network. The second uplink port is connected via a short crossover cable to the neighbored ICAP, allowing the active ICAP to keep the protection ICAP updated with call state and control information.

Uplinks on ESIM

For stand-alone mode the ESIM provides 1 GbE uplink via faceplate. The following small form factor pluggable (SFP) module types may be used there:

- 1000Base-T (RJ45 connector for electrical)
- 1000Base-SX (LC connector for optical for short reach) - multimode fiber
- 1000Base-LX (LC connector for optical for long reach).

The maximum distances for the currently used SFP types are

- For the SX range
  - 220 m with 62.5 µm multi-mode fiber
  - 500 m with 50 µm multi-mode fiber
- For the LX range
  - 275 m with 62.5 µm multi-mode fiber
  - 550 m with 50 µm multi-mode fiber
  - 10 km with single-mode fiber.

SFPs are industry-standard devices.

GbE uplinks on IP-AFM

The four GbE uplinks are designed as 1000Base-SX/LX/T uplink interfaces. They use Small Form-factor Pluggable (SFP) modules which are attached to the faceplate of the IP-AFM(s). The SFP modules are industry-standard hot-swappable devices.

The maximum distances for the currently used SFP types are

- For the SX range
  - 220 m with 62.5 µm multi-mode fiber
  - 500 m with 50 µm multi-mode fiber
- For the LX range
  - 275 m with 62.5 µm multi-mode fiber
  - 550 m with 50 µm multi-mode fiber
  - 10 km with single-mode fiber.

In duplex operation, one GbE port is used for mating a second IP-AFM.

In daisy-chain configurations, one port is used as uplink to the IP network or in case of a daisy-chain as uplink to the host IP-AFM or the previous IP-AFM in a preceding shelf in the daisy-chain.

One GbE port is used as downlink to the next IP-AFM in a succeeding shelf in case of a daisy-chain.

One GbE port is reserved for future use.

FE uplinks on IP-AFM

Only one of the FE ports can be used as uplink to the IP network. If the uplink is a Gigabit optical interface, it can also be used to aggregate IP traffic from the ICAP.

Uplinks on IPADSL2_32p AP

For stand-alone mode the IPADSL2_32p AP provides two 10/100/1000Base-T uplinks (R-J45 connectors) on the faceplate. One of them is intended for future use.

□

OAM&P interfaces for IP-based services

Overview

This chapter describes the maintenance interfaces for operations, administration, maintenance, and provisioning (OAM&P) of the *AnyMedia*® Access System related to IP-based services. Where to access the system for OAM&P activities, depends on whether the packs operate in IPFM controlled mode or in stand-alone mode.

In IPFM controlled mode the interfaces used are located on the IPFM. The following OAM&P interfaces are provided:

- 100Base-Tx port (outband)
- Inband management channel
- CONSOLE port (for initial system turn-up)
- The IP-AFM provides the same type of OAM&P interfaces as the IPFM

For stand-alone mode the OAM&P interfaces used are located on the individual APs.

- An 10/100Base-Tx management port designed as RJ-45 connector (not applicable for the ICAP)
- An RS232 console port connector (USB-A connector) CONSOLE which is used during initial system turn-up.

Note that not all IP APs support stand-alone mode and that not all IP APs provide these management ports.

A PC-based graphical system interface, the *AnyMedia*® Access System graphical system interface software (GSI) or the *Navis*™ *AnyMedia*® Element Management System (NAM) which can manage hundreds of network elements (NE) at a time operate over these OAM&P interfaces.

100Base-T port (outband)

The 100BaseTx port (outband) on the faceplate of the IPFM is a 100 Mbps interface which is used locally or remotely for outband management. It connects the GSI installed on either a PC equipped with an Ethernet LAN card or a computer equipped with a NIC (LAN) to the IP subsystem. An RJ-45 faceplate connector is provided on the faceplate for local access.

In cases where a shelf uses two IPFMs in duplex mode, a special Y cable connection or a hub can also be used. The maximum cable length is 100 m when category 4 or 5 distribution pair unshielded cabling is used. The interface is IEEE 802.3-compliant.

Inband management channel

Inband management denotes a configuration where the management systems use a communication channel embedded in links that also carry user traffic.

For security reasons the inband management channel should be part of a VLAN (Management-VLAN). For more details refer to “Inband management via Ethernet uplinks” (p. 4-14).

CONSOLE port on IPFM (for initial system turn-up)

The CONSOLE port on the faceplate of the IPFM is an RS232 local access terminal interface port for use during initial system turn-up. A DB-9 faceplate connector is provided on the IPFM.

For connecting to the CONSOLE port a null modem cable with male connectors on one side and female connectors on the other side is required.

10/100Base-T port on IP APs (for management system access)

In stand-alone mode the ESIM and the IPADSL2_32p AP can be accessed by the management systems via a 10/100Base-T port on the faceplate of the packs. The connector used is an RJ-45 connector.

Note that a stand-alone ICAP is not equipped with a separate 10/100Base-T port for OAM&P. Instead, it uses inband management via the traffic-carrying RJ-45 ports.

CONSOLE port on IP APs (for initial system turn-up)

For use during initial system turn-up, the IP-AFM and IP APs (ICAP, ESIM, IPADSL2_32 AP, LPZ600) which are capable to operate in stand-alone mode , can be accessed via an RS232 local access terminal interface port. The connector used is a USB-A connector.

A special console cable is designed to connect the USB-A style faceplate console port to an RS232 DB9 DTE port on a PC (see the *Ordering Guide*). A null modem is not required.

□

Alarm interfaces

Overview

As physical alarm interfaces the *AnyMedia*® Access System provides local alarm and status indicators.

Local alarm and status indicators

The packs have light emitting diodes (LEDs) on the faceplate to indicate status and failure conditions. Any alarms indicated by the LEDs are reported also via the OAM&P interfaces.

□

Testing interfaces

Interfaces for manual testing

Interfaces for manual testing are:

- Faceplate jack *DROP* on the CIU/CTU
  This interface is used for metallic test access to the subscriber line.
- Faceplate jack *CHAN/MON* on the CIU/CTU
  This interface is used for metallic test access to the port hardware and for listening to an existing call.

Interfaces for metallic test access

Interfaces for metallic access are:

- TAP connector for metallic test access in the connector field of the *AnyMedia*® LAG Shelf
- Connector on the faceplate of the test application pack.

Control interface for external test head

Interface for external test head testing

- Serial EIA-232C RTU port at the connector field for control access via the CIU/CTU.

□

3 OAM&P for IP-based services

Overview

Purpose

This chapter describes the Operations, Administration, Maintenance, and Provisioning (OAM&P) operations for IP-based services for the *AnyMedia*® Access System.

Contents

Configuration management

Overview

Purpose

Configuration management is the system activity for operations that control and provision the system, including the following:

- Software management - used to manage the nonvolatile program storage (NVPS) of the system.
- Database management - used to manage the nonvolatile data storage (NVDS) of the IP subsystem. The NVDS contains provisioning data.
- Inventory management - system activity of collecting, updating, and reporting data on system equipage and system status.

Contents

Software and configuration data management – IPFM

Overview

Software and configuration data management refers to the management of program images of the IP controller and the IP application packs (IP APs) and to the handling of provisioning data. It also means methods to backup and restore the database. It applies to the IPFM in simplex and duplex mode, to the ESIM in controller mode (in the LAG 200 Shelf only) and to the stand-alone IP APs. It may be used either during initial system turn up or in a running system.

IPFM program image

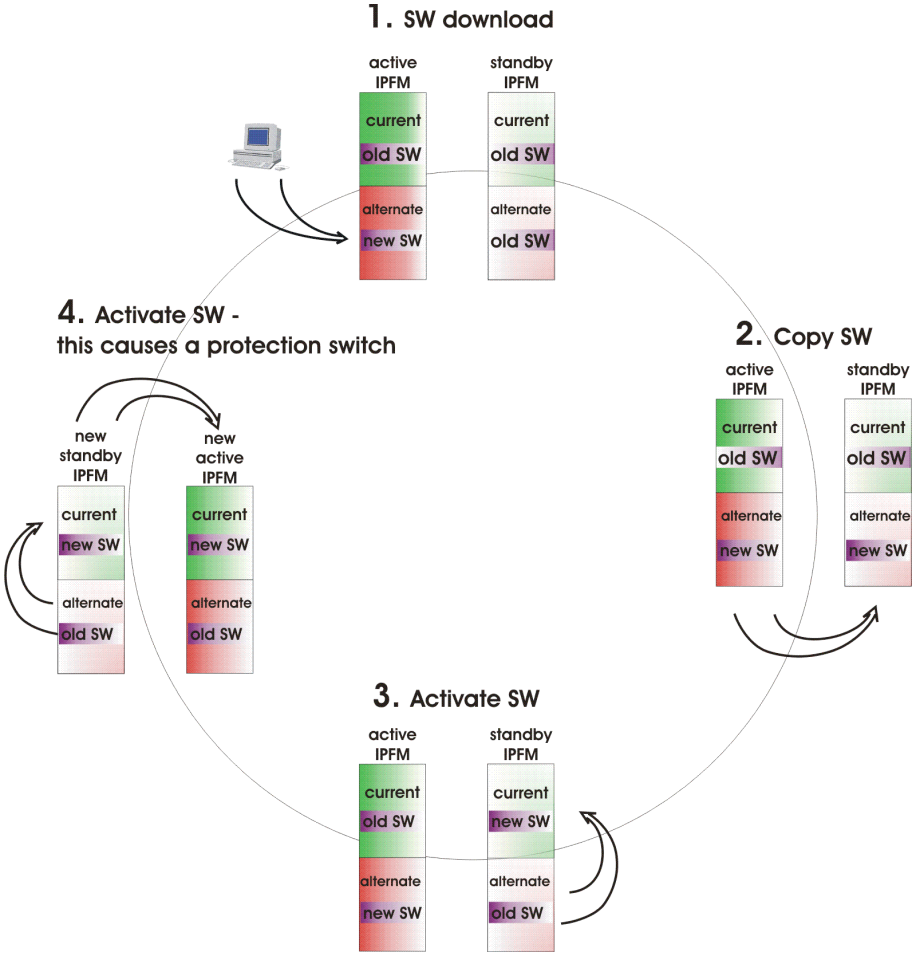
A download of the IPFM program image always goes to the ″Alternate″ storage of the active IPFM. Note that ″Standby″ status implies that ″Current″ software versions of active and standby IPFM are identical. Download of the IPFM software to the standby IPFM copies both the ″Current″ and ″Alternate″ versions of software from the active IPFM to the standby IPFM. When the download is finished the software versions in ″Alternate″ and ″Current″ of active and standby IPFM are equal.

The procedure for upgrade on a duplex IPFM system is as follows:

- Download software to active IPFM
  Result: The new software is now in the ″Alternate″ location.
- Copy the software from the active IPFM to the standby IPFM
  Result: The old software is now in the ″Current″ location on both IPFMs and the new software is now in the ″Alternate″ location on both IPFMs.
- Activate software on the standby IPFM
  Result: The standby IPFM resets. When initialization completes, the standby IPFM is running the new software. The old software is in the ″Alternate″ location.
- Activate software on the active IPFM
  Result: The active IPFM resets and a protection switch occurs. When the IPFM completes initialization, it is running the new software. The old software is in the ″Alternate″ location.

At the end of the procedure the new software is running on both the active and on the standby IPFM. The previous standby IPFM (at the start of the procedure) is now the active IPFM.

The figure below shows the IPFM software upgrade graphically.



AP program images

The APs of the IP subsystem require the download of program code. The program images of the APs are independent files, i.e. they are not included in the IPFM program load. It is the responsibility of the operator to ensure consistency of the various program image versions in the system.

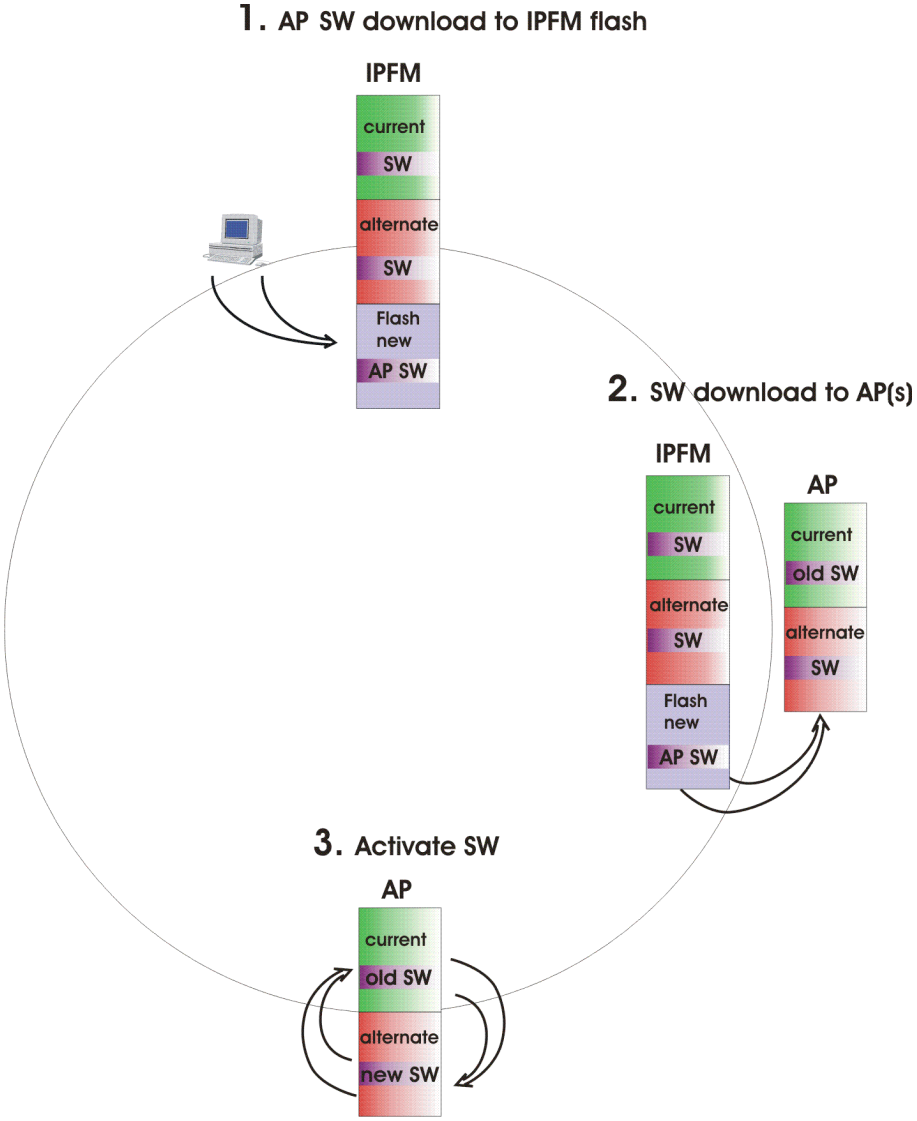
The download of AP program images is performed as follows:

- The AP program image is downloaded into the NVPS of the IPFM via FTP.
- The AP program image is downloaded from the NVPS of the IPFM to the NVPS of the AP(s). The operator may initiate via the GSI/NAM a software download per pack type (VoIP, VSIM) or for individual pack instances. So far, the images on the APs continue to run the current load.
- The new load has to be activated
  - for all packs or
  - for one pack individually or
  - for several selected packs.

  .

The APs store two NVPS (Current, Alternate), with the exception of the VSIM AP. The VSIM AP stores one NVPS.

The figure below shows the AP software upgrade graphically.



Specific software upgrade capabilities for VoIP

Now the *AnyMedia*® Access System provides improved software upgrade capabilities for VoIP.

Software upgrades may consist of

- Application patches only or
- Full software upgrades.

If the software upgrade is an application patch only, the service outage will be approximately 10 seconds. If the software upgrade is a full software upgrade then the service outage is at least 30 seconds.

In order to determine which type of software upgrade is relevant, compare the old SW version number and the new SW version number. The example below shows how to distinguish between a patch and an upgrade.

Initial SW version	03.00.01.00**-**001_001	
Patch	03.00.01.00**-**00**2**_001	If there is any difference after the ″-″. then the SW upgrade is an application patch and the service impact will be brief.
Upgrade	03.00.01.0**1-**001_001	If there is any difference before the ″-″, then the SW upgrade is an application upgrade and the service impact will be greater than for a patch.

AP provisioning changes during operation

Provisioning changes in the IP subsystem are directly done on the running AP, not on the IPFM.

That means two assumptions have to be made for provisioning changes:

- The AP must be inserted and running. No preprovisioning can be done in advance.
- After provisioning is completed a manual ″Save to NVDS″ is required in order to store the changes on the NVDS of the IPFM.

NVDS backup and restore

The system supports backups of the NVDS data in case of failures of the NVDS.

Backups of the NVDS data can be uploaded from the NVDS to an external ftp server. NVDS backup will not occur automatically; it must be initiated manually.

The system also supports restoration of a previous release's NVDS data in the event of a back out of a new software release. The restoration of previous data is done through the NVDS database download (restore) from the external ftp server. After a manual ″Save to NVDS″ action the data are stored in the NVDS of the active IPFM and in case of duplex IPFMs, also on the standby IPFM.

Configuration management for APs in stand-alone mode

By default, stand-alone IP application packs are configured in IPFM controlled mode. When required, the IPFM controlled mode has to be changed to stand-alone mode during system turn-up by downloading and activating a different SW on the AP.

Configuration management like SW download, database backup and restore is supported on APs in stand-alone mode through file transfer protocol (ftp) and secure ftp (SFTP).

□

Software and configuration data management – IP-AFM

Overview

Although the IP-AFM contains two processors which require internally 2 SW images (instead of one on the AFM) the part of the configuration management and of the SW download strategy that is visible to the operator, has been maintained from the ATM AFMs.

The SW download to the XDSL APs is identical to the procedure on the ATM AFM.

NVPS and AP program images

The system has re-programmable program memories in the IP-AFM and each xDSL AP. Each IP-AFM in the non-volatile program storage (NVPS) contains its own program memory and load images for the xDSL APs.

The IP-AFM routinely polls the xDSL APs and verifies the xDSL AP program memory. If the xDSL program memory is corrupt, the IP-AFM will automatically download the appropriate load image to the program memory of the xDSL AP. The software download from the IP-AFM to the xDSL APs may impact subscriber service. If an xDSL AP is replaced, the appropriate load image is automatically downloaded to the new pack if necessary.

The system is capable of modifying the IP-AFM and xDSL AP program memories through:

- IP-AFM software download operation or
- IP-AFM replacement.

IP-AFMs require a different SW than ATM AFMs. Therefore the numbers for the SW versions differ, see example as follows:

- 1.29.**01**.01 is an AFM load
- 1.29.**51**.01 is an IP-AFM load

The version number of the IP-AFM differs in the third part of the version number that carries out a fixed gap of 50.

IP-AFM software download and activation

The software download and activation procedures are the same as for ATM AFMs.

The SW download procedure can be separated from the SW activation procedure. The software download operation is not service affecting. For duplex IP-AFMs, the software is downloaded to both, the active and the standby IP-AFM.

The software download procedure provides the following options (for simplex and duplex mode):

- SW Download only
  A complete IP-AFM SW image is installed in the NVPS ″Alternate″ directory (in duplex in both IP-AFMs simultaneously).
- Activate and reboot
  The SW toggles from ″Alternate″ directory to the ″Current″ directory and vice-versa in both processors. After the reboot that is initiated automatically, both processors run the new SW.
  In order to avoid service disruption, in duplex mode the activation is first done for the standby IP-AFM, which reboots and takes control from the active IP-AFM. The previous active IP-AFM becomes protection IP-AFM before rebooting.
- SW download and activate and reboot
  This procedure combines both procedures above in a single action.

While all these procedures keep the current database, similar procedures can be done with discarding the database:

- Initialize system database and reboot
  The current IP-AFM database is discarded and the IP-AFM is restarted with the initial default DB
- Activate and initialize and reboot
  The SW in NVPS toggles from ″Alternate″ directory to the ″Current″ directory and vice-versa in both processors. After the reboot that is initiated automatically, both processors run the new SW but with the initial database.
- SW download and activate and initialize and reboot
  This procedure combines the procedures above in a single action.

Soak actions are supported for SW updates on trial. They can only be performed in duplex mode.

- Soak and reboot
  The SW is activated only on the protection IP-AFM. When necessary, and possible, the database is evolved. After this a protection switch to the IP-AFM running the image on trial is performed.
  It is possible to switch back to the former active IP-AFM that still runs the old image and database, if the trial SW is not accepted by the operator.
- SW download and soak and reboot
  This procedure combines SW download, soak and reboot in a single action.

NVDS backup and restore

The system supports backups of the non-volatile data storage (NVDS). Backups of the NVDS can be stored on the GSI or EMS and restored if required. NVDS backup does not occur automatically. It must be initiated by the operator either locally or remotely.

□

IP configuration management – Inventory management

Overview

Inventory management information for the IPFM and the IP APs can be retrieved via the IPFM as soon as the packs have been inserted. A technician using the GSI/NAM sees a graphical representation of the *AnyMedia*® LAG Shelves populated with IPFM pack(s) and IP APs.

In mixed configurations, inventory management information for IP packs, as well as narrowband APs, can also be retrieved via the COMDAC. A technician using the GSI/NAM logged into the COMDAC sees a graphical representation of the *AnyMedia*® LAG Shelves populated with both narrowband and IP APs. A technician using the GSI/NAM in a mixed configuration when connected to the IPFM sees a graphical representation of the *AnyMedia*® LAG Shelves populated with IP APs only.

Retrievable inventory items

Electronically readable inventory management information for each IP AP in the system can be retrieved on demand.

Below is a list of definitions for retrievable network inventory items.

Retrievable pack inventory items include the following:

- *CLEI* - a 10-character code that identifies each pack type.
- Serial Number - a 12-character code that uniquely identifies each pack. The serial number includes the date and place of manufacture.
- Apparatus Code - uniquely identifies the equipment function (for example LPI904); packs with different apparatus codes are not interchangeable.
- Interchangeability Code - used to specify the backward compatibility of two packs with the same type and apparatus code but different manufacturing versions (that means different series). The marking takes the form m:n where n is the series of the marked pack and m is the series that the circuit pack is compatible with.
  - Example 1:

    1:3 means that this pack is a series 3 pack. It is backward compatible with series 2 packs and also series 1 packs.
  - Example 2:

    2:3 means that this pack is a series 3 pack. It is backward compatible with series 2 packs only.
  - Example 3:

    2:2 means that this circuit is a series 2 pack. It is not backward compatible with any other series.
- Equipment Catalog Item - a 6-character code that identifies each pack type. This code corresponds to the bar-coded label on the faceplate of the pack and is uniquely equivalent to the *CLEI*.
- Circuit Pack Type (Function Code) - a mnemonic name that identifies the general type of function (for example IPFM).

- On ADSL lines, the following ADSL modem inventory information is retrievable on operator command:
  - Vendor ID
  - Version number
  - Serial number.
- On VDSL lines the current modem SW can be retrieved.

Physical data labels

IP APs include the same type of human-readable inventory data label as narrowband packs.

Reportable data base changes

Autonomous notification is provided when changes occur to the inventory database as a result of changes in the physical inventory.

□

IP fault management

Overview

Purpose

Fault management is the system activity for operations that cover the following:

- Maintenance - automatic and manual activities to ensure continued operation and minimize service degradation.
- Alarms - equipment and facility monitoring that results in alarms.
- Protection switching
  - IPFM protection

    Automatic switch from a failing IPFM to a standby IPFM when a fault is detected on the active IPFM
  - Uplink protection

    Automatic switch from the active IPFM to a standby IPFM when a fault is detected on any uplink of the active IPFM
  - 1:1 Pack protection on ICAP
  - 1:N POTS circuit protection
- IP-AFM uplink protection
  Automatic switch from the active IP-AFM to a standby IP-AFM when a fault is detected on any uplink of the active IP-AFM
- Testing - turn-up tests and on-demand circuit testing.

The IP fault management functions are identical for all *AnyMedia*® LAG Shelf configurations of the *AnyMedia*® Access System.

In principle the alarms are also identical for all LAG Shelf configurations. But due to the differently designated slots in the *AnyMedia* LAG shelf types the GSI identifiers are different.

Contents

IP fault management – Maintenance

Overview

Maintenance is the set of activities performed automatically and/or manually to ensure continued operation and to minimize service degradation. This section addresses the following:

- Maintenance objectives
- Maintenance concepts of detection, isolation, reporting and recovery
- Proactive maintenance.

Maintenance objectives

Accurate maintenance can be performed on a system that has been properly installed and provisioned.

Maintenance provides the tools that fulfill the following objectives:

- Detect the majority of all faults in the system.
- Isolate faults accurately to avoid false dispatching.
- Report faults as soon as the faults occur with sufficient supporting information.
- Support proactive maintenance to discover faults before the faults can affect service.

Detection

Detection is the act of determining that a problem exists in the system. A problem can be either permanent or transient in nature. In the system, the detection of these kinds of problems is accomplished in two ways:

- Unit fault detection
  The first and most prevalent way to detect a problem is unit fault detection. Unit fault detection has been designed into most replaceable units in the system and allows the unit to determine its own health, determine the quality of its inputs, and report any malfunctions. Unit fault detection is used mostly for permanent faults, which are reported as alarms.
- Performance management
  The second way to detect a problem, which is more proactive and used primarily for transient conditions, is performance management (PM). PM monitors the data path integrity between system elements. Some transient conditions are immediately reported as events and some are accumulated until they exceed a predetermined threshold, when a threshold crossing alert (TCA) is reported.

Isolation

Isolation is the process of analyzing system alarms, TCAs, events, that have been detected and reported to determine the root cause of the detected conditions in the system.

The goal is to isolate the fault to a replaceable unit. In most cases, the exact location and replaceable unit are known at the time when the fault is detected. Sometimes additional analysis is needed when a detected event is transient or manifests itself with other sympathetic conditions. For example the removal of an AP (or root cause) causes the loss of communications (sympathetic condition) between the IPFM and the AP.

The isolation of transient errors such as TCAs requires an external operations system to perform analysis of additional data.

Reporting

Reporting is the process of communicating the detected system faults or events to a management system. All system alarms and events are reported across the OAM&P interfaces to provisioned destinations. Most system faults or events are reported autonomously as they occur. Some system faults are discovered and reported during routine system operation and surveillance. Most single faults are reported within a few seconds after the faults have been detected.

In addition to alarm and event reporting, local LED indicators on the equipment faceplate indicate equipment faults or status conditions.

Proactive maintenance

Proactive maintenance is the ability to predict or discover a system failure before it becomes service affecting. The system provides the capability to monitor equipment and data paths continuously or periodically.

The system also provides the capability to allow periodic maintenance activity by performing metallic loop testing to monitor the integrity of transmission paths.

□

IP fault management – Voice and signal processing monitoring

Purpose

For maintenance purposes it is possible to monitor the voice and signaling streams on the ICAP and on VoIP APs and to activate system log facility on individual packs.

Monitoring of the voice stream

The voice stream of each port of the VoIP APs and the ICAP can be monitored, but only one port per pack at a given time. Voice monitoring can be enabled in each direction, outbound and inbound, independently and for both directions.

Independently whether the port is enabled for monitoring or not, the operator can retrieve the status of a port. When the port is active, also the codec used for the outgoing packets is shown. When enabled for monitoring, the voice RTP stream is duplicated and sent to/from the monitoring host. UDP port and IP address of the monitoring host have to be provisioned by the operator. The packet receiver itself has to be provided by the *AnyMedia*® Access System customer.

Monitoring and logging of the signaling stream

Monitoring of signaling messages is implemented in the IP subsystem using the syslog protocol, specified in RFC3164 (BSD Log Protocol).

Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. All syslog messages are sent to the server using the UDP port 514 that has been assigned to syslog.

ICAP and VoIP APs provide the possibility to send RFC3164 compliant syslog notifications.

Depending on the pack type (ICAP or VoIP AP) it is possible to activate specific syslog notifications. The installation of the Kiwi Syslog Daemon, which is part of the GSI software delivery, on the local PC is required to enable logging.

Optionally these notifications can also be logged by some other RFC3164 compliant syslog server on a different host than the GSI.

The ICAP allows logs of

- Megaco control protocol
- Protocol errors
- Control events.

The VoIP APs LPZ60x allow

- RTP tracing
- SLIC Log.

A syslog notification has three discernable parts:

- Facility and priority
  The syslog facility is fixed to “local6” while the priority is different per log category, for example “Info”, “Error”, “Notice”.
- Header
  It contains a timestamp and an indication of the hostname or IP address of the VoIP pack.
- Message (MSG)
  It contains some additional information of the process that generated the message, and then the text of the message.

The various options of system logging should be used for diagnostic purposes only. Setting tracing options during normal operation will decrease the overall traffic capacity of the individual pack(s).

□

IP fault management – common faults and failures

Overview

In this context common faults and failures mean faults and failures that do not apply to specific packs or services but may occur on any pack.

Such common faults and failures may be:

- Pack level faults
- Uplink failures towards the IP network
- Uplink failures in configurations that are daisy-chained via IP-AFMs
- Link failures to the protection controller pack (e.g. to the mate IP-AFM)

Pack level faults

Pack level faults are detected at initialization or when the pack faces a severe condition that forces it to reinitialize. Faults which abort the initialization of the pack have a critical severity. They are reported via the console port and via LEDs located at the faceplate of the packs.

Uplink failures

Uplink failures are related to the uplinks towards the IP network. This may be the Ethernet uplinks on the backplane towards the IPFM in IPFM controlled mode) or the uplinks on the faceplate of IP APs (stand-alone mode). Either the uplinks on the backplane or the uplinks on the faceplates of the IP APs in stand-alone mode are active.

Link failures can be caused by:

- Broken link
- Port problem on the pack
- Remote port problem (on IPFM or on network router)
- Any other network problem detected by the pack layer 1 mechanism.

□

IP fault management – Alarms

Alarm types

The IP subsystem alarms appear in an alarm table. In controlled IPFM mode the alarm table resides on the IPFM, in stand-alone mode the alarm table for alarms generated by the AP resides on the AP.

The following are examples of alarm strings defined for the IP subsystem. A table with all alarms currently defined for the IP subsystem is shown in the *Commands and Procedures for IP-based Services*.

- `CPU utilization (%d) reaches its threshold or voip cpu overload`
- `ipfm uplink failure`
- `ipfm software mismatch between active and standby`

Reporting and retrieving alarms

Environmental alarm, the IP subsystem summary alarm as well as pack failure alarms for the *AnyMedia*® LAG Shelves are reported via the OAM&P interfaces for narrowband services.

Additionally, the alarms for IP APs and the IPFM are reported/retrieved via the IP related OAM&P interfaces.

Reporting/retrieving alarms via IP related OAM&P interfaces

The *AnyMedia*® Access System provides consistent alarm/event information over the IP related OAM&P interfaces. The system also supports query for alarms and status conditions over these interfaces. The functions supported over these interfaces include the following:

- Reporting equipment and facility alarms
- Reporting status and transient conditions, including TCAs
- Retrieving currently active equipment and facility alarms
- Retrieving currently active status conditions
- Retrieving alarm/status history report from the IPFM, the ICAP or from stand-alone APs

Reporting alarms via visual indicators

Alarms are also reported via visual indicators:

- LEDs on the faceplates of all APs and IPFM types in the system reflect fault conditions of the pack.
- Additionally LEDs on the faceplates of the IPFM indicate if status conditions or fault conditions are present on the uplinks.

The behavior of the LEDs is described in the *Data Sheet Book*.

□

IP fault management — Protection switching

Overview

Protection switching provides an automatic recovery mechanism when a fault is detected in the system.The protection switching can also be requested manually.

Protection switching is based on the following principles:

- Redundancy of components where components are protected 1:1 (e.g. IPFM)
- Revertive or non revertive switching to protected components
- 1:N protection (e.g. 1:N AP port protection).

The IP subsystem provides protection switching for the following:

- Pack protection (applicable for IPFM, IP-AFM and ICAP)
- Uplink protection (applicable for IPFM, IP-AFM and ESIM)
- 1:N AP port protection for VoIP AP ports.

Redundant components

For 1:1 protected components, one component serves as the active or primary component. The other component serves as a protection or standby component. If the active component fails, the failure is detected, and service is automatically protection switched to the protection component.

Non-revertive protection

Non revertive switching implies that the components do not return to the original configuration prior to the failure. In non revertive switching, a recovered component becomes the new standby component.

□

Pack protection

Pack protection on IPFM and IP-AFM

The IPFM and the IP-AFM support simplex operation mode as well as duplex protection mode. Therefore, in this context whenever the term pack is used, it applies to the IPFM and to the IP-AFM.

The protection mode is provisionable. Simplex operation mode is the default mode.

In simplex mode only one pack is running in the preferred slot. If a second pack is installed in the protection slot then this pack will not activate. When both packs reboot simultaneously, in duplex protection mode the preferred slot becomes active.

It depends on the shelf type and on the pack type which slot is the preferred slot and which one is the protection slot. The table below shows the accordant slot numbers for preferred IPFM slot and for the IPFM protection slot, while the table after that provides the slot numbers for the preferred IP-AFM and for the IP-AFM protection slot.

Shelf/row	Supported regions	Preferred IPFM slot	IPFM protection slot	Additional AP slots ([1])
AnyMedia LAG 1900 Shelf	For international regions only	AP-1	AP-2	AP-2 to AP-14 in simplex mode AP-3 to AP-14 in duplex mode ([2])
AnyMedia LAG 4300 Shelf		AP-25	AP-26	AP-1 to AP-24 AP-26 to AP-43 in simplex mode AP-27 to AP-43 in duplex mode ([3])
AnyMedia LAG 200 Shelf		Not applicable[4]	Not applicable	AP-2 to AP-3
AnyMedia LAG 2300 Shelf	For North America regions (NAR) only	AP-1	AP-2	AP-2 to AP-16 in simplex mode AP-3 to AP-16 in duplex mode ([5])

Notes:

1. The number of the AP slot assumes that IP-based services only are supported.
2. Controlled and stand-alone mode, ICAPs are only supported in slots 3-14. *Do not insert ICAPs into slots 1-2!*.

3. Controlled and stand-alone mode, ICAPs are only supported in slots 1-24, 27-43. *Do not insert ICAPs into slots 25-26!*
4. The IPFM and the AFM/IP-AFM cannot be used in the LAG 200 Shelf, but an ESIM is used in controller mode in slot 1 instead.
5. Controlled and stand-alone mode, ICAPs are only supported in slots 3-16. *Do not insert ICAPs into slots 1-2!*

Note that the preferred IP-AFM slot is the same slot as the preferred AFM slot and the IP-AFM protection slot is also the same as the AFM protection slot.

Shelf/row	Supported regions	Preferred IP-AFM slot	IP-AFM protection slot	Additional AP slots ([1])
AnyMedia LAG 1900 Shelf	For international regions only	AP-3	AP-4	AP-1 to AP-2 AP-5 to AP-14
AnyMedia LAG 4300 Shelf upper row		AP-25	AP-26	AP-27 to AP-43
AnyMedia LAG 4300 Shelf lower row		AP-1	AP-2	AP-3 to AP-24
AnyMedia LAG 200 Shelf		Not applicable[2]	Not applicable	AP-2 to AP-3
AnyMedia ETSI V5 Shelf		AP-16	AP-15	AP-1 to AP-14
AnyMedia LAG 2300 Shelf	For North America regions (NAR) only	AP-1	AP-2	AP-3 to AP-16
AnyMedia FAST Shelf		AP-16	AP-15	AP-1 to AP-14

Notes:

1. The number of the AP slot assumes that the system runs in duplex IP-AFM operation mode and that xDSL-based services via Ethernet uplinks are supported.
2. The IPFM or AFM/IP-AFM cannot be used in the LAG 200 Shelf, but an ESIM is used in controller mode in slot 1 instead.

Pack protection on the IPFM

The active pack does not automatically update the protection pack with provisioning changes. The provisioning information of the protection pack is synchronized only when a ″Save to NVDS″ operation is performed manually by the operator. As a result, if a side switch occurs prior to a save operation, the system will revert to the last saved configuration.

The protection scheme which is used for the duplex IPFM is the 1:1 non revertive protection.

A side switch from an active pack to a protection pack can be of two different types:

- *Unplanned side switch*
  Unplanned side switches are side switches that occur autonomously without any special preparation by the active and protection packs. Events that cause unplanned side switches include software failure, hardware failure or pack removal.
- *Planned side switch*
  Planned side switches are side switches that are jointly and carefully prepared by both the active and protection packs. Events that cause planned side switches include operator command or software upgrade with/without data base evolution.

In the case of the unplanned side switch, the protection pack has to be in the operational state STDBY (standby) or OOS (out of service). In the case of the planned side switch, the protection pack has to be in the operational state STDBY unless the active pack is undergoing software activation. In this case, the reset of the active pack will force a side switch.

The management IP address of the pack is retained when switching sides.

Pack side switching always implies uplink side switching. I.e. uplinks of the former standby pack are used. A “cross configuration” is not possible, i.e., the active pack cannot use uplinks of the standby IPFM.

Note that for pack side switching (fast side switch) the network traffic is down for less than 1 second.

1:1 Pack protection for IP-AFM

The active IP-AFM serves as the common control and feeder interface unit for the *AnyMedia* Access System services to an IP/Ethernet network. When provisioned in duplex 1:1 protection mode, pack protection as well as uplink protection is supported.

Different uplink protection scenarios for the IP-AFM are shown in the section “Uplink protection scenarios — IP-AFM” (p. 3-31).

The active IP-AFM communicates with the standby IP-AFM via the backplane . Both active and standby IP-AFM are continuously monitored. If the active IP-AFM fails, then the fault is detected and the service is automatically protection switched to the standby IP-AFM.

The IP-AFMs can also be switched on demand.

1:1 Pack protection for ICAP

An ICAP can be 1:1 protected by another ICAP in the same protection group with protection being non-revertive.

A protection group is defined as a pair of neighbored slots - an odd numbered one and the next even numbered slot to the right (slot 43 in the LAG 4300 Shelf is the only slot which cannot be protected because there is no further slot to the right). The left slots in these pairs are defined as the preferred slots. As soon as one pack in a protection group is provisioned duplex, the other pack will become duplex automatically.

Up to 8 E1/DS1 links can be connected to both ICAPs via a Y-cable. The ICAPs can be switched automatically and on demand.

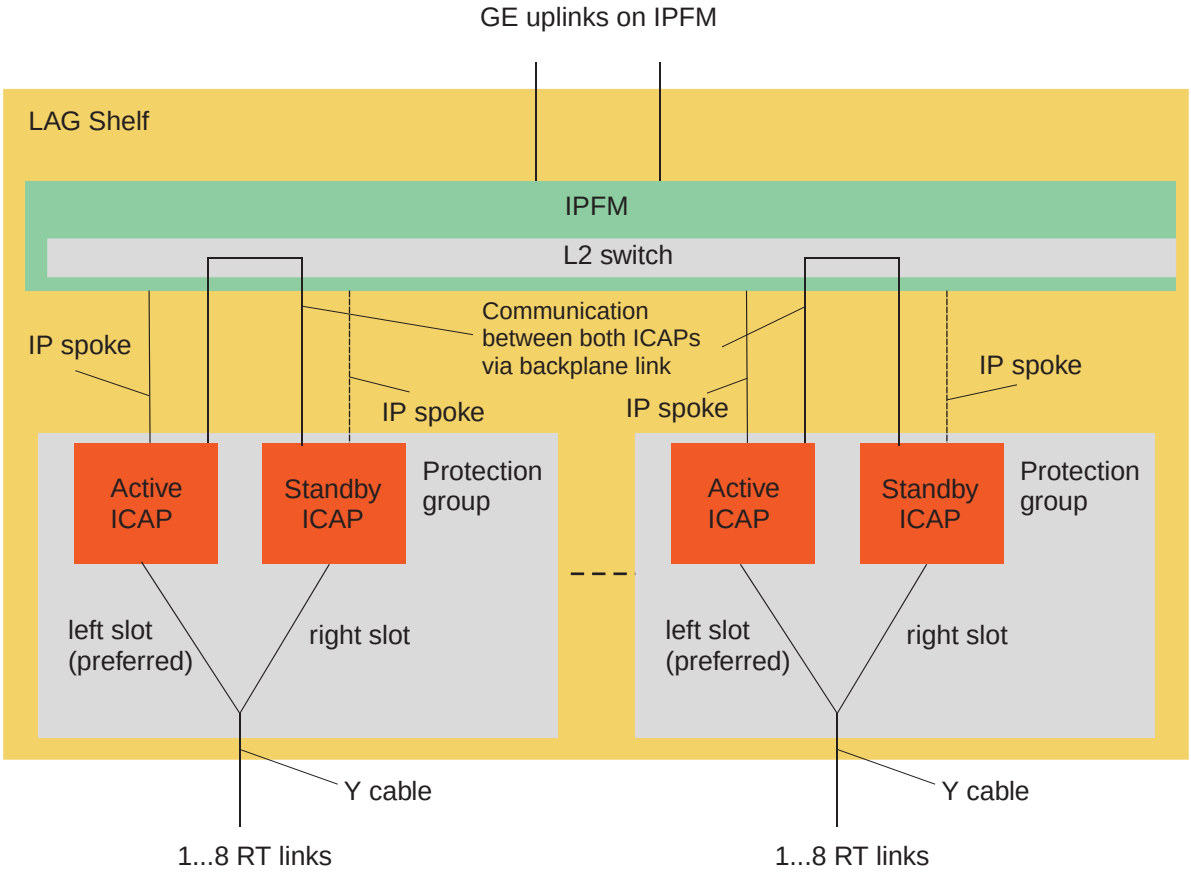
Protected ICAPs need to communicate with each other. This communication is done via a faceplate Ethernet port if the ICAP is operating in stand-alone mode (a bridging faceplate cable is connected to the main input connector of both packs) and via backplane in IPFM controlled mode.

Although the basic protection scheme is similar in stand-alone and in IPFM controlled mode there are some differences:

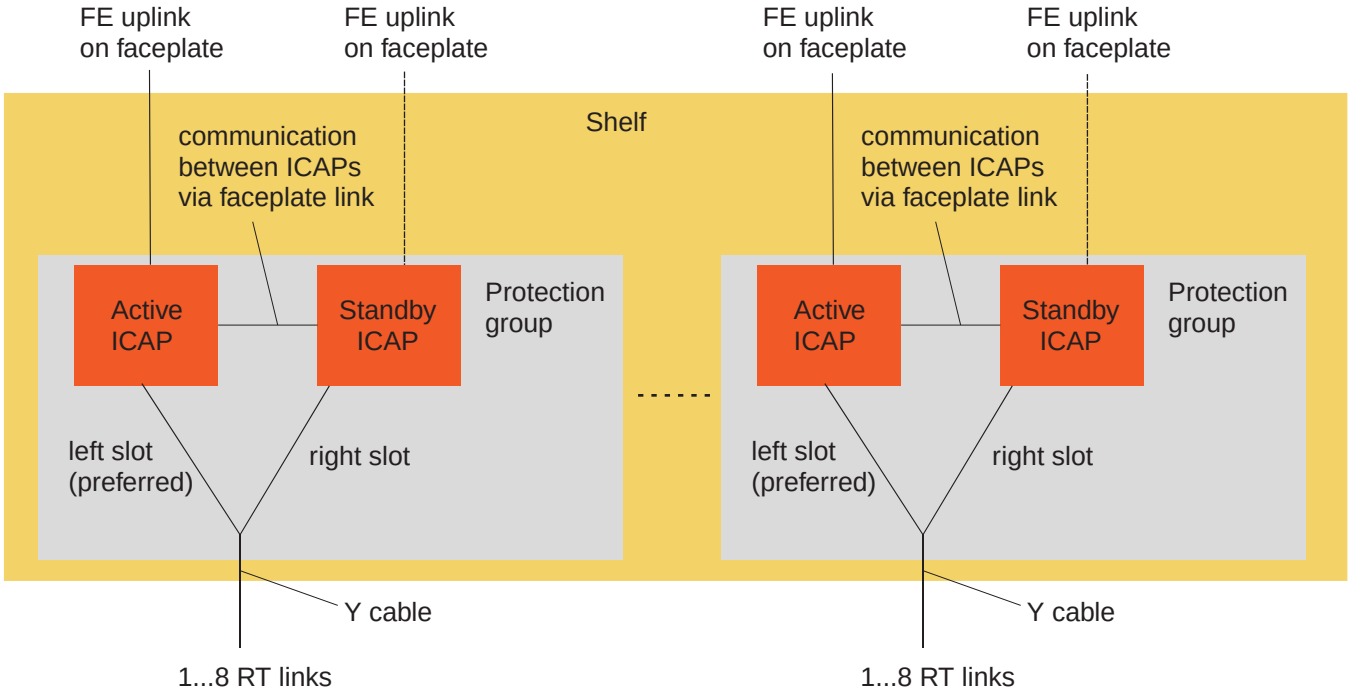
- Stand-alone mode
  - Although a pair of protected ICAPs has two uplinks (one on each ICAP), only one of them can be used at any time. No facility protection of any kind is provided.
  - Only the active pack is managed and visible in the network. The standby pack has all its external interfaces shut off (except the ones to talk to the active pack).
  - In case of a switch over, the newly active pack assumes the identity of the previously active one (IP addresses for service and OAM&P).
- IPFM controlled mode
  - The ICAPs are connected via the IPFM. Therefore any type of facility protection is up to the IPFM.
  - The ICAPs are aggregated via the IPFM. Both packs of a protection group are provisioned as a pair via the identity of the preferred slot.
  - The IPFM stores a configuration file containing the actual database for each slot. In case of a protected ICAP the configuration files for the two slots in a protection group will be identical.
  - In case of an IPFM protection switch the ICAPs will detect a link failure via the backplane spoke, switch to the other one and continue service.

Note that for international regions a non service affecting switch-over is possible, that means no active call will be dropped.

The following figure shows two ICAP protection groups in IPFM controlled mode. In this example the left ICAP in each protection group is in active mode.



The next figure shows two ICAP protection groups in stand-alone mode. In this example the left ICAP in each protection group is in active mode.



Uplink protection

Uplink protection — Overview

Depending on the pack type, the IP subsystem supports different kinds of uplink protection.

The IPFM provides user configurable uplink protection using either

- Link aggregation as defined by IEEE 802.3ad standard or
- Spanning tree protocol (STP) defined by IEEE 802.1d standard or
- Rapid spanning tree protocol (RSTP) defined by IEEE 802.1w standard
- Pack switch if all available uplinks fail
- Uplink layer 1 state (up/down)

Different uplink protection scenarios for the IPFM are shown in the section "Uplink protection scenarios — IPFM" (p. 3-28).

The ESIM provides the same protection capabilities on the downlinks.

Two types of uplink protection are provided by the IP-AFM:

- Rapid spanning tree protocol (RSTP) defined by IEEE 802.1w standard.
- Uplink Layer 1 state (up/down).

The choice of uplink protection depends on the capabilities of the edge router to which the uplinks are connected. Link protection is limited to the links that terminate on the same pack. Links on one pack cannot be used to protect links on the other pack.

Different uplink protection scenarios for the IP-AFM are shown in the section "Uplink protection scenarios — IP-AFM" (p. 3-31).

Uplink protection — Link aggregation

On an IPFM up to two link aggregation groups can be provisioned:

- FE1 and FE2
- GbE1 and GbE2.

On an ESIM, four link aggregation groups are provisionable, the options for the aggregated ports are Port 1 ... Port 8.

When uplinks are aggregated into a single logical link using 802.3ad, maximum usable bandwidth is available to the system when all links are operational. When one link fails, the bandwidth degrades, but transmission is maintained. When the link recovers, bandwidth is increased to 100%. There are 2 to 3 seconds of lost data when a link is lost or recovered.

Uplink protection — (Rapid) Spanning tree protocol

On an IPFM and an IP-AFM any uplink can be configured as spanning tree, on an ESIM additionally ports 1 through 8.

When uplinks are configured using STP or RSTP, one or more links are considered to be a redundant connection and are placed in the blocked state by one of the nodes, that means, no traffic is forwarded to them. When the active link fails, the (rapid) spanning tree protocol unblocks the redundant link(s) and the traffic is restored.

RSTP is mandatory for daisy-chained systems in duplex mode and for applications that require a low transmission outage like video broadcast. RSTP requires proper configuration in the switch equipment.

When RSTP is set on the network switch and the currently active link goes down, RSTP will force the flush of the switch MAC table and floods the unidirectional traffic to the previous standby port.

Unlike the link aggregation failure scenario, STP and RTSP protection will result in traffic disruption until any of the redundant links begins forwarding traffic. This disruption may last up to 30 seconds using STP or about 1 second using RTSP. A 30 second disruption will cause VoIP calls to be dropped (by the subscriber if not by the protocol itself), while a 1 second interruption will likely allow VoIP calls to be maintained.

Uplink protection — Layer 1 state (up/down)

This mechanism is used by IP-AFMs. It relies on the state of the uplink for triggering a side switch operation to reestablish connectivity with network equipment. The active IP-AFM is always the one transmitting subscriber traffic. Whenever the link of the currently active IP-AFM transitions from up to down, a side switch occurs and the previously standby IP-AFM activates its link and reestablishes the connectivity of the system with the network switch.

Typical applications that could employ this option are PPPoE Internet-based services. The traffic for these applications is usually bi-directional, so the network switch will relearn the subscriber MACs as the newly active IP-AFM starts transmission.

Note that this mechanism cannot be used in daisy-chained configurations.

□

Uplink protection scenarios — IPFM

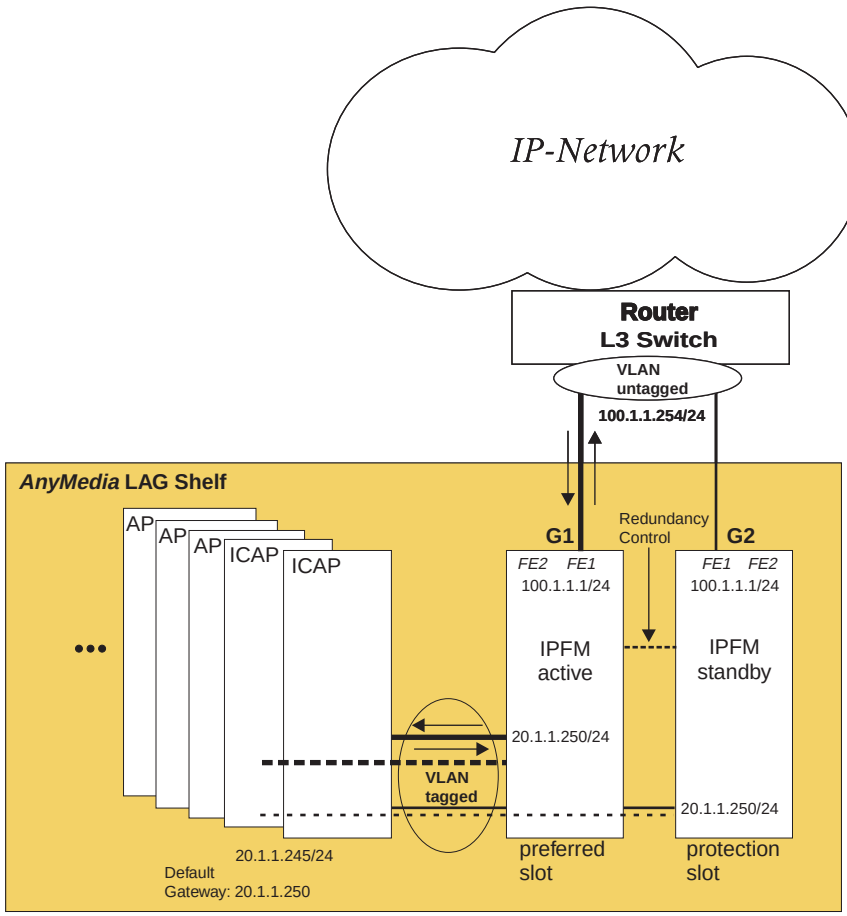
Overview

The uplink protection mechanism is used by IPFMs and relies on the state of the uplink for triggering a side switch operation to reestablish connectivity with network equipment. The active IPFM is always the one transmitting subscriber traffic. From the view point of provisioning the main traffic route should be to the IPFM inserted at preferred slot. The backup route should be to the IPFM inserted at the protection slot.

Whenever the link of the currently active IPFM transitions from **UP** to **Down**, a side switch occurs and the previously standby IPFM activates its link and reestablishes the connectivity of the system with the network switch (e.g. L3 switch).

Redundancy configuration (example) — Layer 3 state (up/down)

In this configuration the IPFM supports the two 10/100Base-Tx Fast Ethernet interfaces (port *FE1* or *FE2*). In this example the *FE1* interface provides the uplink to the IP network. The router (L3 switch) sends the packet via **G1** link to the active IPFM. The redundancy control between active and standby IPFM occurs via backplane. The next figure shows the normal traffic flow in a layer 3 redundancy configuration.



Layer 3 configuration assumption

Layer 3 configuration assumption:

- The link between the router (L3 switch) and IPFM use one of the 10/100Base-Tx Fast Ethernet uplink port (*FE1* or *FE2*) respectively.
- The link **G1** to the preferred slot must be **UP**, then the router (L3 switch) can send the packet to the active IPFM. The **G2** link status is **Down**.
- Router (L3 switch) ports and IPFM(s) ports are part of the same VLAN (untagged VLAN is sufficient for this example) associated with one IP subnet characterized by IP Address and Network mask.
  The Vlan ID *vid1* includes the port connected to the AP. The Vlan ID must match the settings in the L3 VLAN configuration settings (IPFM provisioning).
- Both uplinks (**G1** and **G2**) are provisioned, see example as follows:

  Router (L3 switch)

  – VLAN (untagged)
  VLAN IP: 100.1.1.254/24
  Router port for G1 and G2: IP address 100.1.1.1/24
  Setting for router port **100M-Full** for valid redundancy, no auto-negotiation.

  – IP static route to ICAP (includes ICAP SIG and RTP)
  Destination: 20.1.1.245/24
  Subnet Mask: 255.255.255.0
  Default Gateway (IPFM active/standby): 100.1.1.1

  IPFM(s)

  – VLAN (untagged) for uplinks G1 and G2
  VLAN IP: 100.1.1.1/24

  – VLAN (tagged) for ICAP(s)
  VLAN IP: 20.1.1.250/24

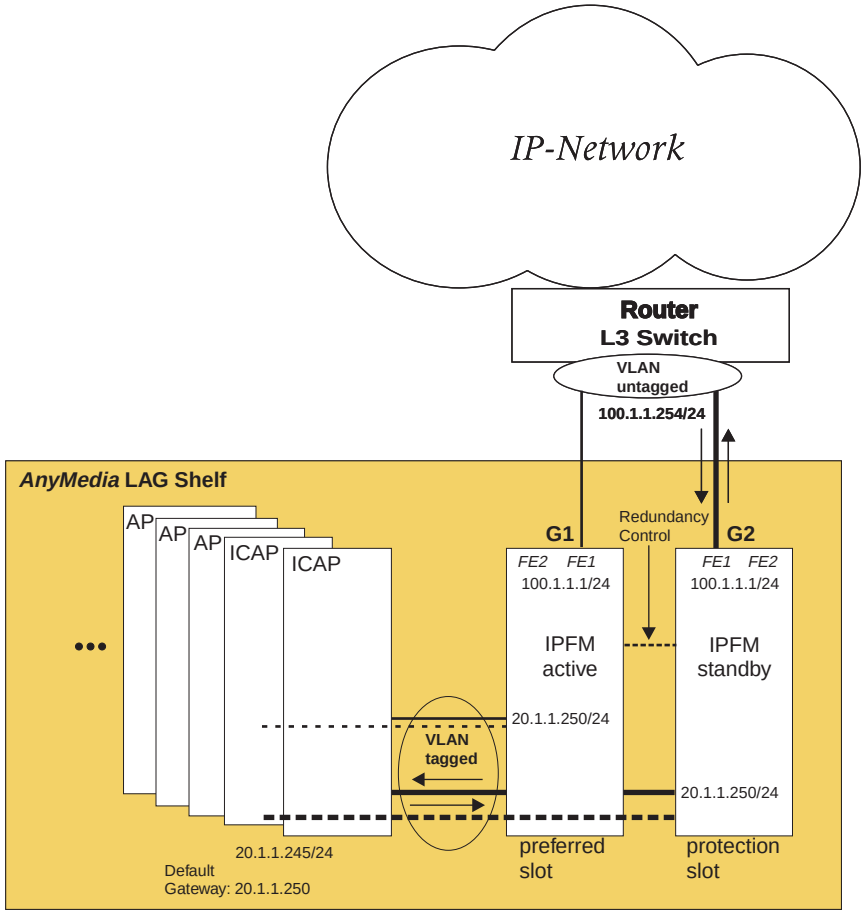
  ICAP(s)

  – Default Gateway to the IPFM: 20.1.1.250

  – IP Address: 20.1.1.245/24

Side switch

The automatic side switch from the active IPFM to a standby IPFM occurs when a fault is detected on any uplink of the active IPFM. The following figure shows the side switch scenario which will react to this fault condition. Other fault conditions are pack failures on the active IPFM.



The uplink G1 goes **Down**.

Note that in case of resetting the IPFM by command or removing the active IPFM, the provisioning scenario is the same as above.

The side switch happens due to uplink protection with the router port setting **100M-Full**. The uplink **G2** goes **Up** and the IPFM in the preferred slot is rebooting.

□

Uplink protection scenarios — IP-AFM

Overview

The ADSL portion of this controller pack is identical to the legacy AFM packs. Therefore, all the subscriber-related fault management capabilities supported by the ATM AFMs are also provided by the IP-AFM.

As the ATM feeder portion of the pack is now terminated internally on the pack, it is no longer monitored by the fault management system.

The IP-AFM fault management features focus on the GbE/FE ports/links used to connect the pack to the network, to daisy-chained shelves and to a mate IP-AFM.

The following scenarios present typical deployment configurations with the IP-AFM and analyze how the system will react to the following fault conditions:

- Network link failures
- Mate IP-AFM and daisy chain link failures
- IP-AFM board failures.

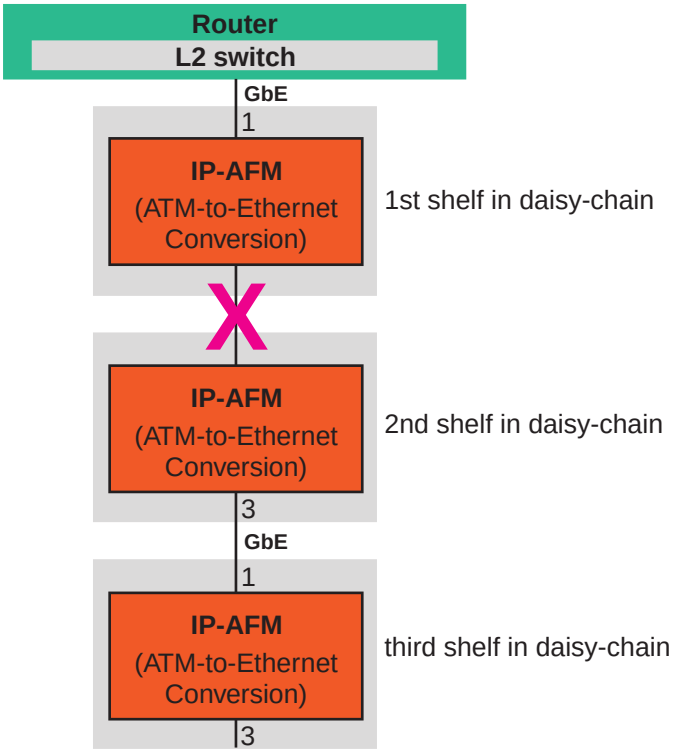
The scenarios presented cover the following IP-AFM deployments:

- Simplex/ daisy-chained configuration without Rapid Spanning Tree Protocol (RSTP)
- Duplex/ daisy-chained configurations using RSTP for dual path protection
- Duplex configuration without RSTP (no daisy-chain).

Background

All the ports used for daisy chain need to be enabled by the administrators. The IP-AFM does not allow the operator to disable the ports used as uplink. This behavior prevents the system from loosing the inband management channel connectivity during maintenance operations. For provisioning the Ethernet ports as uplink, see “Daisy-chain uplink port provisioning” (p. 4-78).

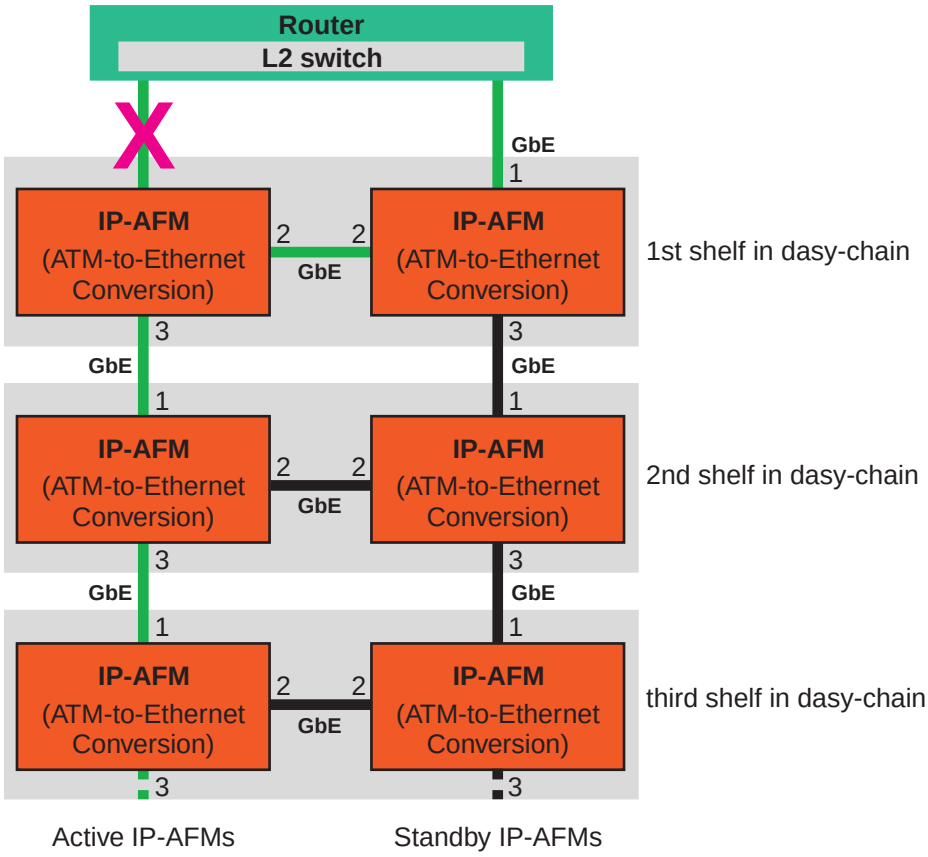
Simplex/ daisy-chained configuration



In simplex deployments the RSTP protocol machine is turned off since there are no alternative paths to search for in case of failures and RSTP operation would block traffic from daisy-chained shelves connected to an IP-AFM recovering from a pack failure.

The traffic from daisy-chained shelves is not affected by the reset of an IP-AFM pack since the layer 2 device controlling the face plate ports will be kept alive during a pack recovery process.

Duplex/ daisy-chained configurations with RSTP

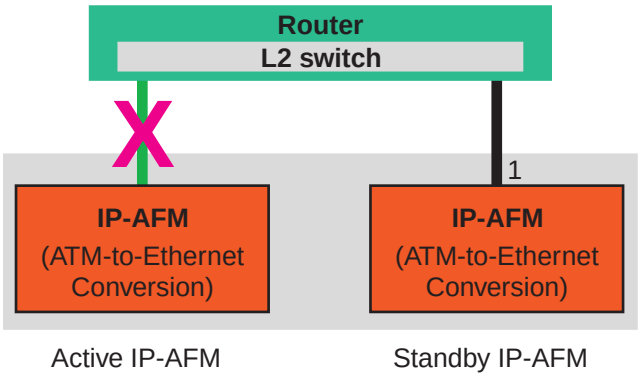


Link failures and pack problems are handled by the RSTP protocol machines running on each of the participating IP-AFMs. No special fault handling mechanism is required to protect the paths between the packs and the network.

Although RSTP provides alternative paths in case of link failures, the active IP-AFM raises a minor alarm.

In duplex/daisy-chained configurations, the active and standby IP-AFMs are cross-connected by a crossover cable on the faceplate (SFP2). Therefore the path of the subscriber traffic can be bypassed to a standby IP-AFM (see traffic flow path in the figure above).

Duplex configuration without RSTP (no daisy chain)



This deployment is used when the network router/L2 switch does not support the RSTP protocol.

A failure on the uplink of the active IP-AFM causes a side switch in order to allow traffic to flow via the newly active IP-AFM. The side switch occurs only if the link state of the previous standby IP-AFM is active.

A failure on the uplink of the protection IP-AFM is reported to the active IP-AFM which will raise a minor alarm.

IP-AFM processor (circuit) failures

Processor (circuit) failures apply to the dual processor architecture of the IP-AFM. The following failures may occur:

- Communication failures between the host processor and the application software processor.
  The interworking between the two processors is interrupted.
  These failures are considered severe failures since they are either associated with a hardware or with a major software problem. They trigger either a side switch or a recovery of the controller pack.
- Software load mismatch
  These alarms are also issued when the software images running on the host processor and application software processor are not the same. This is a rare situation which can occur only when a new application software image can not be successfully loaded after a reboot of the controller pack. In this case the alarm will be issued to inform the managing system that a new software download operation is required. The pack will revert to the load level before the upgrade and consider this scenario as an upgrade failure.

□

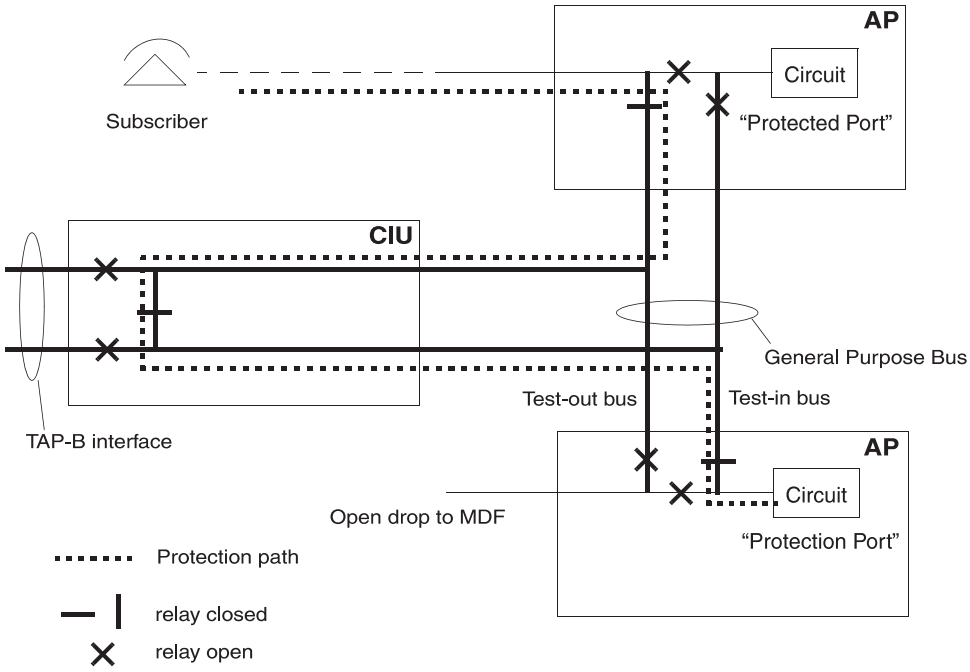
AP port protection and provisioning

AP port protection

By using the metallic test bus architecture of the backplane it is possible to provide a 1:N port protection. The 1:N port protection is supported by the application pack types LPZ600 and LPZ602 for both the port to be protected and the port providing protection (valid for international regions only). The basic concept is to switch a metallic test path from the port to be protected via the general purpose bus on the backplane, via the CIU which inter-connects the outward bus with the inward bus and then again via the general purpose bus to another application pack port which provides the protection circuit. The same metallic infrastructure is used as for TDM AP port protection.

AP port protection requires a COMDAC and a CIU to be present in the *AnyMedia*® Access System and the VoIP AP must be provisioned in the narrowband subsystem.

The figure below shows the metallic protection path for application pack port 1:N protection.



The 1:N protection for application pack ports supports only manual protection switching, that is, on operator demand. It is solely on operators discretion whether to switch a protection for a specific port, probably based on test results from former metallic line tests, circuit tests or due to subscriber complaints.

While a protection switch is active, no metallic line tests involving the test bus are possible in the system. Only pack circuit tests are possible except for the AP where the failed circuit resides and the AP providing the protection circuit.

AP port protection — Provisioning

No automatic subscriber configuration data transfer between protected and protecting port is done at port protection switching. This needs to be done manually by the network operator beforehand.

The following provisioning actions are required:

- Select slot number of the protecting pack.
- Select the port number of the protecting port.
- In the N+1 protection tab select the pack number of the protected pack.
- In the N+1 protection tab select the port number of the protected port.
- Start 1:N protection.

For deactivating 1:N protection, follow the same steps as described above and stop the 1:N protection.

□

IP fault management – Testing

Metallic line testing

Metallic line testing is supported for international regions only and requires the presence of a COMDAC, a CIU and a TAP10x in the shelf. It is currently supported only in international regions by the VoIP AP and by the IPADSL2_32p AP.

Testing is performed under control of the COMDAC via its TL1 interface. Via the UART interface of the AP the COMDAC communicates with the pack and controls its test relays.

The COMDAC sends a test request to the AP, whether a test session can be started. The test request message includes the characteristics of the requested test session like BLOCKED/UNBLOCKED/FORCED, INT/TALK. Once the AP has granted the test request the COMDAC switches the test relays appropriately and controls any subsequent TAP10x measurement. While being in a blocked test session the AP rejects any incoming call on the subscriber under test.

A test session stops, i.e. the AP returns to normal operation of the port, after having received a test request stop message from the COMDAC.

Talk to subscriber

The ″Talk to Subscriber″ feature for international regions basically combines metallic line testing with the possibility to have a conversation between the test center operator and the subscriber at certain points in between tests. As for metallic line testing the presence of a COMDAC, a CIU and a TAP10x is required.

In order to support this feature, a virtual subscriber per VoIP pack has to be provisioned. This virtual subscriber is registered as any other port with a public ″directory number″ at the SIP/H.248 server. It is used to terminate an incoming call of a test center operator. If the COMDAC has established a ″TALK″ session, the VoIP AP switches its test relays accordingly. An incoming call to the virtual subscriber will be switched to the port under test to allow the conversation of the test center operator with the subscriber at the far end. He/she may alert the subscriber using the TST-RINGSGNL TL1 command if the subscriber on the far end is still on-hook. If the COMDAC releases this test session, the VoIP releases the call of the virtual subscriber.

The overall procedure and test session states associated with the ″Talk to Subscriber″ feature are the same as for the existing narrowband system.

During the actual tests the call is put on hold temporarily.

Automatic answering trunk

The IP subsystem is able to provide a virtual subscriber (automatic answering trunk (AAT) subscriber) for responding to incoming test calls. A special number is used to reach the AAT subscriber from any point in the network. This special number must be provisioned on the VoIP AP. The AAT subscriber registers with the SIP proxy as any

other port using the special number. A call to the AAT subscriber comes in via the standard SIP protocol. The AAT subscriber then responds with a 400 Hz stutter tone towards the network (G.711 RTP).

Howler tone on command

Generally, a howler tone can be generated towards a subscriber to make him/her aware of the fact that he/she has not gone on-hook after the termination of a call. Generation of a howler tone may already be part of the call protocol. In this case it is generated by the system autonomously for a limited amount of time.

In addition to this, the operator may apply howler tone on command. I.e., the VoIP AP must provide means to starting, stop and configure the howler tone sending via SNMP. This is supported on a per port level, i.e. there may be multiple howler tones active at a time. The only operator visible configuration item for the howler tone is a timer value which defines the maximum number of seconds the howler tone shall be applied. If set to 0 the howler tone is applied until the line leaves the reduced battery state, or an on-hook is detected or the tone sending is terminated on command by the operator.

Howler tones are customer specific. I.e., the VoIP AP has to store customer-specific sound sample for the howler tone. The selection of the correct sample occurs via the customer key code.

Circuit fault detection

Circuit tests on the VoIP AP are supported for the international regions and performed:

- Whenever the VoIP AP initializes
- When an operator invokes a circuit test.

When the circuit test is invoked via the TL1 interface then the test request has to be granted by the IP subsystem. If granted, the test result is reported at the TL1 command interface, after the circuit test is finished. If a circuit is declared failed by the VoIP AP then the COMDAC raises the circuit fault condition.

□

IP performance management

Overview

Purpose

Performance management is the system activity for collecting and reporting data on the quality of transmission.

In the IP subsystem performance management operation includes:

- Remote monitoring (RMON) according to RFC1757 supported by IPFM, ESIM, ICAP (in stand-alone mode), VDSL AP and IPADSL2+ AP.
- Call statistics supported for H.284 (Megaco).
- VDSL transmission performance monitoring per DSL Forum TR-057, Section 5.
- Provisioning of thresholds via performance management profiles (applicable for VSIM APs).
- Monitoring these thresholds and sending traps if the thresholds are exceeded.
- Downstream IW cross-connection traffic monitoring on IP-AFM (IW stand for ATM-Ethernet interworking)
  Note that the IW cross-connection traffic statistics in the downstream flow will not be supported in R1.29.1.
- IP-AFM Ethernet ports statistics
- ADSL/ADSL2+ transmission performance monitoring
- Upstream/downstream IP packet statistics per IPADSL2+ port.

Performance management in a different sense, that is regarding the performance of the *AnyMedia*® Access System, is collected and reported for the CPU load of the individual packs.

Contents

Remote network monitoring – Ethernet statistics group

Overview

In the IP subsystem remote network monitoring is implemented as Ethernet statistics group according to RFC1757. The Ethernet statistics group contains statistics measured by the probe for each monitored Ethernet interface on the device.

These statistics take the form of free-running counters that start from zero when a valid entry is created. Each entry contains statistics for one Ethernet interface.

In the IP subsystem of the *AnyMedia*® Access System the following items are monitored:

- Drop Events
- Received Packets
- Received Broadcast Packets
- Received Multicast Packets
- Received Packets with CRC Error
- Received Undersized Packets (<64 Bytes)
- Received Oversized Packets (>1516 Bytes)
- Received Fragments
- Received Jabbers
- Collisions
- Received Frames with Size 64 Bytes
- Received Frames with Size 65-127 Bytes
- Received Frames with Size 128-255 Bytes
- Received Frames with Size 256-511 Bytes
- Received Frames with Size 512-1023 Bytes
- Received Frames with Size 1024-1518 Bytes

□

Call statistics on an ICAP AP

Overview

The ICAP provides call statistics on demand. The ICAP collects counts of events for the entire call traffic at a monitoring interval of 5 minutes. There are 288 × 5-minutes register to store the data and one current 5-min register. In total, registers cover a period of 24 hours. The registers are numbered from 3 to 289, and ″Current″ and Previous″ for the most recent complete register and the second most recent complete register respectively.

The following measurement entities are defined:

- H.284 (Megaco) command counters
  - Add
  - Subtract
  - Modify
  - Move
  - Audit
  - ServiceChange
  - Connection loss to the MGC (MgcConnLoss)
  - Invalid *Termination ID*/package (InvTermID)
  - ProtoError
  - Notify
  - TransPendMG2MGC
- Call processing success rate-statistics
  - Successful calls (CollSucc..)
  - Call failures (FailColl..)
  - Premature releases (StableCollFail..)
- Protocol failure counters
- Signaling transport event counters.

□

VDSL performance management

VDSL performance management operation

The VDSL AP supports VDSL transmission performance monitoring per DSL Forum TR-057, Section 5.

For performance management on the VDSL spans, the system continuously collects performance management data internally on a 15-minute interval basis and monitors if the provisioned thresholds are exceeded. Performance management data are collected on the VDSL interface for the following events:

- 15 Min ES (Sec)
- 15 Min LOF (Sec)
- 15 Min LOL (Sec)
- 15 Min SES (Sec)
- 15 Min UAS (Sec)

″Send Init Failure Trap″ can be enabled or disabled..

Once a performance management count exceeds a threshold, an autonomous report is generated. The behavior of the system in such a case, is provisionable (sending of failure traps towards the IP address recorded in the trap receive table, can be enabled or disabled).

VSIM PM profile

The performance management thresholds for the individual performance management (PM) parameters are set via PM profiles. VSIM PM profiles can be used for any number of VDSL ports. They can be modified or deleted, or new profiles can be created as required. Note that the profiles always include a predefined profile that cannot be edited or deleted.

The IP subsystem includes the following predefined PM profile for VDSL ports:

Profile	Default Values
1-DEFVAL	All TCAs disabled (that means, set to zero as shown in the table above)

IP-AFM performance management

Overview

Performance management on the IP-AFM consists of:

- ADSL performance management with the same capabilities as used in the ATM AFMs
- ATM connection traffic management based on capabilities existing on ATM AFMs. In downstream direction additional parameters are provided for monitoring discarded/tagged packets at the Ethernet portion of the IP-AFM.
- RMON like Ethernet ports statistics group on the FE and GbE ports.

Note that the ATM feeder interface statistics of the current AFM does not apply to the IP-AFM, since the ATM feeder is an internal part of the IP-AFM.

Performance monitoring on the Ethernet ports

Performance monitoring on the Ethernet ports is performed via a set of counters according to RFC1757 as described in “Remote network monitoring – Ethernet statistics group” (p. 3-40).

This monitoring applies to the following ports on the IP-AFM:

- Two Fast Ethernet ports (FE1 and FE2).
- Three Gigabit Ethernet ports (GbE1–Network, GbE2–Mate, GbE3–Daisy-chain).

The IP-AFM provides a continuous monitoring mode for these Ethernet ports for a provisionable time period and with a provisionable frequency. The counts are retrievable. The performance monitoring can be enabled or disabled.

□

IPADSL2+ performance management

Overview

Performance management for IPADSL2 services consists of:

- ADSL/ADSL2+ transmission performance monitoring
- IP packet statistics per ADSL2+ port
- ATM bridge port performance management
- Performance management on the GbE faceplate ports.

ADSL/ADSL2+ transmission performance monitoring

ADSL/ADSL2+ transmission performance monitoring between AP and CPE includes:

- Count dying gasp events
- Count received and transmitted ADSL SFs (blocks)
- Count corrected and uncorrected ADSL SFs (blocks).

IP packet statistics per ADSL2+ port

The IP subsystem supports performance monitoring for ADSL 2+ ports by maintaining upstream and downstream IP packet statistics per ADSL2+ port.

ATM bridge port performance management

ATM bridge ports are monitored via a set of statistics associated to the ATM RX (upstream flow) / TX (downstream flow) channels and the ATM<->Ethernet Interworking functions.

Performance management can be enabled / disabled on a per ATM bridge port basis. The statistics comprise 15 minutes and 24-hours counters for the various measurements provided by the layer 2 interworking system. Counters are updated every 15 minutes and 24-hours periods.

Type of statistics	Description
ATM statistics associated to the upstream traffic flow	Number of completed AAL5 frames received
	Number of aborted frames
	Number of frames with CRC errors
	Number of frames with frame size error
	Number of incomplete or discarded frames due to underflow in the receive buffer queue
	Number of received frames discarded due to frame size exceeding the Maximum SDU size
	Number of received frames dropped due to buffer pool overrun
	Number of received framed dropped due to frames size exceeding the maximum receive frame size
	Number of reassembly timeout errors that have occurred
Inter-working statistics associated to the upstream traffic flow	Number of frames discarded by the policing mechanisms
	Number of frames dropped to congestion on the interworking system
	Number of frames dropped to congestion on the transmit queue of the network interface
	Number of bytes forwarded to the network interface
	Number of packets forwarded to the network interface
ATM statistics associated to the downstream traffic flow	Number of completed AAL5 frames transmitted
Interworking statistics associated to the downstream traffic flow	Number of frames discarded by the policing mechanisms
	Number of frames dropped to congestion on the interworking system
	Number of frames dropped to congestion on the transmit queue of the ATM interface (towards subscriber)
	Number of bytes forwarded to the ATM interface (towards subscriber)
	Number of packets forwarded to the network interface (towards subscriber)

Performance management on the GbE faceplate ports

Performance management of the GbE ports on the faceplate of the IPADSL2 AP is performed according to RFC 2819. Currently the EtherStats Group is supported.

Performance management can be enabled/disabled per GbE port.

□

IP security management

Access security

Overview

Security management is the system activity for authentication of a security identifier (ID). Security is provided for the IP related OAM&P interfaces by the security Id on SNMP.

Access security

The system authenticates the security ID before establishing a connection. Once the security ID is authenticated, the user has access to all SNMP commands and GSI capabilities.

The same security ID is used for each of the IP related OAM&P interfaces. A default security ID is installed as a result of IPFM power-up. Any security ID mismatch over these interfaces results in an autonomous message being returned to the message source.

The security ID for an IP related OAM&P interface may be changed at any time following IPFM power-up.

Default login

The default login to the IP subsystem is:

- login: `admin`
- password: `changeme`

□

Filtering/Security management for IP-based services

Overview

There is a variety of well-known possibilities for attacking and tapping the VoIP service including:

- DoS (Denial of service) attacks
- ARP Spoofing
- Man-in-the middle.

Filtering/Security mechanisms

There are several security mechanisms implemented in the *AnyMedia*® Access System to minimize the likeliness of attacks:

- Use of the H.248 Authentication Header (H.248 specific)
- Challenge mechanism using the MD5 algorithm (SIP specific)
- Priority tagging
- Tagged VLAN
- MAC filtering
- Broadcast storm control per VLAN or per pack
- DHCP filtering
- NetBEUI/NBT/NetBIOS filtering.

Authentication header (H.248 specific)

Use of the H.248 AH provides an interim security mechanism as long as IPSec and IPv6 are not supported. Since IPv4 is used, the H.248 Authentication header (AH) is supported.

Corresponding provisionable parameters are:

- Enable/disable AH
- Security parameters index (SPI) field of the AH
- Algorithm to be used in the AH key string.

The mechanism does not provide protection against eavesdropping; thus forbidding third parties from monitoring the connections set up by a given termination. Also, it does not provide protection against replay attacks. However, it provides the identification of the initiator of attacks.

The AH header affords data origin authentication, connectionless integrity and optional anti-replay protection of messages passed between the soft switch and the *AnyMedia*® Access System. The AH header is defined within the H.248 protocol header. The header fields are exactly those of the SPI, sequence number and data fields as defined in RFC2402. The semantics of the header fields are the same as the transport mode of RFC2402, except for the calculation of the integrity check value (ICV). The ICV

calculation is performed across the entire transaction preceded by a synthesized IP header consisting of a 32 bit source IP address, a 32 bit destination address and a 16 bit UDP destination port encoded as 10 hex digits.

Challenge mechanism (SIP specific)

For SIP the challenge mechanism according to RFC3261 is supported, specifically using the MD5 algorithm.

Priority tagging

Voice and signaling packets can be marked on the VoIP AP to be put in high priority queues. This ensures that voice signaling traffic always get precedence over flooding packets of lower priority. The corresponding ToS and 802.1p bits must be provisioned accordingly

Tagged VLAN

A tagged VLAN is used to separate VoIP traffic from other traffic. With the establishment of VLANs, groups of ports can be combined into virtual broadcast domains, isolated from each other. Any packet handled by the system is tightly coupled to an appropriate VLAN tag. So, it is always possible to reliably discriminate traffic into separate and independent domains.

Malicious users often seek to gain access to the management console of a networking device, because if they are successful they can easily alter the network configuration to their advantage. In VLAN-based network architecture, the management connection should be in one dedicated VLAN. VLANs 4093 and 4094 are reserved for internal communication. For the inband management channel a dedicated VLAN can be defined as well. This is highly recommended.

MAC filtering

When an unknown packet is received from a port on a switch, without knowledge of where to forward the packet, it is broadcasted to all ports belonging to the same VLAN. To reduce broadcast traffic and to secure that a host is not moved into another broadcast domain, it is possible to manually assign MAC addresses to VLANs. The *AnyMedia*® Access System supports up to 512 dynamic MAC entries per IPFM or ESIM port or up to 4096 MAC entries per pack. So, the operator can control the access of hosts directly. Also, the operator has to delete the MAC address/VLAN entry if necessary. This prevents the system from autonomously deleting entries via a built-in aging function.

Broadcast storm control

Some IP APs (IPFM, ESIM) allow to configure broadcast storm control per VLAN, for other IP APs (IP-AFM, VSIM AP, IPADSL2 AP) the broadcast storm control can be activated on a per pack basis.

The traffic level where the traffic is blocked for the dedicated VLAN can be set in a range from 16 up to 1048560 pps. A value of 0 means that the broadcast storm control is disabled for this VLAN, independent of whether the global enable/disable function is set to ″enabled″. Up to 64 ″storm control groups″ are supported.

For broadcast storm control activated on pack basis a provisionable threshold specifies the rate (in Mbps), above which the broadcast storm control mechanism will take place.

DHCP filtering

DHCP filtering is provisionable. When enabled, the DHCP responses are accepted from the uplinks while DHCP responses from downlinks are dropped.

NetBIOS/NBT filtering

When NetBIOS/NBT filtering is enabled on the ESIM, all NetBIOS/NBT packets are filtered on both, the uplinks and downlinks, whereas, when enabled on an IP ADSL2+ AP, the packets are filtered only on the subscriber side.

□

4 System planning and engineering for IP-based services

Overview

Purpose

This chapter provides the information necessary to plan and engineer IP-based applications of the *AnyMedia*® Access System.

Note that VoIP is currently supported only in international regions.

Contents

IP related system capacity

System capacity

Overview

This section describes the IP related capacity that means the number of ports in the *AnyMedia*® Access System depending on the LAG Shelf type used and on the AP types.

Number of user ports

The following tables shows the number of supported user ports in the IP subsystem, depending on the LAG Shelf type used and on the AP types. For the calculation it is assumed, that exclusively IP-based services are supported in the shelves and that all AP slots are equipped with APs of the same type.

Shelf types for international regions						
AP type	**LAG 1900 Shelf Number of ports**		**LAG 4300 Shelf Number of ports**		**ETSI V5 Shelf Number of ports**[1]	**LAG 200 Shelf Number of ports**[2]
	Simplex IPFM	**Duplex IPFM**	**Simplex IPFM**	**Duplex IPFM**		
Number of slots for APs	**13**	**12**	**42**	**41**	**16**	**2**
ICAP LPI600 in simplex	24576[3]	24576	83968[3]	83968	32768	-
ICAP LPI600 in duplex	12288[3]	12288	41984[3]	41984	16384	-
VoIP AP LPZ600	416	384	1344	1312	512	32
VoIP AP LPZ602	832	768	2688	2624	-	128
VSIM AP LPV417	208	192	672	656	-	16
IPADSL2_32p AP	416	384	1344	1312	512	64
ESIM LPE408	104	96	336	328	-	8

Notes:

1. Stand-alone mode only.
2. In the LAG 200 Shelf the ESIM in controller mode must always be equipped in slot 1.

3. Both IPFM slots cannot be equipped with ICAPs. Therefore the capacity is the same in simplex and duplex mode.

Shelf types for NAR region			
AP type	**LAG 2300 Shelf Number of ports**		**FAST Shelf Number of ports**[1]
	Simplex IPFM	**Duplex IPFM**	
Number of slots for APs	**15**	**14**	**16**
ICAP LPI600 in simplex	28672[2]	28672	32768
ICAP LPI600 in duplex	14336[2]	14336	16384
VoIP AP LPZ600	-	-	-
VoIP AP LPZ602	960	896	-
VSIM AP LPV417	240	224	-
ESIM LPE408	120	112	-

Notes:

1. Stand-alone mode only.
2. Both IPFM slots cannot be equipped with ICAPs. Therefore the capacity is the same in simplex and duplex mode.

IP-AFM related system capacity

The ATM xDSL capacity of IP-AFM system configurations depends on the different *AnyMedia*® shelf types and is based on the number of ATM xDSL packs installed. The IP-AFM supports:

- Full ATM backplane capacity with up to 622 Mbps total (upstream plus downstream cells) divided as follows:
  - 280 Mbps for the DS direction
  - 280 Mbps for the US direction
  - The remaining bandwidth is used for OAM&P and internal system communication.

  These values are hard-coded and not provisionable by the operator.
- Up to 736 ATM xDSL subscribers depending on an *AnyMedia*® LAG 4300 Shelf type. This subscriber capacity assumes simplex configuration on lower row of the LAG 4300 Shelf and 32-line APs.
- Up to 5500 VCs across all ATM xDSL ports for end-user traffic
- Up to 243 VPs across all ATM xDSL ports for end-user traffic.

ICAP related call capacity

The number of RTP streams is limited within the ICAP depending on the used RTP codec. The maximum number of supported 3-way calls is independent from the used codec but limited to 48. See the following table:

Codec	Channel density per ICAP ([1])
G.711 with RTP encapsulation	512
G711 with App I and II	384
Clear Channel	512
G.726 (16k, 24k, 32k, 40k)	256
G.729AB	256
G.723.1A	192
T.38 Fax Relay	256

Notes:

1. At maximum 240 + 48 = 288 RTP streams may exist within the ICAP. The number 240 derived from the downstream TDM channel capacity.

□

General IP installation recommendations

Overview

Purpose

This section provides general and service independent installation recommendations which have to be considered when planning and engineering the IP subsystem of the *AnyMedia*® Access System .

Contents

Slot numbering and AIDs for the *AnyMedia*® LAG Shelves

Slot designations

The slots which can be used for inserting IPFMs, AFM/IP-AFMs and APs in the different LAG Shelf types are shown in the table below.

Shelf/row	Supported regions	IPFM slots	AFM/IP-AFM slots	AP slots
AnyMedia® LAG 1900 Shelf	For international regions only	1, 2 ([1])	3, 4([2])	2 ([1]) -14
AnyMedia® LAG 4300 Shelf *lower* row		-	1, 2([2])	2([2]) - 24
AnyMedia® LAG 4300 Shelf *upper* row		25, 26 ([3])	25, 26 ([3])	26 ([3]) -43
AnyMedia® LAG 200 Shelf		- ([5])	- ([5])	2, 3
AnyMedia® LAG 2300 Shelf	For North America regions (NAR) only	1, 2 ([1], [4])	1, 2 ([1], [4])	2 ([1]) -16

Notes:

1. In simplex IPFM or AFM/IP-AFM mode slot 2 is usable for an AP, but not for an ICAP.
2. In simplex AFM/IP-AFM mode the slot 4 on LAG 1900 and slot 2 on LAG 4300 lower row is usable for an AP
3. In simplex/duplex IPFM or AFM/IP-AFM mode slot 25/26 is usable for an AP, but not for an ICAP.
4. The LAG 2300 Shelf does not yet support IP-based services via IPFM(s) and simultaneous xDSL-based services via AFM/IP-AFM(s) at the same time.
5. The IPFM or AFM/IP-AFM cannot be used in the LAG 200 Shelf, but an ESIM is used in controller mode in slot 1 instead.

AIDs

A reference list of the access identifiers used for the user interfaces of the different LAG Shelf types is shown in the following table. These AIDs appear only on the GSI and the *Navis*™ *AnyMedia*® Element Management System.

Entity	AIDs on LAG 1900 Shelf	AIDs on LAG 4300 Shelf	AIDs on LAG 2300 Shelf	AIDs on LAG 200 Shelf
Application pack	ap-{1}-{2-14}	ap-{1}-{2-24} ap-{1}-{26-43}	ap-{1}-{2-16}	ap-{1}-{2-3}

Entity	AIDs on LAG 1900 Shelf	AIDs on LAG 4300 Shelf	AIDs on LAG 2300 Shelf	AIDs on LAG 200 Shelf
Port on an AP	ap-{1}-{2-14}-{1-64}	ap-{1}-{2-24}-{1-64} ap-{1}-{26-43}-{1-64}	ap-{1}-{2-16}-{1-64}	ap-{1}-{2-3}-{1-64}
IPFM	ap-{1}-{1-2}	ap-{1}-{25-26}	ap-{1}-{1-2}	Not applicable[1]
AFM/IP-AFM	ap-{1}-{3-4}	ap-{1}-{25-26} ap-{1}-{1-2}	ap-{1}-{1-2}	Not applicable[1]

Notes:

1. The IPFM and the AFM/IP-AFM cannot be used in the LAG 200 Shelf, but an ESIM is used in controller mode in slot 1 instead.

□

Cables and hardware

Associated Hardware

Alcatel-Lucent provides various cables with different lengths and hardware to support IP-based services.

For ordering information see the *Ordering Guide*.

□

Engineering the LAN connection

LAN connection for IP-based services

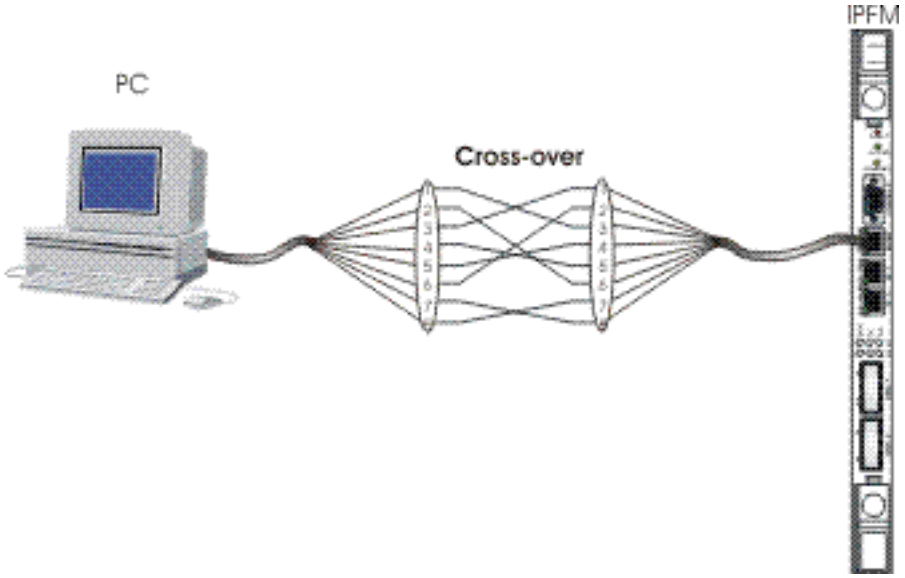
The LAN port for OAM&P is accessed via an RJ-45 connector located on the faceplate of the controller packs or standalone IP APs (except ICAP). This interface can be used for local and remote access.

Configuration options

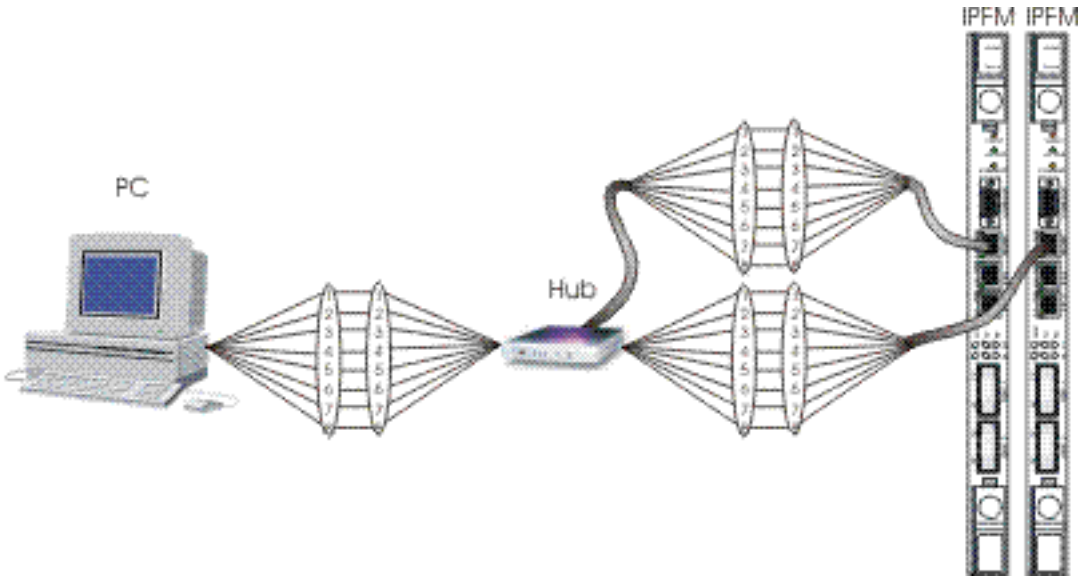
There are two configurations of LAN connections:

- direct connection
- connection through an Ethernet hub.

The example below shows the peer to peer connection with a crossover LAN cable to an IPFM controller pack.



The example below shows the connection via hub with a straight through LAN cable to IPFMs.



When controller packs (for example IPFMs or IP-AFMs) are used in duplex mode on a single shelf, the LAN interfaces are joined at a hub or by a special Y-assembly. In either case, both controller packs use the same IP address.

An alternative for using the Y-assembly in duplex mode is to connect the LAN cable to the active controller pack. In this case, if the controller pack executes a protection switch, the cable has to be moved to the newly active controller pack.

Two examples are given below to illustrate the difference between the two types of cabling.

- Example 1 illustrates the wiring for a crossover cable used with a direct connection.
- Example 2 describes the wiring for a straight-through cable, such as would be used when making a permanent connection between the controller pack and a 10/100BaseT Ethernet hub.

Example 1. Direct connection to controller pack

In this example, a temporary local connection is to be made between a PC/GSI and a single IP controller pack (for example IPFMs or IP-AFMs) in simplex mode to carry out initial turn-up of the *AnyMedia*® LAG Shelf for IP-based services.

A crossover 100BaseT cable is used to connect the 100BaseT RJ-45 LAN port of the PC/GSI to the IPFM RJ-45 faceplate connector.

This is a standard cable and can be ordered from commercial catalogs.

Example 2. LAN connection for IP-based services

In this example, the *AnyMedia*® LAG Shelf turn-up has been completed, and a permanent connection is to be made between a Tier 2 NMS or *Navis*™ *AnyMedia*® Element Management System (NAM) and the IP controller pack. (This example assumes the IPFM is in simplex mode.) To make the permanent connection, the controller pack will be connected to a 100BaseT Ethernet hub.

A straight-through 100BaseT cable with RJ-45 connectors on both ends is used to make this connection. This is a standard cable and can be ordered from commercial catalogs.

Hub connection

The hub functions as a multi-port repeater (that is, it receives and regenerates signals received from any attached device). The hub is transparent to the IP addresses and creates a small star-type local area network of IP systems, ATM xDSL systems, narrowband systems, and the GSI.

□

Inband management via Ethernet uplinks

Overview

Inband management denotes a configuration where the management operating systems use a communication channel embedded in links that also carry user traffic.

The mechanism of the inband management channel allows the management systems (i.e. NAM and GSI) to be located somewhere in the network and to utilize the infrastructure in place for the user data. Among others, this includes routing and protection. The interfaces carrying the inband management channel at the *AnyMedia*® Access System typically are the uplinks. However, subscriber side interfaces can also be setup to get management access.

General inband management configuration

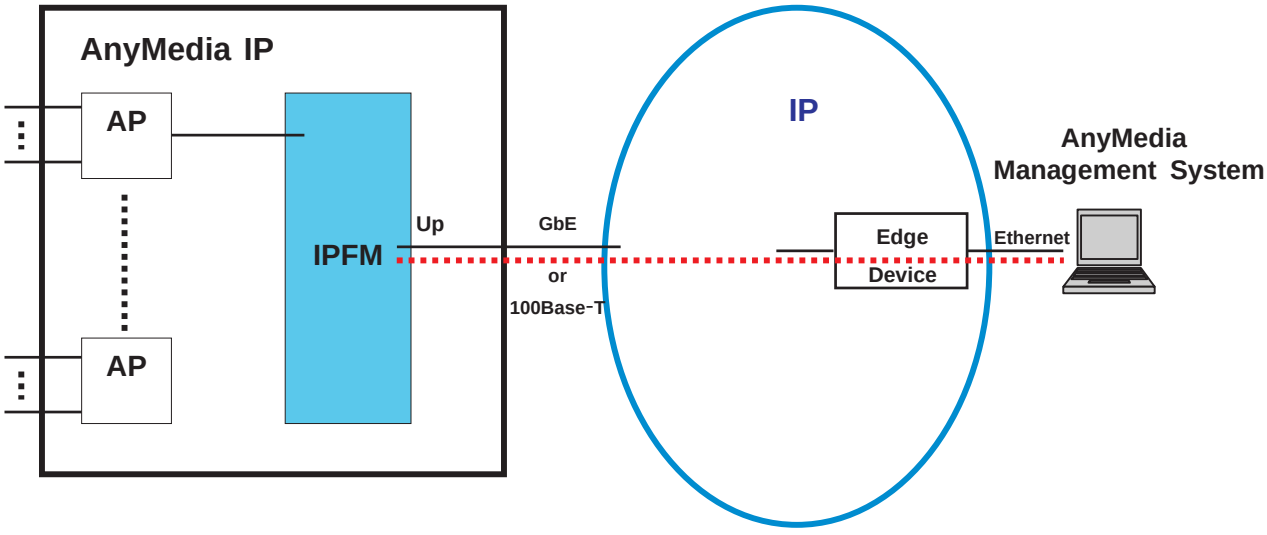
The Ethernet uplinks are used for carrying the inband management channel. The inband management channel is established between the *AnyMedia*® management system and the controller pack (for example IPFM or IP-AFM) where the NE side management information is evaluated for the IP subsystem. At the IP subsystem the inband management channel is terminated on the active controller pack.

The public IP address via which the IP subsystem is reached is retained after a side switch of the controller pack.

For security reasons the inband management channel should be part of a VLAN, in this description called “Management-VLAN”. The Management-VLAN has to be one of the user definable VLANs (VLAN-ID range 1 to 4092). The VLAN-IDs used for IP subsystem internal purposes must not be used for the Management-VLAN.

Inband management channel configuration example

The following example shows the principle of the inband management channel configuration via IPFM.



Inband management channel setup — Management IP network

All devices like switches or routers, which are within the route to/from the management system from/to the IP subsystem, have to be included in the Management-VLAN. The host, which is directly connected to the management operating system, has to tag the IP packets arriving from the management operating system with the VLAN-ID, if not already tagged with this ID by the management operating system itself. In the reverse direction, the tag should be removed because most of the management operating systems cannot handle tagged packets. If more than one *AnyMedia*® IP subsystem is managed remotely by the *AnyMedia*® management operating system all these subsystems have to be in the same Management-VLAN.

□

Time of day handling

Purpose

Consistent time of day must be ensured on the controller packs (for example COMDAC, AFM, IPFM, IP-AFM), NAM and GSI.

Options

There are different mechanisms implemented for the GSI and the NAM and the behavior roughly is as follows:

- On the GSI the operator can select whether to set date and time on the COMDAC and/or on the AFM and/or on the IPFM and/or on all of them.
  For the selected controllers
  - the time can be taken from the underlying PC
  - or a different time can be entered manually.
- The NAM provides the option to synchronize the NEs to the NAM time as soon as the NAM detects a provisionable maximum deviation of the clocks via the time stamps of messages coming from the NE.
  The automatic synchronization can be disabled.

IP subsystem specials

The IP subsystem supports in addition to the mechanism described above network time protocol (NTP). For VoIP pack controlled mode (as opposed to stand-alone mode) NTP support by only the IPFM is required.

If enabled by the operator the IPFM determines time of day via NTP autonomously at regular intervals.

In this mode, the time derived from the NTP server always prevails. Any incoming requests from a management system to change the setting is rejected.

□

Quality of Service provisioning for the IP subsystem

Overview

Purpose

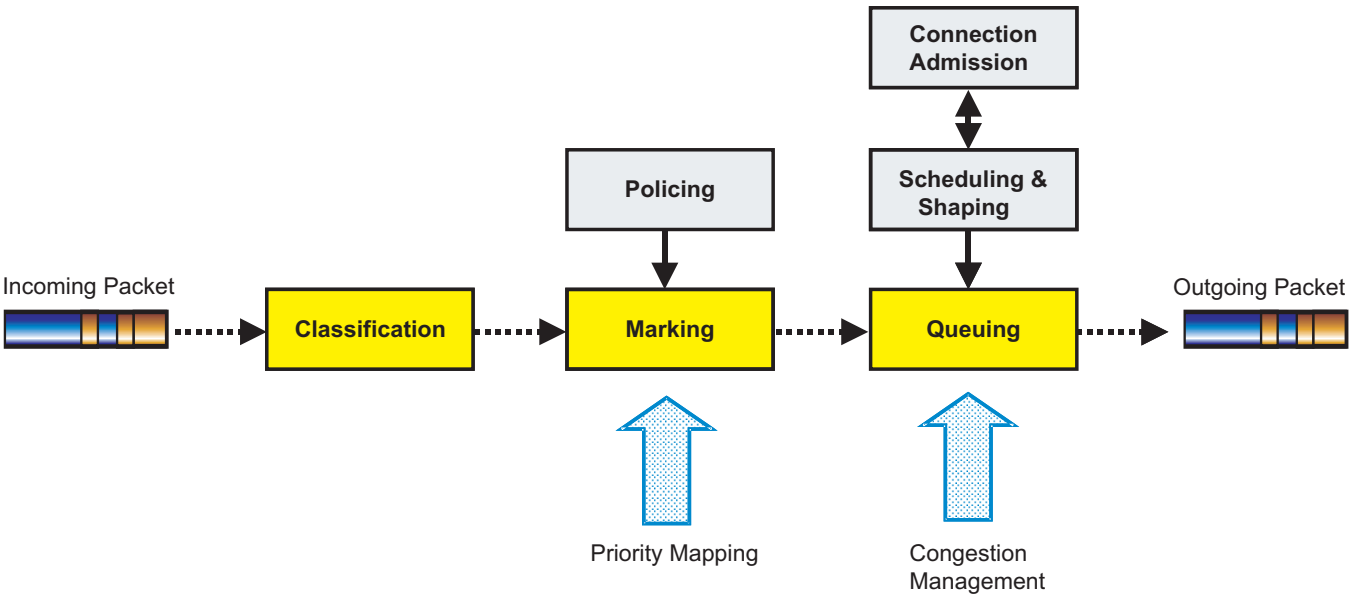
This section provides an overview about quality of service (QoS) functions generally used in IP networks. Then it specifies the QoS functions supported by the IP subsystem of the *AnyMedia*® Access System and discusses the QoS capabilities of the individual IP pack types. Finally it provides recommendations for QoS provisioning.

Contents

QoS functions for IP systems

Overview

The following figure shows schematically which QoS functions may be generally involved in providing quality of service in an IP network.



The individual functions are used to accomplish specific tasks for QoS.

- Classification
  Classification is required at the ingress points of the access network. This function ensures that traffic requiring a preferred treatment is classified in a correct QoS class (service class), i. e. assigning priority to different flows of traffic depending on how critical and delay-sensitive they are.
- Marking
  Packets are marked at the egress point of the system according to the service class at all layers of the protocol stack.
  - 802.1p priority
    L2 priority; eight priorities are supported. The priority information is included in the 802.1Q header field.
  - TOS priority
    L3 priority; according to RFC1349 the TOS service octet is divided into two groups: - the precedence field (bit 0 to 2) is intended to denote the importance or priority of the packet - the TOS field (bit 3 to 6) denotes how the network should make trade-offs between throughput, delay, reliability, and cost.
  - DSCP priority (DiffServ)

The DSCP replaces the TOS bits and retains backward compatibility with the three precedence bits so that non-DiffServ compliant, TOS enabled devices will not conflict with the DSCP mapping. So, the TOS field has new meaning and is re-named as Differentiated Service Code Point (DSCP). The DSCP is 6 bits wide allowing 64 different forwarding behaviors. Service types are defined like Expedited Forwarding (EF), Assured Forwarding (AF1...4) and Best Effort (BE) service.

- Queuing
  Queues are established on each potential congestion point. The number of queues depends on the device capabilities. The queues are read out using the scheduler algorithms.
- Policing
  The traffic policing function ensures that users of a network comply with the traffic profile agreed with the network operator in the service level agreement (SLA). Individual traffic has to be policed in the access network at the upstream link. Policing in downstream direction is normally not needed at the network boundary because traffic shall be delivered according to the SLA.
- Connection admission control (CAC)
  Before establishing a connection, the CAC checks whether bandwidth is available to serve this connection properly. Static and dynamic CAC functions are available. Dynamic CAC is based on control protocols like RSVP.
- Scheduler
  Different scheduling mechanisms can be applied, e.g.:
  - Strict priority
    The queues are served according to a strict priority scheme. The highest priority queue is read out till no more packets are in, then the queue with the next lower priority is served.
  - Weighted round robin (WRR)
    The weights (bandwidths) are defined based on a queue, service class or port. The traffic is transmitted out of a queue till the bandwidth limit is reached or till the queue is empty. Then the next queue is served, also till the bandwidth limit is reached.
- Traffic shaping
  The traffic shaping function limits traffic bursts to a defined level. It introduces delay to the traffic.

Not all IP network devices have to provide all of this functionality. Which functionality is required for a network element depends on e.g. congestion points in the system, the supported service and the IP network architecture.

QoS for voice traffic

It is only needed to differentiate between voice traffic types when a network device may be congested so that in case of congestion, e.g. emergency calls have higher priority than normal calls. Therefore, different service types may be required for voice traffic. In normal case all voice traffic can be handled in the same way.

The VoIP AP can support voice traffic type differentiation for emergency calls when the SIP call control protocol is used.

QoS for video traffic

Video traffic is usually provided by dedicated Internet service providers (ISPs) and will be typically consolidated in one or more VLANs.

The traffic can be classified using the following packet information:

- VLAN ID
- Source/destination IP address (of ISP)
- Packet type (e.g. unicast or multicast).

QoS for data traffic

In this context, data traffic means e.g. file transfer (peer-to-peer traffic) and internet service. Such type of traffic needs very detailed classification, e.g. based on the L4 protocol and protocol port numbers.

QoS provisioning aspects

For providing QoS in an IP network, several provisioning aspects have to be considered in order to minimize congestion and to provision the network elements for a proper packet handling:

- Queuing
  How much queues are supported per access port.
- Scheduling algorithms
  Which scheduling algorithms are supported by the network element
- Policing
  Is it possible to discard traffic which is sent above the SLA.
- Traffic shaping
  Can bursty traffic be shaped so that traffic is not discarded.

□

QoS in the IP subsystem of the *AnyMedia*® Access System

Overview

The IP subsystem of the *AnyMedia*® Access System supports the following QoS functions:

- Classification of the incoming traffic
- Marking of packets
- Bandwidth allocation and scheduling
- Prioritization of this traffic
- Queuing and scheduling.

Later in this chapter it is described which of these QoS functions are supported by the individual IP pack types.

Service classes

The IP subsystem supports four service classes. The service class definition is proprietary. So, the operator is free to evaluate the applications and services and to associate them to separate service classes. Note that the service classes are used only if the scheduler mode has been set to ″WRR″. In scheduler mode ″Strict″ they are not supported.

The service classes (called SC1 through SC4) have no priorities in themselves. That is, the SC1 does not necessarily have higher priority (or lower priority) than the others. However, how the user allocates guaranteed bandwidth to them and if they are assigned to a specific queue will determine the actual priority treatment.

The DiffServ standards (RFC2474/2475) define a per-hop-behavior (PHB), for the communication of the PHB with the other network elements via which a packet is transported. A mapping of the *AnyMedia*® service classes to the DiffServ PHBs may be helpful when connected to a DiffServ domain. The following table shows an example for a possible service class definition and a mapping to DiffServ PHBs:

Description	low latency, low loss, low jitter, mission critical traffic	low latency, general data services	delay tolerant, non-real-time application	best effort application
Traffic Type	VoIP, signaling traffic	VoD, distributed gaming	OAM&P traffic (PM[1], accounting data)	Emails, HTTP traffic
DiffServ Classification	EF[2]	AF1-3[3]	AF4[3]	BE[4]

802.1p	7	5,6	3,4	0,1,2
DiffServ or 802.1p priorities may be assigned to the AnyMedia Service Classes:				
AnyMedia Service Class	SC 1[5]	SC 2[5]	SC 3[5]	SC 4[5]

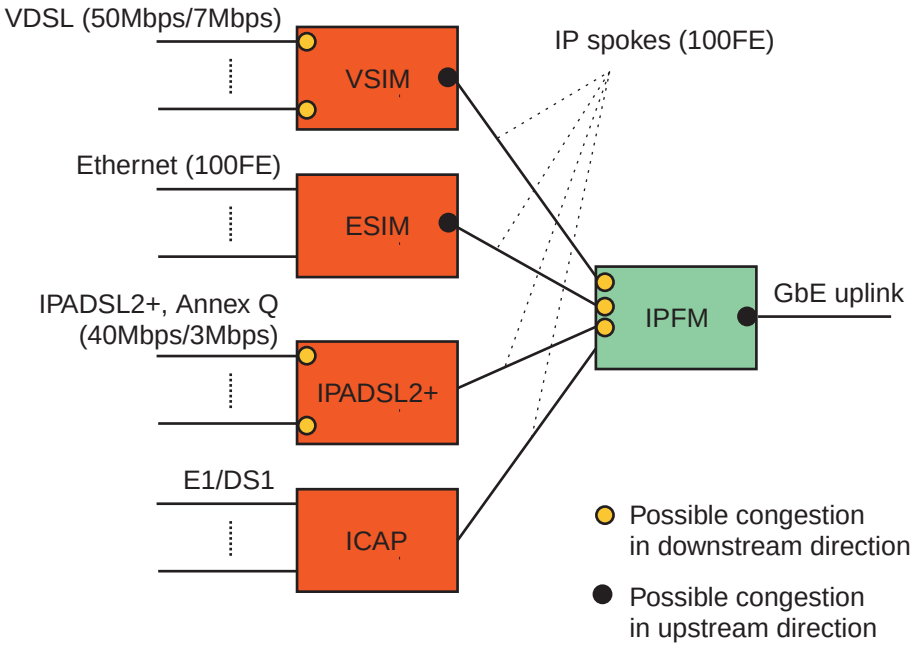
Notes:

1. PM Performance management
2. EF Expedited forwarding PHB
3. AF Assured forwarding group; four independent AF classes with three different discard priorities are defined
4. BE Best effort PHB
5. The service class is provisionable.

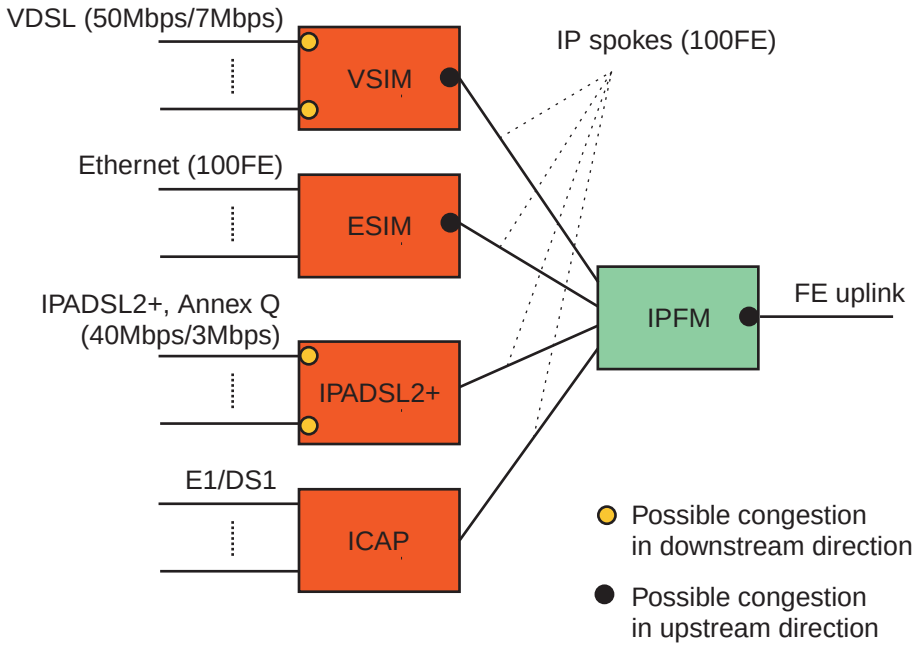
Congestion management

Congestion points are always egress points. At each congestion point buffers are located. In case of congestion, packets are dropped according to a proprietary discard algorithm.

The following figure shows possible congestion points in the system using the GbE uplink.



The next figure shows possible congestion points in the system using an FE uplink.


VDSL (50Mbps/7Mbps)
VSIM
IP spokes (100FE)
Ethernet (100FE)
ESIM
IPFM
FE uplink
IPADSL2+, Annex Q
(40Mbps/3Mbps)
IPADSL2+
E1/DS1
ICAP
Possible congestion
in downstream direction
Possible congestion
in upstream direction

IP controller (IPFM/ESIM) — QoS capabilities

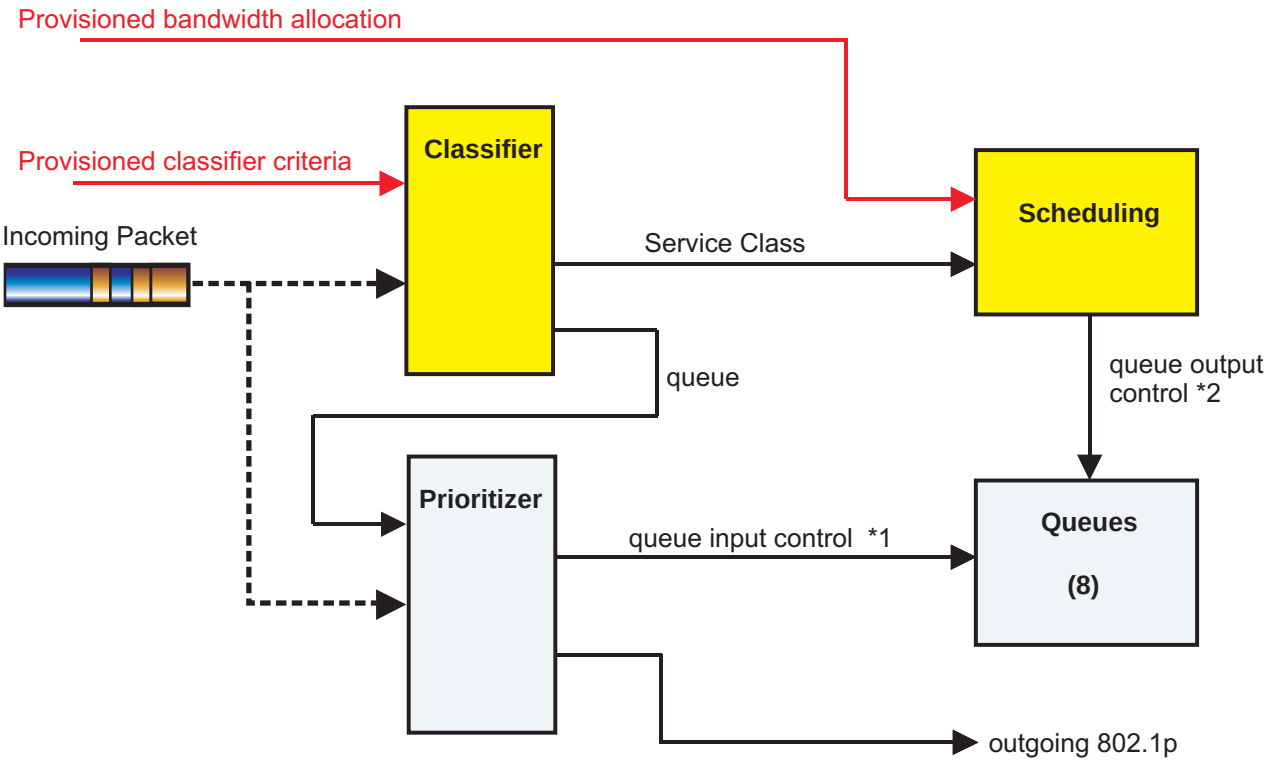
Overview

The IP controller adds enhanced QoS capabilities. To packets arriving at the controller (upstream or downstream direction) the following functions can be applied:

- Classification and marking
  - A service class can be defined to each packet.
    Up to 4 service classes are supported when the scheduling mode is ″WRR″. There is no separate service class allocated for the management traffic.
  - The TOS byte can be re-written (when in DSCP mode).
  - The packet may be dropped.
- Bandwidth allocation and scheduling
  Guaranteed and nominal bandwidths are assigned to the service classes per port and for management traffic.
- Output queuing
  - According to the classifier rules the packets are stored in the eight output queues
  - In case of congestion, packets are dropped by the discard function.

Functional QoS blocks on the IP controller

The following figure shows which functional blocks are provided by the IP controller.



*1 selection in which queue the traffic is stored
*2 queue read-out selection

At the IP controller, traffic is first classified and associated to a service class. Bandwidth is allocated via provisioning to the service classes per port and to the port itself. The prioritizes is used to define which traffic is stored in which of the eight output queues. The read-out of the queues is based on the queue priority and on the guaranteed bandwidth setup in the scheduler. In case of congestion the scheduler evaluates which packets have to be discarded.

Classification and marking

The packet classifier looks into Layer 1 to Layer 4 in the packet data and classifies the packets according to operator definable rules.

The classification is used to:

- Map the packets to up to four different service classes.
- Determine to which internal priority queue a packet shall be assigned.
- Filter traffic by accepting or rejecting packets on a per packet basis.
- Set the TOS bits of the packets to a new value.

The following information can be used to single out any packet:

- Ethernet type (e.g. IP, IPX)
- Packet type (unicast, multicast, broadcast)

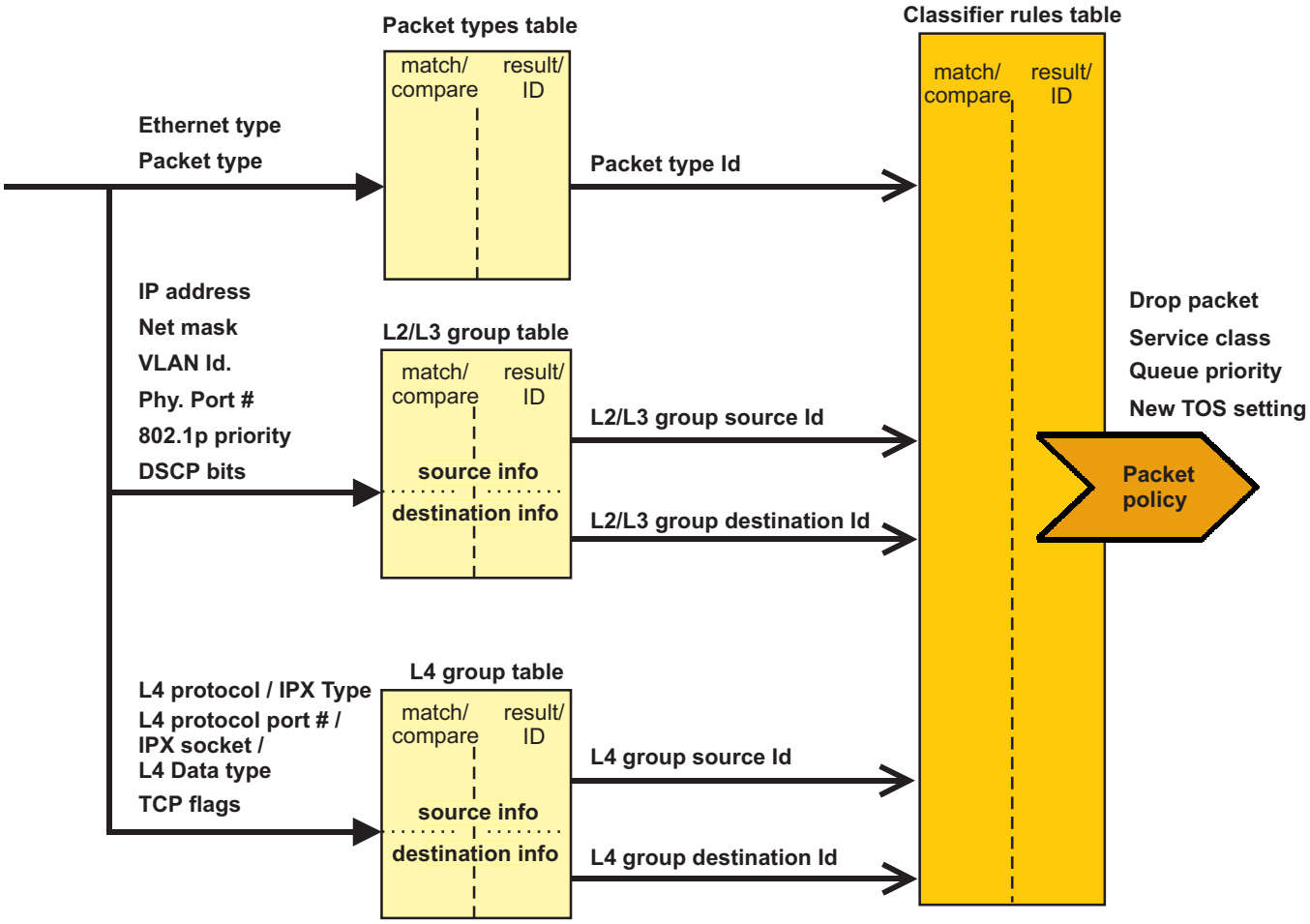
- Network mask
- Source/destination IP address
- Incoming/outgoing VLAN ID
- Data (L4 information)
- TCP flags
- 802.1p bits or DSCP bits
- Source/destination physical port number
- L4 protocol type (e.g. TCP, UDP)
- Protocol port number
- IPX network address
- IPX packet type
- IPX Socket

The classifier function is based on four tables:

- Classifier rules table (max. 512 entries)
- Packet table (max. 64 entries)
- L2/L3 group table (max. 128 entries)
- L4 group table (max. 128 entries)

Important: It is the operator's responsibility to create consistent entries in the classifier tables. When inconsistent table entries are combined in a classifier rule, that rule will not be hit. The end result can be loss of transmission of any lines and can also result in the inability to even communicate with packs in the shelf.

The following figure shows how these tables are used to provision the classifier function.



The packet data is matched against the packet table and twice against the L2/L3 group table and L4 group table, once for the source information and once for the destination information. Each of these tables returns a result value if a hit occurs. These five results, together with a VLAN ID, are then matched twice against the classifier rules table, once for the incoming VLAN ID and once for the outgoing VLAN ID (this applies only to routed packets; for L2 switched packets incoming and outgoing VLAN ID are the same). Action is taken based on the result from the classifier rules table.

Note that the first match in a table is used as result. If more than one entry in a table match, the entry with the lower identifier is used. Because the sequence of the entries cannot be modified by the operator, a careful provisioning of the classifier rules sequence is necessary.

The packet table, L2/L3 group table and the L4 group table can be used for classification independently from the others. Also ″don’t cares″ are allowed in all tables.

Default classifier rules are set to route packets to the CPU (e.g. ARP messages). An additional rule ″catch-all″ is implemented because each packet has to match at least to one table entry.

The packet classification function is used as pure classification and for access control of a packet. The actions which can be defined for a packet handling are:

- Drop a packet
- Accept a packet and
  - define a service class
  - define the output queue in which the packet shall be stored
  - re-write the TOS bits
- Accept a packet and route it to the CPU.
  This action is not provisionable by the operator.

Scheduling

Two scheduling algorithms are supported . The scheduling algorithm can be selected per port.

- Strict priority scheduling (default scheduling type)
  In strict priority scheduling mode the queues are read out sequentially according to their priorities. This means that a high priority queue is read out till no packet is available within this queue. Then the next lower priority queue is read out. No service classes are used in this scheduling mode.
- Weighted round robin scheduling (WRR)
  The IP controller also provides a kind of weighted round robin algorithm.
  The scheduler works on service classes and on output ports. Bandwidth is allocated per service class and per port. The scheduler decides whether to accept or discard packets so that the bandwidth requirements are met.

  Per port the following bandwidth limitation can be provisioned:

  - Maximum bandwidth

    Depending on whether the provisioned maximum bandwidth or the physical port bandwidth is higher, this value is used as ″Max bandwidth″. The sum of all guaranteed bandwidths of all service classes on a port must be less or equal to the ″Max bandwidth″. Note that the bandwidth per port increases when link aggregation is enabled.

  Per service class the following bandwidths can be provisioned per port:

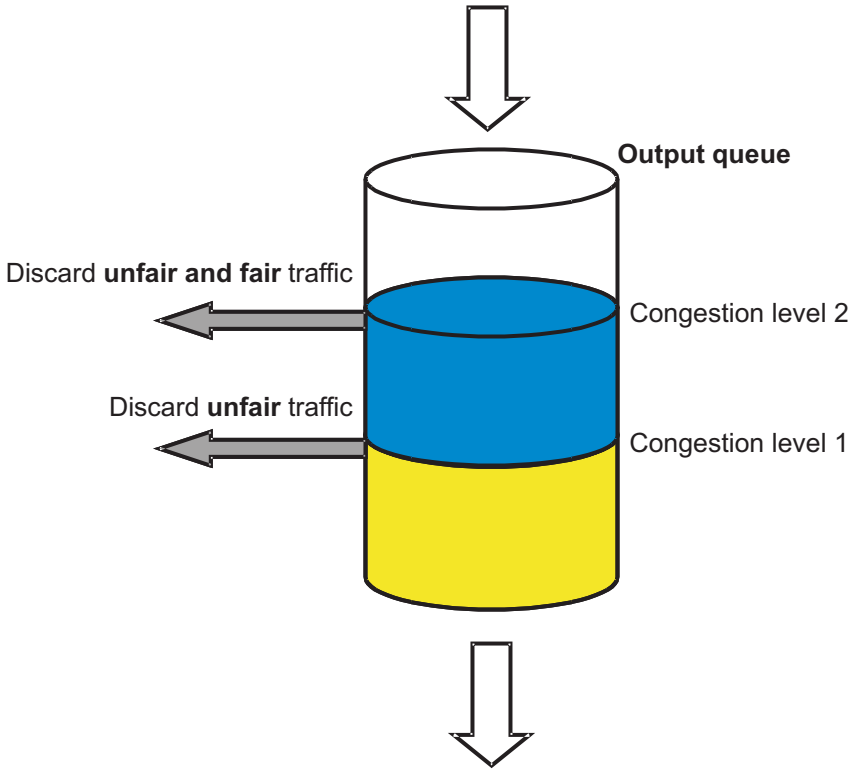
  - Nominal bandwidth

    The nominal bandwidth defines the threshold, after which traffic will be rates as ″unfair″. In case of congestion, unfair traffic will be dropped first.

    Nominal bandwidth should be set to a higher value then the guaranteed bandwidth.
  - Guaranteed bandwidth

    This bandwidth is reserved at the port for this service class. Guaranteed bandwidth is also served during congestion state of the port.

The following figure shows the discard mechanism at an output queue.



The packet handling is based on the following prioritizer rules:

- Output queue and queue priority are strictly mapped (queue 0 has priority 0,…).
- The outgoing 802.1p bits are equal to the incoming 802.1p bits.
- The prioritizer only uses queue priority.
  Therefore it is recommended to mapping high service class priority to high queue priority. Do not assign different service classes to the same queue priority.

Queue priority is determined by:

- Classifier rules table entry (if defined)
- 802.1p bits (if no queue priority is defined)
- TOS/DSCP bits (if no 802.1p bits are available)
- 0 (else).

Queuing

Up to eight queues per port are supported by the IP controller.

Traffic is stored in the queues depending on the priority rules or it may be stored by default in certain queues based upon the content in the packets.

The queue priorities are based on (priority from top to bottom):

- User provisioned queue priority based on rules
- 802.1p bits
- DSCP bits.

The operator must make sure that traffic of a service class is assigned to one dedicated queue, so that in one queue there is no mixture of different service classes. The OAM&P traffic is assigned internally to output queue 7.

□

VoIP AP — QoS capabilities

Overview

The VoIP pack offers QoS on three levels:

- VLAN tagging and 802.1p priority
- IP TOS settings
- Subscriber priority.

The three levels are provisioned independently from each other.

Marking of voice packets

At the VoIP AP the following priorities can be set:

- TOS/DSCP byte
  At the VoIP AP it is possible to set the TOS/DSCP byte for the RTP stream as well as for the control messages via operator command for:
  – Normal calls
  – Emergency calls.
  The TOS/DSCP byte for both call types and both messages (voice, control) can be set independently.
- 802.1p bits for voice traffic.
  Configured 802.1p bits will be set for all packets generated by the VoIP AP.

Traffic management

There is no congestion point on the VoIP AP so that no traffic management function (scheduler, prioritizer etc.) has to be supported.

□

ICAP — QoS capabilities

Overview

The ICAP can operate in two different modes.

- In stand-alone mode the ICAP offers basic QoS on following levels:
  - IP TOS settings
  - VLAN tagging (1 VLAN id) and 802.1p priority
  - 4 user classes

  The three levels above are provisioned independently from each other.
- In controlled mode the IPFM adds enhanced QoS capabilities.

Marking of voice packets

At the ICAP in stand-alone mode the following priorities can be set:

- TOS/DSCP byte

  At the ICAP it is possible to set the TOS/DSCP byte for the RTP stream as well as for the control messages via operator command for:
  - Normal calls
  - Emergency calls.

  The TOS/DSCP byte for both call types and both messages (voice, control) can be set independently.
- 802.1p for voice (normal call, emergency call) traffic (highest priority).
  Configured 802.1p bits will be set for all packets generated by the ICAP.

Traffic management

There is no congestion point on the ICAP so that no traffic management function (scheduler, prioritizer etc.) has to be supported.

□

VSIM AP — QoS capabilities

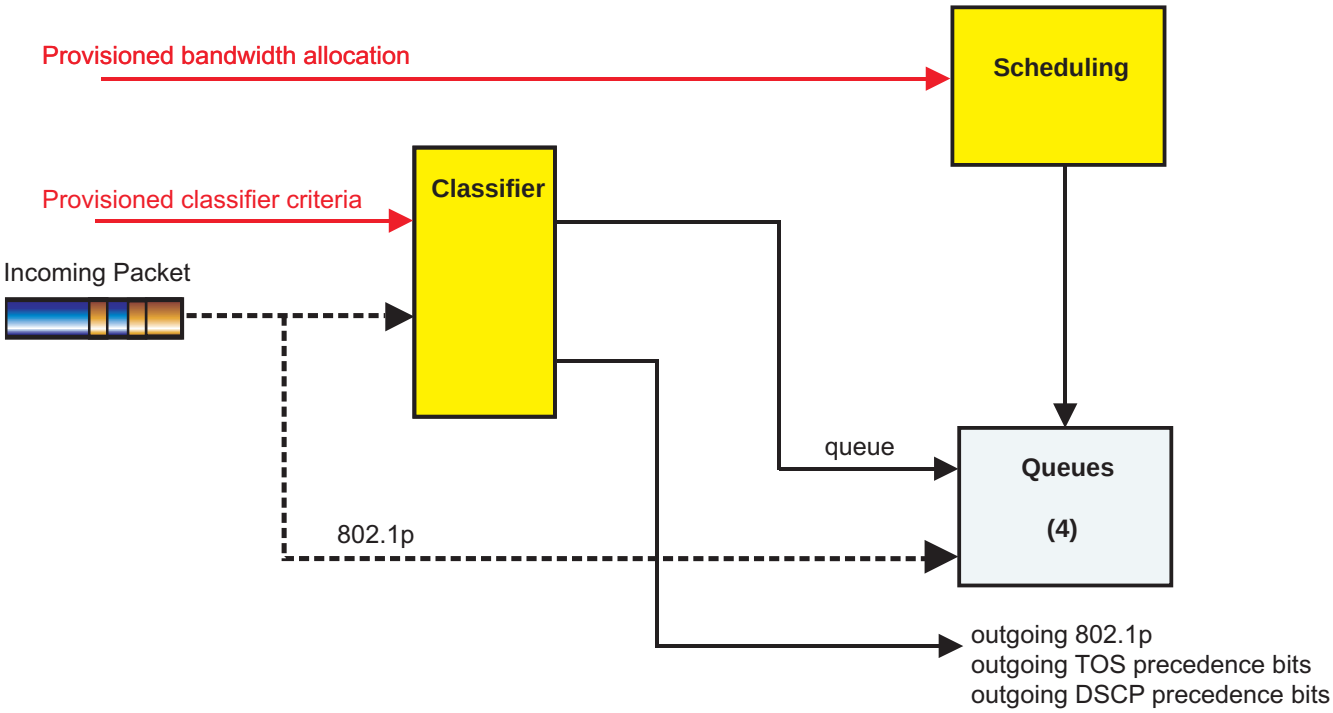
Overview

Similar to the IP controller the VSIM supports the following QoS functions:

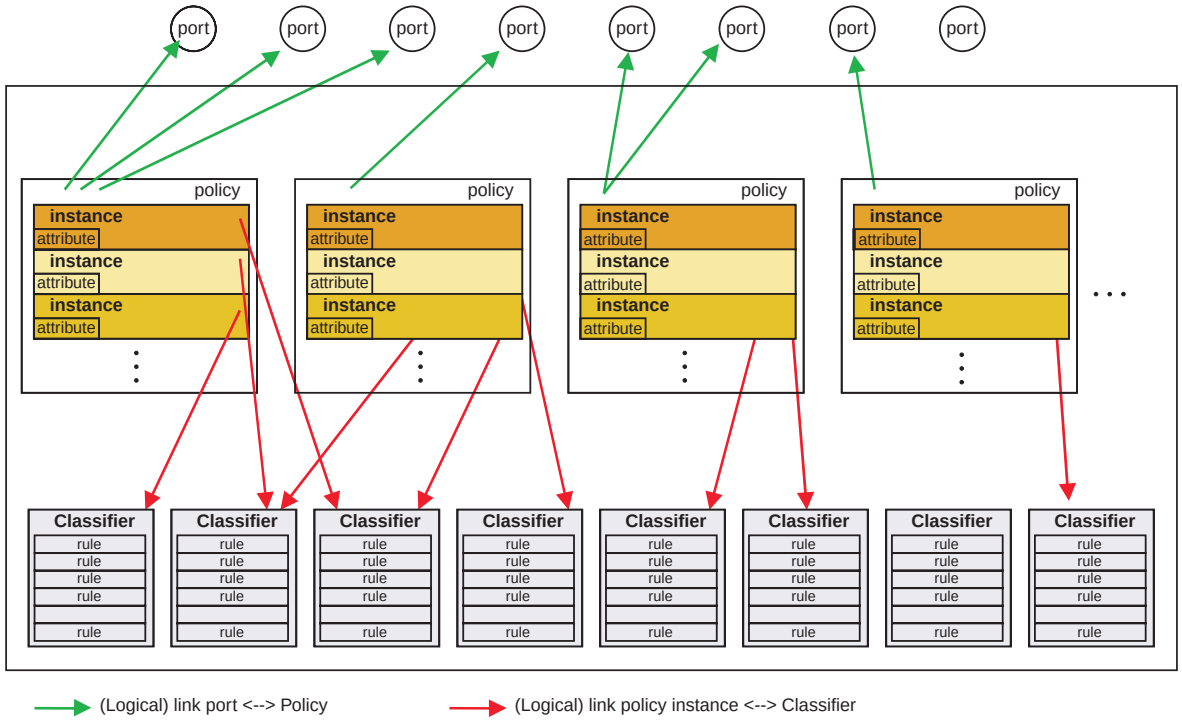
- Classification and marking
- Scheduling
- Queuing.

Functional QoS blocks on the VSIM AP

The following figure shows which functional blocks are provided by the VSIM AP.



Classifier/policy block on VSIM APs (internal logical links)



The classifier/policy block is built of dedicated classifiers and policies.

- There are up to 12 policies
  Each policy:
  - Is identified by a number (automatically assigned) and a user-defined name.
  - Is linked to one or more ports.
  - Contains up to 8 policy instances.

  Each instance:
  - Is identified by a number (automatically assigned)
  - Is linked to a classifier.

  Each policy-attribute:
  - Defines a single action, that will be performed with a packet. Actions could be: output queue to use, discard, redirect, change 802.1Q priority, change IP priority, IP precedence
  - Several actions can be performed with the same packet, but not all combination are allowed.

  Policies cannot share policy instances. If policies should contain identical policy instances, these policy instances must be created in each policy.
- There are up to 8 classifiers.

Each classifier:

– Is identified by a number (automatically assigned) and a user-defined name

– Can be linked to several policy instances.

– Contains up to 6 classifier rules.

Each classifier rule contains a comparison type (and value).

Packets, that match the comparison can be included or excluded. Dependent on this, packets that match or packets that do not match the comparison will then be handled by the policy attributes of the linked policy instance.

Classification and marking

The packet classifier looks into Layer 1 to Layer 4 in the packet data and classifies the packets according to operator definable rules.

The classification is used to:

- Determine to which internal priority queue a packet shall be assigned.
- Filter traffic by accepting or rejecting packets on a per packet basis.
- Set the priority bits (802.1p, TOS precedence, DSCP bits) of the packet new.

The following information can be used to single out any packet:

- Ethernet type
- Source/destination IP address and network mask
- Source/destination MAC address and address mask
- VLAN ID
- 802.1p bits
- TOS bits and match mask
- DSCP bits
- Source/destination physical port number
- L4 protocol number
- L4 protocol port number

Classification of packets is done at the ingress point at the uplinks and the subscriber lines.

A classifier is assigned to a policy instance. A policy is assigned to one or several ports and several policies may be assigned to one port. This means, that via a port packets are transmitted which may be assigned to up to twelve different service types. The policy instance defines in which queues these services are stored.

The packet classification function is used as pure classification and for access control of a packet. The actions which can be defined for a packet handling are:

- Drop a packet
- Accept a packet and route it to another port.

- Accept a packet and
  - define the output queue priority
  - re-write the 802.1p bits
- Re-write the TOS precedence bits
- Re-write the DSCP bits.

Scheduling

At the VSIM two scheduler types are supported which are provisioned per pack:

- Strict priority scheduling
  In strict priority scheduling mode the service classes are read out sequentially according to their priorities. This means that a high priority service class is read out till no packet is available with this service class. Then the next lower service class is read out.
- Weighted round robin scheduling (WRR)
  For each of the four output service classes the weight is provisionable in the range of 0 to 100, in steps of 5. This means that a port (uplink or subscriber port) has in total a value of 400. To calculate a bandwidth, the total port bandwidth has to be divided by 400 and multiplied with the provisioned weight. The service classes are read out sequentially till the allocated bandwidth is transmitted or no more packets are available in the queue. So, also in case of congestion all service classes are served.
  Assigned bandwidth per SC:
  $BW_{SCx} = (BW_{port} \times Weight_{SCx})/(Weight_{SC1}+...+Weight_{SC4})$
  Queues are emptied until the bandwidth limit is reached or the queue is empty.
  This results in:
  - No overbooking
  - All service classes are served even in case of congestion.

  Traffic is discarded on a per packet basis.

Queuing and prioritizer

Four queues are supported at each port of the VSIM.

The packets are stored in the queues according to the following rules:

- Packet is tagged
  The 802.1p queue assignment information is used. The mapping of the 802.1p information to an output queue is done according to the provisioning see also table below. The queue defined by the policy attribute is not regarded in this case!
- Packet is untagged, policy attribute is defined for the packet
  An output queue is defined by the policy attribute. The packets are stored in the output queue provisioned via the policy attribute.
- Packet is untagged, no policy attribute is defined for the packet
  Untagged packets get the port priority assigned. This priority is provisionable and is directly mapped to a specific queue, independent of the priority mapping provisioned in the queue assignment. If the packets should use a certain queue, the priority has to be set accordingly.

The following table shows the default mapping of the 802.1p information to the output queues (applies to tagged packets only). The default queue mapping was implemented according to IEEE 802.1D, Annex H.

802.1p value	Output queue	Traffic type[1]
0	1	Best effort
1	0	Background
2	0	Spare
3	1	Excellent effort
4	2	Controlled load
5	2	Video, < 100 msec latency
6	3	Voice, < 10 msec latency
7	3	Network Control

Notes:

1. Traffic type according to IEEE 802.1D, table H- 15

Provisioning recommendation

The VSIM uses the highest priority queue (which is queue 3) to transport internal management packets.

If user data is given the same priority by placing it into queue 3, it is possible that internal management packets will be discarded due to possible congestion of this queue.

In **strict priority scheduling mode** it is suggested that queue 3 is either not used for any user data to avoid this potential loss of internal management packets.

If this queue is used for user data, you must make sure there is no ability to congest the backplane interface (100 Mb) with user data and that at least 5 Mb (without overhead) is reserved for the management traffic. Thus, the combined upstream traffic rate from all VSDL ports must not exceed 95 Mb with overhead included.

If **WRR scheduling mode** is used, the bandwidth reserved for the highest priority queue must be sufficient for internal management traffic which is bursty in nature. A weight of no less than 5 should be used for queue 3. Again it is still recommended to avoid using queue 3 for user data. If it is used, user data cannot exceed the Queue Weight - 5. Thus, if the Queue 3's Weight = 20, user traffic must not exceed 15 Mb.

□

IP-AFM – QoS capabilities

Overview

Currently the IP-AFM controller pack supports the following QoS functions:

- Packet classification and marking
- ATM QoS

Packet classification and marking

The IP-AFM provides packet classification and marking as follows:

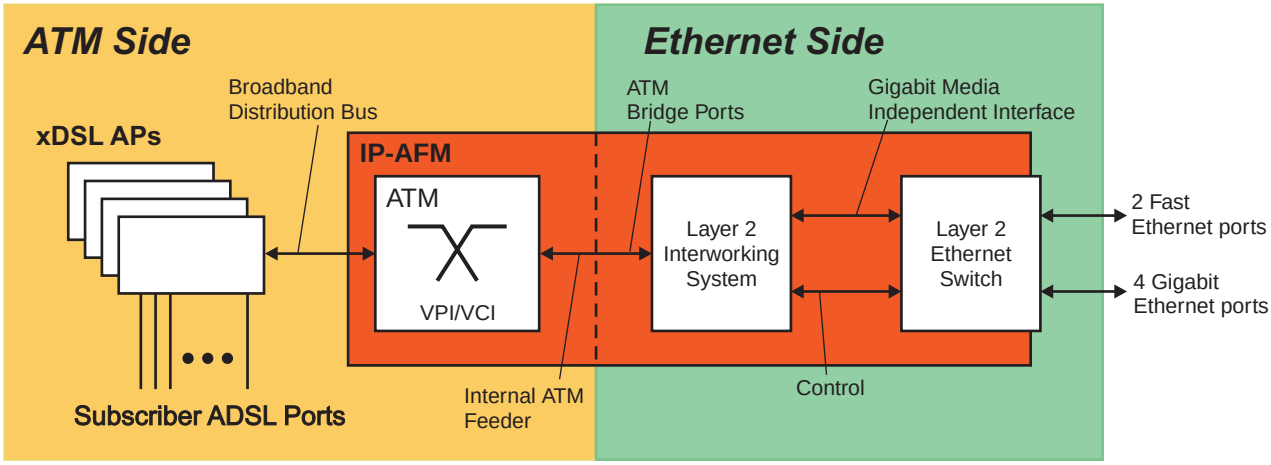
- Packet classification is done by filtering of DHCP/NetBEUI/NBT/NetBios frames specified at the ATM bridge port level.
  The ports can be set to accept or drop packets of the above types ingressing the system via the ATM Bridge Ports.
  Acceptance of tagged or untagged frames.
- Packet marking is limited to the insertion of the 802.1 tag consisting of a VLAN identification and a 3 bits priority field specified at port provisioning time.

ATM QoS

ATM QoS management with 4 service classes is performed on the ATM side of the IP-AFM. It is not required towards the Ethernet side since there are no congestion points in the upstream direction.

- VP/VC assignment
- Connection admission control (CAC)
- Shelf parameter provisioning
- ATM bridge port provisioning – scheduling
- Congestion management in upstream and in downstream direction.

IP-AFM architecture view



VP/VC assignment

The VPI/VCI ranges are:

- ATM internal network feeder (the same as for ATM AFMs):
  - VPI Range: 0 to 255
  - VCI Range: 33 to 9723
- ATM xDSL Distribution
  - VPI Range: 0 to 255
  - VCI Range: 0 to 1023

Downstream and upstream VPs are not applicable anymore to IP-AFMs. VPs/VCs distribution across the xDSL packs is done as in ATM AFMs.

Connection admission control

As in ATM AFMs, connection admission control (CAC) is performed in the upstream direction at the internal feeder interface and in the downstream direction at the subscriber interface. CAC is provisioned for the CBR, rt-VBR and nrt-VBR. The CAC algorithm used is the same as in ATM AFMs.

In the IP-AFM the upstream and downstream bandwidth take into account the total bandwidth of the internal feeder. This bandwidth is hard-coded at 311,25 Mbps (~ 0,7 cells per second) for downstream flow and 281,25 Mbps (~ 0,66 cells per second) for upstream flow.

Remaining bandwidth is reserved for OAM&P inband channel and board internal communication.

Shelf parameter provisioning

The shelf provisioning parameters for ATM QoS are:

- Shelf peak cell rate
  As in ATM AFMs, this parameter specifies the maximum bandwidth in cells per second that a shelf can guarantee. In the IP-AFM, the upper bound for this field is 280 Mbps for downstream and upstream respectively.
- Overbooking factor – remains as in ATM AFM
- Cell loss ratio (CLR) – remains as in ATM AFM
- The definitions for ″Effective Bandwidth″ and ″Admissible Bandwidth″ remain as in the ATM AFMs.

ATM bridge port provisioning – scheduling

In the **upstream direction**, congestion management takes place at the ATM portion of the IP-AFM, see “Congestion management in upstream direction” (p. 4-40). Since the maximum upstream flow is limited to 281,25 Mbps, there is no need for congestion management on the Ethernet side of the IPAFM, when the interface to the network is a Gigabit Ethernet port.

If the uplink port is one of the Fast Ethernet ports (100Base-T), the operator must provision the ATM bridge ports with the proper 802.1 priority bits, see “IP QoS - IP-based congestion management” (p. 4-40).

In **downstream direction**, scheduling is performed based on the 4 transmission queues in the ATM devices associated to each xDSL port. The priority queue is directly mapped from the ATM service category. CBR traffic is assigned to the highest priority followed by rt-VBR, nrt-VBR and UBR.

Congestion management in upstream direction

In the upstream direction congestion management takes place at the ATM portion of the IP-AFM.

The parameters that govern upstream policing are specified in the ATM traffic profile:

- Cell loss priority (CLP) – specifies if the sustainable cell rate (SCR) of rt-VBR/nrt-VBR apply to CLP=0 (compliant cells only) or to CLP0+1 (compliant and noncompliant cells).
- Cell tagging – specifies if nonconformant cells will have the CLP bit set to 1 in order to indicate that the priority of this cell has been downgraded due to violation of the traffic contract.
- AAL5 frame discard – specifies if early packet discard (EPD)/partial packet discard (PPD) must be invoked for this connection.

The existing ATM AFM congestion management schemes are supported at the internal feeder interface using the following non-provisionable thresholds:

- CLP=1 – defines when PPD must be exercised
- EPD – defines when entire AAL5 frames must be discarded
- Maximum Limit – all cells are discarded.

Congestion management in downstream direction

In downstream direction, scheduling is performed based on the 4 transmission queues in the ATM devices associated to each xDSL port. The priority queue is directly mapped from the ATM service category. CBR traffic is assigned to the highest priority followed by rt-VBR, nrt-VBR and UBR.

IP QoS - IP-based congestion management

In the **upstream direction**, the IP-AFM layer 2 Ethernet switch prioritizes the traffic based on the 802.1 priority field. The device supports 4 priority queues, which are mapped to the 802.1 field as indicated below:

- 0, 1 and 2 are mapped to priority queue # 0 (highest priority)
- 3 is mapped to priority queue # 1
- 4 and 5 are mapped to priority queue # 2
- 6 and 7 are mapped to priority queue # 3.

The mapping above is used whenever the IP-AFM uplink port is one of the Fast Ethernet ports (100Base-T).

The congestion management in **downstream direction** is performed based on the ATM service category of the VCC cross-connection associated to the ATM bridge port. The scheduling is done based on a strict priority mechanism, see “ATM bridge port provisioning – scheduling” (p. 4-39)

IPADSL2 AP — QoS capabilities

Overview

The IPADSL2 AP supports the following QoS functions:

- L2-L4 Packet classification and marking
- ATM QoS/ IP QoS with 4 Service Classes

In the **upstream** direction, the IPADSL2 AP is able to mark, via the insertion of the standard 802.1p tag, the priority that the packet will have when handled by the devices that form the customer aggregation network.

In the **downstream** direction, the IPADSL2 AP is able to map the packet into one of the four supported ATM services classes. This mapping is based on the association of the VLAN ID and Destination MAC address to the ATM Bridge Port to which the packet is to be sent.

Packet classification

Packet classification is done based on the following:

- Filtering of DHCP/NetBEUI/NBT/NetBios frames specified at the ATM bridge port level.
  The ports can be set to accept or drop packets of the above types ingressing the system via the ATM Bridge Ports.
- Acceptance of tagged or untagged frames.

Packet marking

Packet marking is limited to the insertion of the 802.1 tag consisting of a VLAN identification and a 3 bits priority field specified at port provisioning time.

Scheduling and congestion management

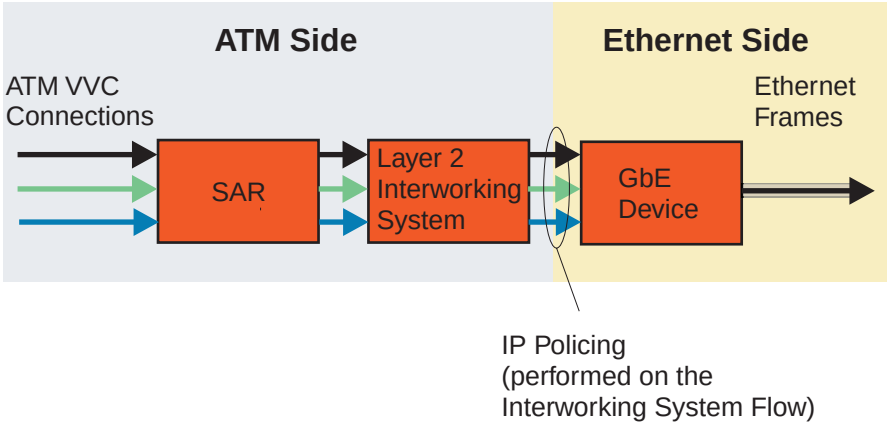
In the **upstream** direction there is no congestion point since the aggregated upstream rate of all the ADSL2+ ports (32 x 3 Mbps = 96 Mbps) does not exceed the capacity of the 100 Mbps / 1 Gbps Ethernet uplink interface of the IPADSL2 AP. For this reason, no traffic scheduling or congestion management mechanism is required in the upstream direction.

In the **downstream** direction, scheduling is performed based on the 4 transmission queues existing in the ATM devices associated to each ADSL2+ port. The operator can specify which transmission priority queue will be used for the downstream traffic of the ATM bridge port when configuring the Traffic Profile associated to the bridge port.

Upstream policing.

In the up-stream direction, IP policing is used. Non-conforming packets are discarded.

Policing in the upstream direction can be enabled/disabled as specified by the operator in the Traffic Profile associated to the ATM Bridge Port.

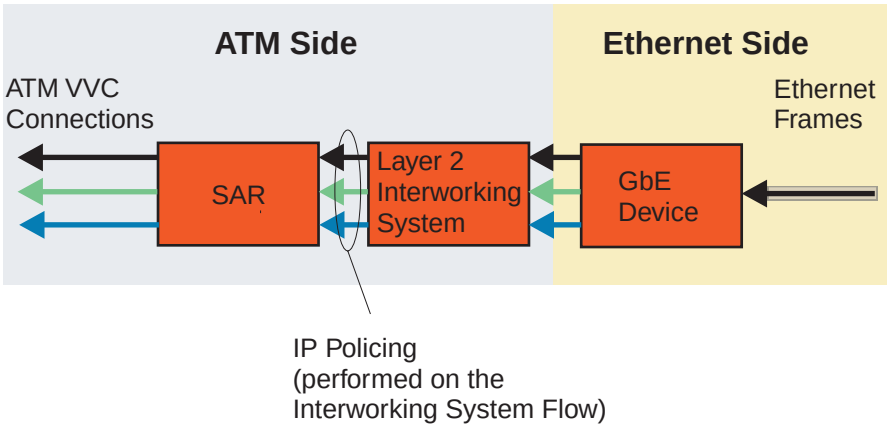


Downstream policing.

In the downstream direction, policing is performed on the flow that points to the ATM Tx channel of the ATM Bridge port.

As in the upstream direction policing, this flow is associated to the ATM bridge port. Policing behavior in the downstream direction can be set to discard non-conforming packets or to set the CLP bit of the corresponding ATM cells.

Policing in the downstream direction can be enabled/disabled as specified by the operator in the Traffic Profile associated to ATM bridge port.



□

General QoS provisioning recommendations

Strategy

For QoS provisioning on the IP subsystem the following is recommended:

1. Assign VoIP traffic to a dedicated VLAN.
   This isolates the traffic from subscriber data traffic and it permits to provision a concise classifier to match VoIP traffic. Otherwise, it is difficult to provision a classifier, because signaling (SIP/H.248) uses a deterministic port #, but RTP packets can be assigned to thousands of port values.
2. The VLAN assignment can be made
   - on the controller with untagged uplinks from the VoIP APs, or
   - on the controller and on the APs using tagged uplinks.

   Both VLAN assignment options are supported. Tagged uplinks permit 802.1p priority to be set on the APs, but this provides no clear advantage.
3. Construct a classifier to match the VoIP VLAN number.
   If SIP signaling is used and it is desired to provide differentiated QoS for emergency services, then provision multiple classifiers to match all combinations of the VoIP VLAN and TOS octet. Also, provision the TOS values on the APs.
4. Assign the classified VoIP traffic to high-priority queues.
   If WRR scheduling is used, then allocate bandwidth for the VoIP service class.
5. Assure that default classifiers are defined for subscriber data packets.
   The subscriber data traffic must be assigned to lower-priority queues than VoIP traffic. Optionally re-mark the subscriber data packets.

□

QoS provisioning recommendations for the management channel

Background

At the congestion points within the system the management channel is treated as any user traffic. This means that the management channel can be ruled out by user traffic. To secure that the management channel is always transported, bandwidth has to be reserved at the congestion points. This is done by setting up the scheduler. The management channel has to be identified using the classifier and assigning the management information to a dedicated service class. Bandwidth can then be assigned to this service class.

The possible congestion points in the system are shown in "Congestion management" (p. 4-22).

Set up the management channel

For setting up the management channel, the following has to be considered:

- Decide whether the management channel has to have the highest priority of all transported traffic or whether it is acceptable that management traffic may be ruled out by user traffic e.g by VoIP traffic.
- If management traffic has to be transported also in congestion state the following steps are required:
  - Set up the classifier (ideally use one of the first ones) for the management traffic packets.
  - Packet classification can be based on e.g. the VLAN Id 4094 which is internally used for management transport.
  - Assign a high priority service class to the management traffic packets.
  - Set up the scheduler.

There are two possibilities to set up the scheduler:

- Weighted round robin scheduling (recommended)
  Provision guaranteed bandwidth for the Service Class to which the management channel is assigned (via the classifier).
- Strict priority scheduling
  When using strict priority scheduling the highest queue priority has to be assigned to the management traffic. All other traffic should be assigned to lower queue priorities to ensure the transport of the management information.

For bandwidth calculations consider the following amount of management traffic:

- For SW image transfer a transmission rate of approximately 1 Mbps shall be reserved.
- Transmission bursts of up to 20 Mbps may occur.
- Manual provisioning, alarm retrieval and configuration retrieval bandwidth is negligible.

□

System turn-up provisioning for the IP subsystem

General system provisioning items

Provision IP packs in the NB subsystem

In order to make use of general system functionality such as LED test or metallic line testing, it is generally recommended to provision all IP packs in the NB subsystem first (not applicable for IP subsystems in a LAG 200 Shelf, because this shelf type does not support an NB subsystem).

The IP APs have to be provisioned in the NB subsystem anyway, in order to use testing capabilities. On the COMDAC the pack level of the IP APs is handled in the same way as for ATM xDSL packs. It is provisioned via the existing TL1 command ENT-AP. Additionally, as for classic POTS APs, 32 POTS drops are auto-created for each provisioned VoIP AP to support metallic line test.

Save to NVDS

Note that all provisioning activities require a manual ″Save to NVDS″ in order to be stored on the NVDS of the IPFM (or to the ESIM in controller mode) and to be transferred to the standby IPFM.

Provision APs for stand-alone mode

By default, stand-alone packs come configured in controlled mode. When required, the controlled mode has to be changed to stand-alone mode during system turn-up.

From the management perspective, the stand-alone AP acts as an individual NE. Therefore, for proper management the following data needs to be provisioned at pack level for stand-alone mode:

- Expected shelf type
- Shelf Id
- Physical slot number
- IP address of the stand-alone pack
- Mask and default gateway or static route for the IP connection to the pack.

□

Initial system turn-up for IPFM

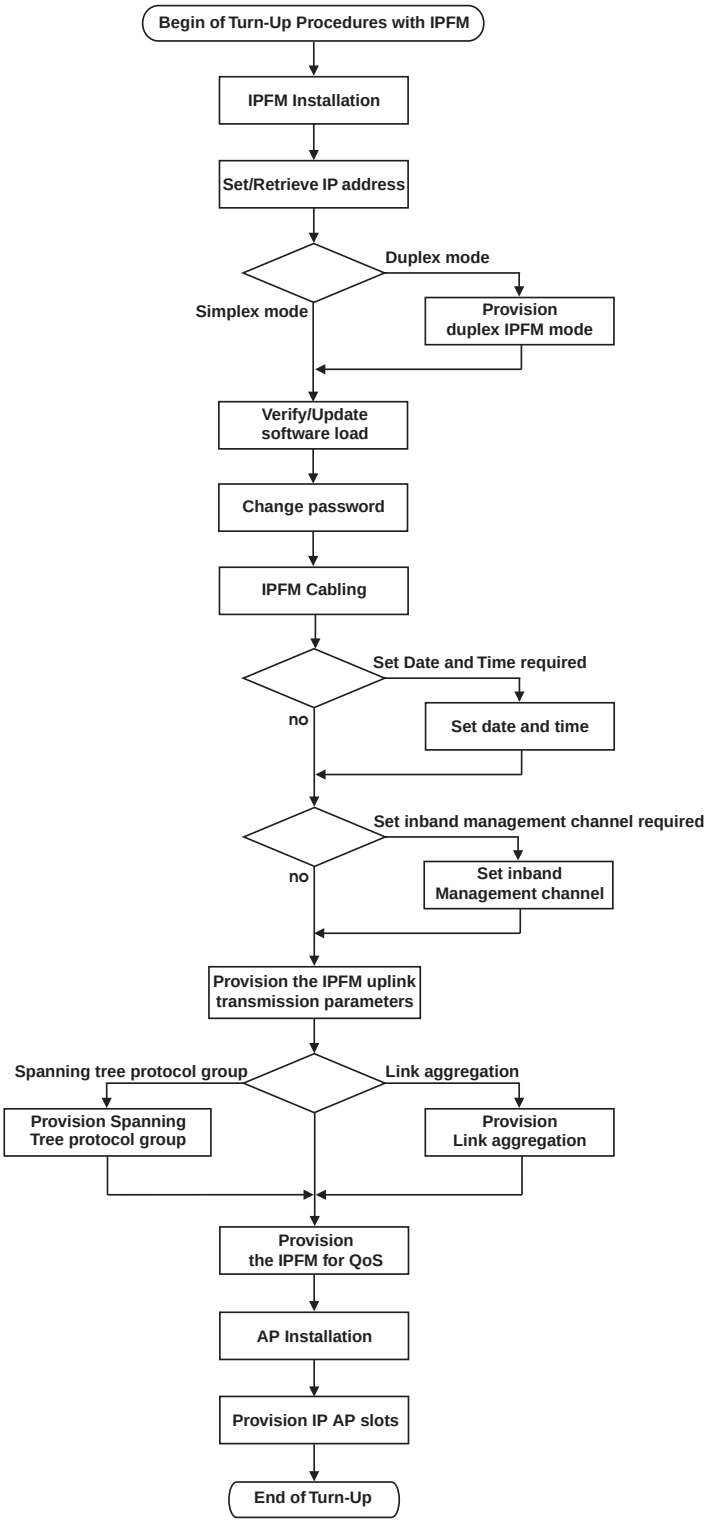
Required procedures

This section describes which procedures are required for the initial system turn-up provisioning for the IPFM and their correct order. These procedures apply to simplex IPFM mode and also to duplex mode. Where a different approach is necessary for simplex and duplex mode, this is reflected in the procedures.

Note that not all of these procedures are required for each system turn-up. Some of them are optional.

The detailed procedure descriptions are provided in the *Commands and Procedures for IP-based Services*.

The following flowchart shows from a high-level view the procedures that are required for an initial system turn-up with the IPFM as controller:


Begin of Turn-Up Procedures with IPFM
IPFM Installation
Set/Retrieve IP address
Duplex mode
Simplex mode
Provision duplex IPFM mode
Verify/Update software load
Change password
IPFM Cabling
Set Date and Time required
no
Set date and time
Set inband management channel required
no
Set inband Management channel
Provision the IPFM uplink transmission parameters
Spanning tree protocol group
Link aggregation
Provision Spanning Tree protocol group
Provision Link aggregation
Provision the IPFM for QoS
AP Installation
Provision IP AP slots
End of Turn-Up

1. Install IPFMs.
   Depending on whether the system will run in simplex or in duplex IPFM mode, install one IPFM in the preferred IPFM slot and one in the IPFM protection slot.
2. Set IP address.
   Set the management IP address via the serial port of the active IPFM (in the preferred slot).
3. Provision duplex IPFM mode (if duplex mode is required)
   If the subsystem is to run in duplex IPFM mode, provision duplex mode and enable IPFM uplink protection if required.
4. Verify/Update software load
   Verify and update, if necessary, the software load for the IPFM.
5. Change password
6. IPFM Cabling
   Insert the appropriate GBIC modules and provide a connection (optical or electrical) from the IPFM to the Ethernet transport network. The IPFM supports two GbE uplinks and two Fast Ethernet FE uplinks. Install the required uplink cables.
7. Set/Retrieve Date and Time
   Set the date and/or the time-of-day either for the COMDAC, or for the AFM or for the IPFM or for all of them. Optionally the time of day can be synchronized to an NTP server.
8. Set inband management channel if required
   Determine an existing VLAN on the IPFM to be used for the inband management channel or define a new one and assign an IP address / subnet mask for that VLAN.
9. Provision the IPFM uplink ports
   Set the IPFM uplinks (up to 4) into service and provision port specific parameters.
10. If link aggregation is required provision link aggregation as defined in IEEE 802.3ad
    It provides downlink protection and increased bandwidth. Link aggregation is applicable to IPFMs. Link aggregation builds up a group of physical ports that act as one single logical link. It is limited to links of the same type and that terminate on the same pack.
11. If spanning tree protocol group is required provision spanning tree protocol group according to IEEE 802.1d standard or a rapid spanning tree protocol (RSTP) group according to IEEE 802.1w standard
    STP and RSTP provide loop prevention and link protection.
12. Provision the IPFM for QoS
    QoS is supported on each port, no matter, whether upstream or downstream.
    This procedure is subdivided in the following subprocedures:
    - Provision/modify the classifier rules
    - Provision the scheduler.

    Note that it is the operator's responsibility to create consistent entries in the classifier tables.

13. Install APs.
14. Provision IP AP slots.

□

Initial system turn-up of the ESIM as controller in the LAG 200 Shelf

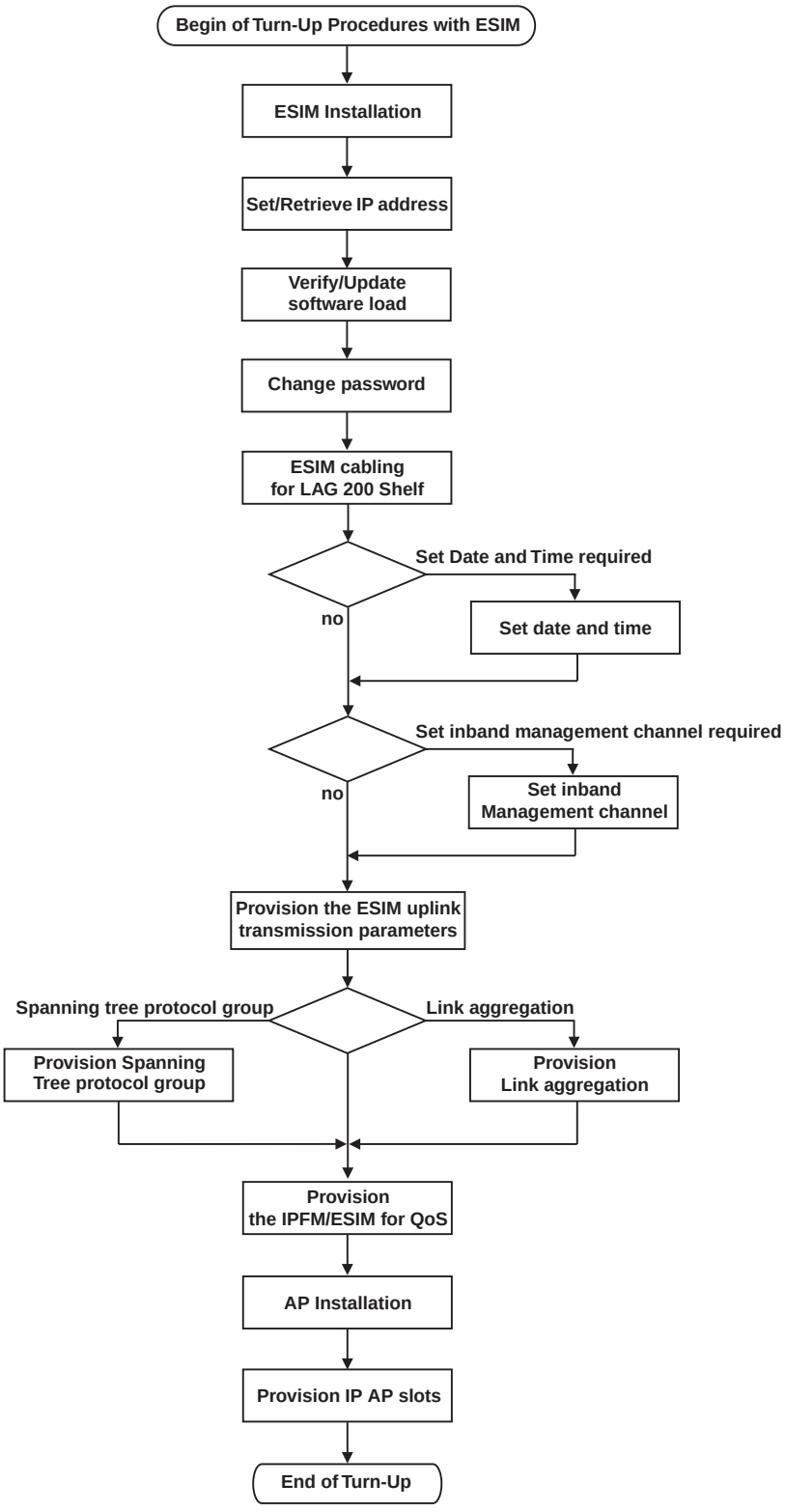
Required procedures

This section describes which procedures are required for the initial system turn-up provisioning for the ESIM used as controller in the LAG 200 Shelf and their correct order.

Note that not all of these procedures are required for each system turn-up. Some of them are optional.

The detailed procedure descriptions are provided in the *Commands and Procedures for IP-based Services*.

The following flowchart shows from a high-level view the procedures that are required for an initial system turn-up with the ESIM as controller in a LAG 200 Shelf:



1. Install ESIM.
2. Set IP address.
   Set the management IP address via the serial port of the ESIM.

3. Verify/Update software load
   Verify and update, if necessary, the software load for the ESIM.
4. Change password
5. ESIM Cabling
   Insert the appropriate SFP modules and provide a connection (optical or electrical) from the ESIM to the Ethernet transport network. The ESIM supports one GbE uplink and eight Fast Ethernet FE ports via SFP modules. Install the required cables.
6. Set/Retrieve Date and Time
7. Set inband management channel if required
   Determine an existing VLAN on the ESIM to be used for the inband management channel or define a new one and assign an IP address / subnet mask for that VLAN.
8. Provision the uplinks/downlink ports
   Set the uplink/downlinks into service and provision port specific parameters.
9. If link aggregation is required provision link aggregation as defined in IEEE 802.3ad
   It provides link protection on the Fast Ethernet links and increased bandwidth. Link aggregation builds up a group of physical ports that act as one single logical link. It is limited to links of the same type and that terminate on the same pack.
10. If spanning tree protocol group is required provision spanning tree protocol group of Fast Ethernet links according to IEEE 802.1d standard or a rapid spanning tree protocol (RSTP) group according to IEEE 802.1w standard
    STP and RSTP provide loop prevention and link protection.
11. Provision the ESIM for QoS
    QoS is supported on each port, no matter, whether upstream or downstream.
    This procedure is subdivided in the following subprocedures:
    - Provision/modify the classifier rules
    - Provision the scheduler.

    Note that it is the operator's responsibility to create consistent entries in the classifier tables.
12. Install APs.
13. Provision IP AP slots.

□

Service activation provisioning for VoIP services

Overview

Purpose

This section describes the provisioning activities which are required after general system turn-up in order to provide VoIP-based services to the subscribers.

Service activation for VoIP comprises of the following:

- Wire the APs
- Provision the pack type
- Provision the VoIP parameters that apply to all ports on the AP
- Provison the individual port parameters.

Contents

Provisionable items for VoIP services — Overview

Introduction

Provisionable items for VoIP services include:

- Pack type
- Port parameters that apply to all ports on an AP in common
- Individual port parameters.

All provisionable items in detail and provide default values and ranges where applicable see *Commands and Procedures for IP-based Services*.

Provision pack parameters

When the pack type for the individual slot has been provisioned on shelf level to the correct pack type (e.g. LPZ600, LPZ602, LPI600), no other parameters have to be provisioned on pack level.

Provision port parameters (for all ports)

Provisioning the port parameters for all ports on a VoIP AP includes the following:

- Parameters on system level, including the customer key code which defines customer specific parameters like control protocol (SIP or H.248 or MGCP), soft switch type, country specific settings, etc.
- Parameters on network level, e.g. pack IP address, gateway, etc.
- Transmission parameters, including the audio codec, jitter buffer size etc.
- Control parameters, including general control parameters, e.g. default digit map, but also SIP or H.248 or MGCP specific control parameters
- Other port parameters, including the administrative state of all ports on the pack
- VLAN Id, priority tag.

Provision port parameters (for individual ports)

Provisioning the port parameters for individual ports on a VoIP AP includes the following:

- Control parameters, including the administrative state
- Physical parameters, e.g. transmit gain, receive gain
- Monitor call status parameters
- *Termination ID* used in H.248 protocol applies only for H.248 VoIP ports provisioning.
  The *Termination ID* is CKC-dependent and combines an interface part parameter with the card and port part parameter (*PortRemPhyCard* value). This triple must be unique across all H.248 VoIP ports.

□

More details on provisionable items for VoIP services

Overview

The following sections provide more detailed information on some provisionable items for VoIP services. These include:

- Customization
- Voice coding and packetization
- Digit analysis
- Signaling parameters (H.248 or SIP or MGCP)
- Direct dialing in multiple numbers
- Call restriction control (provisionable for SIP only)
- Multi-line hunt group function (provisionable for SIP only)
- Call waiting (provisionable for SIP only)
- Provisioning of a protection port

□

Customization

Overview

In a POTS VoIP environment not only substantial customer-specific but also softswitch specific variations are expected. The notion of customer key codes (CKC) as traditionally applied for international V5 applications is similarly used to control the above variations in the VoIP world.

Via the CKC the following categories of parameters will be controlled:

- POTS (similar to V5 applications)
- SIP control behavior
- H.248 control behavior
- MGCP control behavior.

The POTS VoIP allows to either run SIP or H.248 or MGCP on the pack. However, there are many parameters being specific for SIP or for H.248 or MGCP, respectively. The GSI automatically adapts to the signaling used: i.e., it provides only provisioning options applying to the signaling used.

Pack audit and alarming within H.248 (Megaco) protocol

The pack audit and alarming functionality is based on the capability of the H.248 protocol to support wildcarding and/or assignment associated with H.248 *Termination ID* addressing.

- The pack audit functionality is implemented via a *Termination ID* wildcard request from the media gateway controller (MGC) to the media gateway (MG) for the service state information of a set of VoIP subscriber lines.
  The pack audit is supported by all H.248 subscribers.
- The pack alarming functionality is realized via a service state change message sent from the MG to the MGC by using wildcarding for the *Termination ID* parameter identifying a set of subscriber lines.
  The pack alarming is controlled via CKC setting and is supported only in ICAP configurations working together with the proprietary remote terminal (RT) signaling and control interface via E1 links.
  The *AnyMedia* RTs will forward pack status information to the ICAP in the *AnyMedia* host terminal for stimulating the wildcard service state change messages towards the MGC.

The pack audit and alarming functionality may be supported by a structured hierarchical *Termination ID* parameter structure that is defined to be used between the MG and the MGC (depending on customer specification and/or MGC capabilities).

The wildcard service state change messages at H.248 protocol level are generated whenever

- a pack failure is detected or cleared.
- a pack is removed or inserted.

- a pack is moved to OOS (forced or normal mode) or to IS if an RT interface fails or recovers.
- an RT interface is moved to OOS or IS (either at the ICAP or at the RT).

Subsequent individual POTS subscriber line service state messages will only be sent to the MGC if the state of the line deviates from what the pack state implies.

The POTS subscriber line individual service state messages at H.248 protocol level are generated whenever

- a line is moved to OOS (forced mode) and the pack is usable or in *Shutting-Down* state.
- a line is moved to OOS (normal mode) and the pack is usable.
- a line is moved to IS and the pack is usable.
- a line becomes faulty.
- a pack failure clears and the line is faulty or OOS.
- a pack is moved to IS and the line is faulty or OOS.
- a pack shut-down is stopped and the line is OOS-SHD.
- a port/circuit test request is initiated and granted.

The pack audit and alarming functionality at H.248 protocol level makes use of the mapping of the *Termination ID* parameter (which is the identity of a VoIP subscriber line in the H.248 protocol context) to its physical address parameter (which represents the circuit number of an AP in a special RT). For further provisioning information, see *Commands and Procedures for IP-based Services*.

An example of the *Termination ID* protocol structure might be *alln-i<interface#>/c<card#>/p<port#>*.

.

□

Voice coding and packetization

Description

This section describes properties and provisioning options related to the voice coding and packetization

- Supported codec per VoIP AP
  G.711 with a-law as well as µ-law coding supported by LPZ600, LPZ602 and LPI600
  G.726, multiple rates 40, 32, 24, 16 kbps adaptive differential pulse code modulation (ADPCM) supported by LPZ602 and LPI600
  G.729, Annex A and/or Annex B supported by LPZ602 and LPI600
  G.723.1, 5.3, 6.3 kbps dual rate speech coder supported by LPZ602 and LPI600
  T.38 (Fax) supported by LPZ602 and LPI600
  Clear-channel mode for special ISDN services supported by LPZ602 and LPI600
- Echo cancelers
  Echo cancelers are supported according to ITU-T G.165 and ITU-T G.168. Their usage is determined on a per call basis.
- Receiver jitter buffer
  The VoIP AP supports a jitter buffer for the received RTP voice stream. The jitter buffer used for normal calls is provisionable per pack (LPZ600/LPZ602) or per RTP profile (LPI600). The jitter buffer used for voice band data calls (VBD) is set automatically by the application pack to a fixed (static) size.VBD refer to traditional inband data transfers as performed by modems or fax machines.
- Handling of modem calls via the RTP stream
  To provide a modem signal via the RTP stream in an acceptable manner, special measures must be taken as soon as a modem call is detected. A modem call is identified by the G.165 2100 Hz tone with phase reversal received from the far end (modem pool).

  Then the following actions are taken:

  – Set the jitter buffer length to the static value for VBD
  – use the G.711 CODEC
  – disable the echo canceler.
- Packetization interval for G.711 codec is provisionable as follows:
  For LPZ600 in the interval of 20 ... 100 msec in increments of 10 msec. The default interval is 20 msec.
  For LPZ602 in the values of 10, 20, 30, 40, 50, 60 msec. The default interval is 10 msec.
  For LPI600 in the values of 10, 20, 30 msec. The default interval is 10 msec
- Packetization interval for G.726 codec is provisionable as follows:
  For LPZ602 at G.726-32 in the values of 10, 20, 30, 40, 50, 60 msec and at G.726-16/24/40 in values 10, 20,30 msec. The default interval is 10 msec.
  For LPI600 in the values of 10, 11, 20, 22, 30 msec. The default interval is 10 msec.

- Packetization interval for G.729 codec is provisionable as follows:
  For LPZ602 in the values of 10, 20, 30, 40, 50, 60, 80 msec. The default interval is 10 msec.
  For LPI600 in the values of 10, 20, 30, 40, 50, 60, 70, 80 msec. The default interval is 10 msec.
- Packetization interval for G.723.1 codec is provisionable as follows:
  For LPZ602 and LPI600 in the values of 30, 60 msec. The default interval is 30 msec.
- Packetization interval for clear channel mode is provisionable as follows:
  For LPZ602 and LPI600 in the values of 5, 10, 20, 30 msec. The default interval is 10 msec.
- Compensation of packet arrival sequence errors
- Packet loss concealment (PLC)
  In case of lost packets of the RTP stream, there is an algorithm to substitute the lost packets. The LPZ600 replays a packet up to 3 times (≈ 30 msec if the packetization interval is 10 msec). After that silence is played for further missing packets.
  PLC per G.711, Appendix I is supported by LPZ600 and LPI600.
  PLC per G.729a is supported by LPZ602 and LPI600.
  PLC per G.723.1 is supported by LPZ602 and LPI600.
- Compressed silence
  When compressed silence is received on the incoming RTP stream then silence is played towards the subscriber. The LPZ600 does not generate compressed silence on outgoing RTP.
  Silence compression detected from the network is supported by the LPZ600/LPZ602 and LPI600.
- G.711 silence suppression
  The VoIP AP can detect G.711 suppressed silence on a per call basis for the incoming RTP stream. Towards the subscriber, silence is played accordingly.
- QoS parameters
  The IPv4 TOS octet can be set independently for signaling and media (RTP) packets generated by the VoIP AP. For SIP operation, the TOS can also be set independently for emergency call signaling and media packets. Classification and prioritization in the IPFM can then provide the desired QoS treatment based on the TOS values.
- Voice encapsulation supported by LPZ600, LPZ602 and LPI600
  This involves RTP over UDP (RFC3550).
- Session description protocol (SDP)
  SDP per RFCs 3264 and 2327 is used for SIP as well as H.248 and MGCP.

□

Digit analysis

Overview

Digit collection, analysis and possible translation in the *AnyMedia*® LAG Shelf is performed locally by each VoIP AP. The primary mechanism for defining the tree type dialing plans is via digit maps resembling the H.248/MEGACO digit map concept.

There is a default digit map and digit maps for special purposes in separate tables.

Apart from that, some strings like prefixes are considered long term stable for a customer and hence are controlled via the customer key code.

Digit map timers

The collection of digits according to a digit map may be protected by three timers, a start timer (T), short timer (S), and long timer (L). These timer values are provisionable.

1. The start timer (T) is used prior to any digits having been dialed. If the start timer is configured with the value set to zero (T = 0), then the LAG will wait indefinitely for digits.
2. If the LAG determines that at least one more digit is needed for a digit string to match any of the allowed patterns in the digit map, then the long timer (L) is used.
3. If the digit string has matched one of the patterns in a digit map, but it is possible that more digits could be received which would cause a match with a different pattern, then instead of reporting the match immediately, the LAG uses the short timer (S) and waits for more digits.

Digit maps supported by the VoIP AP

The *AnyMedia*® Access System has the following internal digit maps:

- Emergency digit map
- Default digit map.

The control protocol (H.248) may also supply a digit map for a particular call. The emergency digit map is defined to be exact pattern match such as ’110|118|119’.

When a subscriber’s dialed numbers match this digit map, then the system will act in a specific manner for emergency calls. The emergency digit map is defined internally via the customer key code (CKC).

Emergency and default digit maps are all exclusive.

In addition to the digit maps defined above, the gateway may also define some predial digits for subscribers to use some special services. For example, a caller may want to dial 184 or 186 to explicitly enable or disable caller ID information from being displayed on the caller’s device for a particular outbound call. Dialing ’*68’ may mean a callback service, etc. Those predial digits and the corresponding services are defined by the CKC, they are not part of any digit map.

Number translation

In some cases substrings of collected numbers must be replaced by a different string. Applications of this are abbreviated dialing or unified number service. In the first case the short code dialed by the subscriber is replaced by the full digit string. In the second case, the unified number (e.g. a country-wide usable number for reaching a special service) dialed by the subscriber is replaced by a region specific number to reach the special service.

The *AnyMedia*® Access System supports the identification and replacement of leading strings. In this case, if the leading digits of a dialed string match any of the abbreviated strings in a provisionable list, then all those leading digits will be replaced by the corresponding assigned digit string in an INVITE message. Number translation is implemented via a table lookup. The table of leading strings and replacement strings are provisionable.

Priority of analysis

At any time, if a dialed string may match multiple digit maps, then the digit maps are used according to the following order:

1. The built-in emergency digit map
2. Control strings. (″184″, etc.)
3. Number translation
4. The default digitmap
5. Its replacement if supplied by the control protocol.

With every new digit, matches are attempted on the gathered digits in the order shown above.

- If an emergency number is matched, the call is placed.
- If a control string is matched, the action is taken and gathered digits are discarded.
- Control strings are configurable to be used to identify prefix digits after which a **Second Dial Tone (SDT)** is autonomously applied towards the subscriber.
- If an abbreviated dialing prefix is matched, the gathered digits are replaced with those from the table lookup.
  Abbreviated dialing and control string matching are disabled for the rest of the dialing sequence.
  Abbreviated dialing cannot generate a control string. The new digit set is immediately checked against the emergency numbers and the standard digit map.
- When the standard digit map is matched, the call is placed.

The sequencing above guards against abbreviated dialing entries superseding emergency numbers or control strings.

□

Signaling parameters (H.248 — MGCP — SIP)

General information

Similar to the traditional telephony the VoIP needs a signaling system. This can be realized with different protocols:

- H.248 (also called as MEGACO)
- MGCP (Media Gateway Control Protocol)
- SIP (Session Initiation Protocol)

During the VoIP service provisioning the user will be asked for the CKC (Customer Key Code). Each customer gets its own customer CKC from Alcatel-Lucent. The CKC contains all customer specific values. There is also defined which signaling standard the customer uses.

H.248 protocol

The communication of two gateways will be performed by the H.248. This is also called MEGACO (MEdia GAteway COntrol protocol).

When the CKC for the signaling protocol H.248 is used, the GSI automatically changes the provisioning mask to the menu **IP SubSystem** - **VoIP** - **H.248**.

MGCP protocol

The MGCP protocol (version 1.0) is very similar to H.248. It complies with RFC3435

MGCP is used to control telephony (media) gateways from external call control elements called media gateway controllers or call agents. MGCP is a master/slave protocol, where the gateways are expected to execute commands sent by the call agents.

Under MGCP there are media gateways and signaling gateways. The media gateway converts the voice ″media″ to IP under the control of the media gateway controller using MGCP and the signaling gateway connects to established PSTN signaling protocols for conversion to SIGTRAN (Signaling Transformation). This gateway would normally be a part of a softswitch.

In case the service provider uses the signaling protocol MGCP the GSI automatically changes the provisioning mask to the menu **IP SubSystem** - **VoIP** - **MGCP**.

SIP protocol

SIP call signaling uses UDP over Ipv4 as the transport layer. SIP messages may arrive from the network in multiple portions to be reassembled by the VoIP AP. The UDP port number used for the SIP signaling is provisionable on the VoIP AP, default port is 5060.

The SIP call signaling is compliant with the following RFCs:

- RFC3261: “SIP - Session Initiation protocol”
- RFC3262: “Reliability of Provisional Responses in the Session Initiation Protocol”
- RFC3264: “An Offer/Answer Model with the Session Description Protocol”
- RFC3311: “The Session Initiation Protocol UPDATE Method”
- RFC3323: “A Privacy Mechanism for the Session Initiation Protocol”
- RFC3325: “Private Extension to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted networks”
- RFC3725: ″Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)″
- RFC2976: ″The SIP INFO Method″ * Sending/Receiving mid call PSTN signaling messages″
- RFC 4028: “Session Timers in the Session Initiation Protocol”
- RFC 4566 - SDP: Session Description Protocol.
- draft-levy-sip-diversion-08: “Diversion Indication in SIP * support Reception of Diversion Header on incoming INVITE message”
- RFC 3847 “A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)”

SIP server redundancy configuration with ICAP

SIP server redundancy is a mean to switch to a backup SIP server when the primary SIP server is recognized as failed. The SIP protocol defines a lot of SIP server functionality which is not necessarily combined within one physical server.

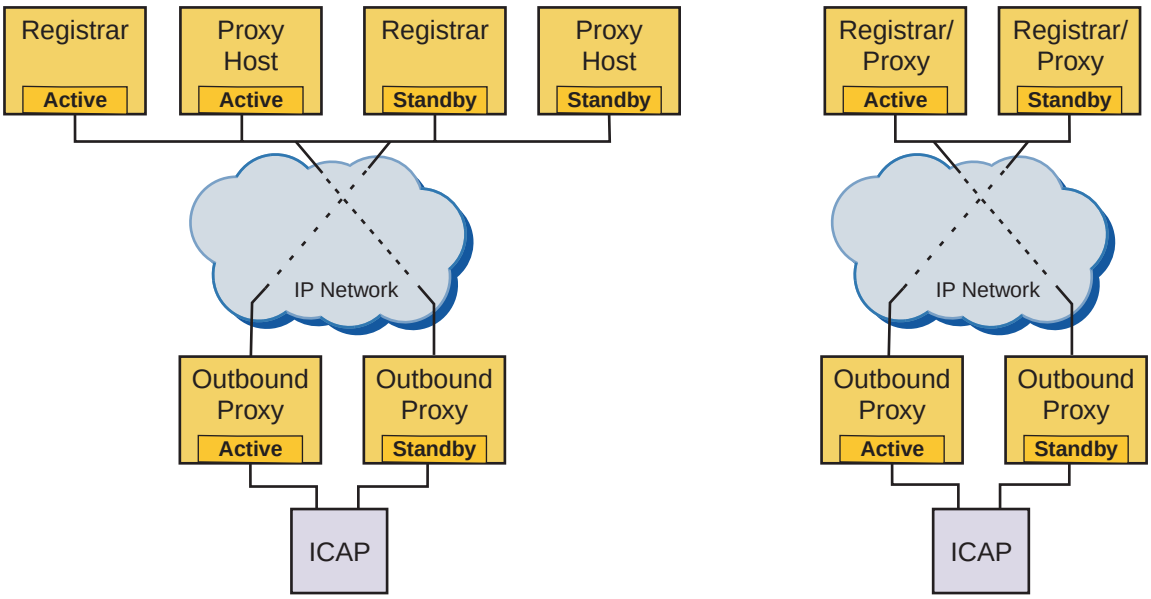
- Registrar
  The Registrar host is the server to handle `register` requests of the ICAP.
- Proxy
  The Proxy host is the first SIP server destination to which nearly all other outgoing SIP requests and responses at call processing are sent to.
- Outbound Proxy
  If the optional Outbound Proxy host is specified then this is the first SIP server to which all SIP messages will be sent.

Ideally redundancy is provided for all this functionality.

Network scenarios with Outbound Proxies

If Outbound Proxies are used, all SIP transactions, especially `registers` and `invites` are routed via this host. Once a failure of the Outbound Proxy host is detected in a redundant configuration, the ICAP switches to the next priority Outbound Proxy host. This scenario can be used regardless whether the Proxy host and the Registrar are separate or combined boxes.

The two figures below show the ICAP in a network configuration with redundant Outbound Proxies, once with Registrar hosts and Proxy hosts as separate boxes and on the right side as combined boxes.

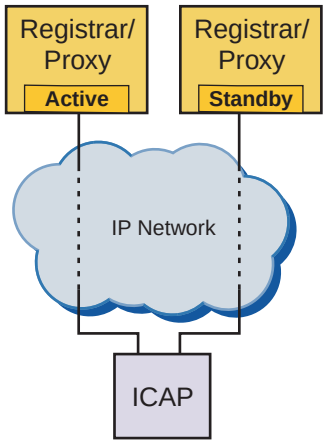


The Outbound Proxy has to support a redundancy mechanism for the Registrar and/or Proxy host in this scenario. The ICAP does not provide a redundancy for the Registrar and/or Proxy host but only for the Outbound Proxy host.

In this scenario, one redundant Registrar/Proxy server pool is assigned to the Outbound Proxy during system provisioning.

Network scenario with no Outbound Proxies – Proxy host identical with Registrar

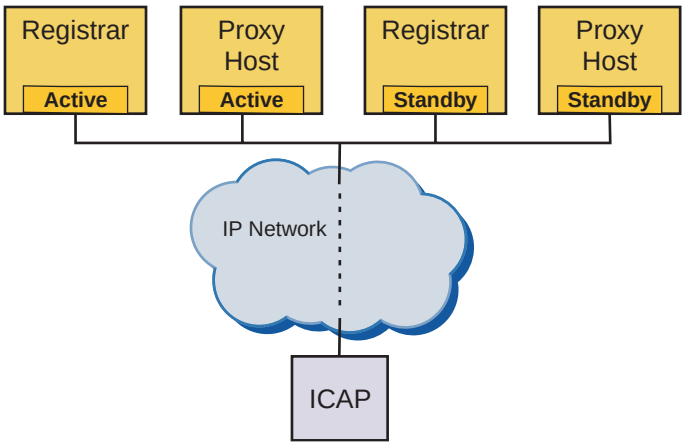
In this scenario no Outbound Proxy is used and the Proxy host is combined with the Registrar. The ICAP directly switches between the active and the standby Registrar/Proxy hosts.



In this scenario, one redundant Registrar/Proxy server pool is assigned to the ICAP during system provisioning.

Network scenario with no Outbound Proxies – Proxy host and Registrar host are separate

In this scenario no Outbound Proxy is used either. The Proxy host and the Registrar host are separate boxes with separate IP addresses/fully qualified domain names (FQDNs). The protection of the Proxy host and of the Registrar host are independent of each other. Both can have a different set of protection hosts and the protection switching does not occur simultaneously for both. The Proxy host is switched due to failed `invites` while the Registrar is switched because of failed `registers`.



In this scenario, one redundant server pool is assigned to the primary Registrar and another redundant server pool is assigned to the primary Proxy during system provisioning.

□

Direct dialing in — multiple numbers

Overview

Direct dialing in (DDI) is used, when lines are connected to a PBX to allow incoming calls to be routed directly to an extension by dialing the appropriate number.

DDI enables direct calling without going through an attended operator console, when the call is transferred to an extension of the PBX from the CO.

Description

The direct-dial-in/extension number is received from the a-side. It is converted to PB (Push Button) or V.23 signals and transferred transparently via VoIP port and subscriber line to the PBX connected to this line. Direct-dialing service is provisionable (enable/disable) per POTS subscriber line. The used signaling mode (PB/V.23) for transferring the extension number to the PBX is provisionable per POTS subscriber as well.

The number of digits to be sent to the subscriber line is controlled by either the MGC/softswitch or provisionable in the ICAP.

□

Call restriction control (provisionable for SIP only)

Overview

The purpose of call restriction control is to avoid network congestion, for example in disaster areas. Congestion can be caused by excessive rates of originating calls being generated in the disaster area and/or by excessive rates of calls destined to the disaster area. The network can be designed to restrict in such cases calls from low priority customers to preserve high quality calls for priority customers by the following methods:

- Definition of call priorities
- Rejecting calls on the SIP proxy
- Restricting calls on the *AnyMedia*® Access System.

Call restriction control by the *AnyMedia*® Access System

The *AnyMedia*® Access System provides manual restriction control for calls:

- Four subscriber priorities according to RFC3261 are defined per port. Each subscriber gets assigned one of the four priorities by provisioning
  - Non-urgent
  - Normal (default)
  - Urgent
  - Emergency.
- On pack level for each subscriber priority a threshold can be provisioned in % (0...100). (Default: 100%).
  If the threshold level of a subscriber priority is reached, no originating calls from subscribers with this priority are passed and an announcement is played towards the subscriber.
  Calls from subscribers with priority emergency and to an emergency number always pass independent from subscriber priority. In worst case an active call of a subscriber with lower priority is dropped.
  If the number of calls is below a certain threshold priority level, calls from subscribers with all priorities are accepted again.

□

Multi-line hunt group function (provisionable for SIP only)

Description

The following two modes of line hunting are envisaged for the SIP support of multi-line hunt groups (MLHG):

- line hunting performed locally on the VoIP AP
- line hunting driven line by line by the proxy In both cases an MLHG may be distributed among different VoIP APs as well as LAGs

In the *AnyMedia*® Access System, currently only the second mode of the line hunting will be supported. Lines being a member of a hunt group must be provisioned as such. This knowledge is required by the VoIP AP in order to suppress call waiting if a hunt group line is encountered busy during the line hunting process performed by the SIP proxy.

□

Terminating/originating call (provisionable for SIP only)

Terminating call (CLIP)

Caller's number display (Inbound Caller ID) can be provisioned to be enabled or disabled for a standard terminating call and can separately be provisioned for a 3-party call like call waiting. In the latter case the number of the 3rd party attempting to call one of the busy subscribers is displayed or not.

If a subscriber (caller) has subscribed to the caller's line identification presentation (CLIP) service, then a caller's number maybe transferred to the caller. The caller's number is present in the display part of the header from the INVITE message.

The caller's number display is possible:

- During a terminating call
- If the subscriber is already in another call, a third party call is arriving and the subscriber is enabled for call waiting service.

Even if the subscriber has subscribed to the CLIP service the caller's number may not be presented due to:

- The caller denies display of number (anonymous present in the From Header).
- Caller has dialed specific number ("184" in front).
- The CLIP service is not available from the network.
- The caller uses a coin phone.
- The CLIP service overlaps with another service (e.g. direct dial-in using PB method).

Originating call (CLIR)

For regular calls a caller may be provisioned for restriction of the display of his number (Outbound Caller ID Blocking). This provisioned restriction is overwritten, if the caller dials the specific number "186" in front. The other way around, if the caller is provisioned to have no restriction, he/she may enable CLIR on a per call basis by dialing the prefix "184". The caller number restriction is indicated by appropriate setting of the privacy header (priv-value = ″id″, RFC3325) and in the display part of the from header, e.g. anonymous (see also RFC3323).

For emergency calls the caller may separately be provisioned to restrict display of his number. Apart from this, the handling is the same as for regular calls. Caller's number insertion is enabled by default for emergency numbers defined by the CKC. A provisioning option permits blocking the number insertion by dialing the 184 prefix.

□

Call waiting (provisionable for SIP only)

Description

In the IP subsystem of the *AnyMedia*® Access System the call waiting feature can be enabled/disabled per subscriber.

When there is a terminating call from a third party while another call is in progress, the called party can talk to the third party by putting the original call on hold. During an emergency call and modem calls the call waiting feature is suppressed.

During an ongoing call, a terminating call from a third party causes the *AnyMedia*® Access System to send an “incoming identification tone” (IIT). This tone indicates to the end-user that there is an incoming call. When the called party (end-user) decides to accept the call from the third party, a hook flash is sent from the called party to the IP subsystem. A new call is established between the third party and the called party and a “hold service tone” (HST) is sent to the on-hold terminal. The HST may be a tone or music stored on the VoIP AP. The format of the music is .au.

As long as there is a call on-hold, it can be switched back and forth between the call in progress and the call on-hold as many times as required. This feature is also called “brokering”. When a disconnect signal is detected from the subscriber’s line while there is a call on-hold and that call on-hold continues after a certain period of time, ringing signal (IR) is sent to the subscriber’s line. The call on-hold may be released by disconnecting from the other party (by receiving BYE request or detecting a disconnect signal) in the called party’s subscriber’s line. It does not affect the call in progress.

In case of a modem dial-up call, another call request to that subscriber shall be disconnected by sending back “486 Busy Here” response to the INVITE request of the second call without taking call waiting actions.

□

Audible/Visible Message Waiting Indicator (provisionable for SIP only)

Description

In the IP subsystem of the *AnyMedia*® Access System the message waiting indication (MWI) feature can be activated per subscriber and is used to notify the customer that new messages are waiting.

The message waiting indication feature requires support from within the SIP network. The MWI info itself is signalled, via customer key code dependent SIP signaling, towards the system. The system temporarily stores this information and signals it further down towards the subscribers equipment.

The type of message waiting indication which is to be used to indicate the waiting messages to the subscriber is configurable to:

- **Audible indication** (e.g. a customer key code dependent special dial tone is used instead of the normal dial tone at originating call attempts)
- **Visual indication** (e.g. activates a customer key code dependent line signaling to trigger a visual indication on the subscriber equipment, e.g. the activation of a light or info text in an display).

□

Provisioning of a protection port

Provisioning of the protection port

The protection circuit for the whole shelf may reside on any VoIP AP. It is provisioned via SNMP. There can only be a single protection circuit on a pack. In order to not waste resources the operator has to ensure that only a single protection circuit is provisioned per *AnyMedia*® LAG Shelf.

For protection switching and protection release a COMDAC and a CIU are necessary in the system.

The protection switching is a manual action by the operator. A circuit may be protection switched irrespective of whether there is a fault condition on it or not. The SNMP command requesting the protection switch is directed to the VoIP AP providing the protection circuit. The operator specifies the protection port and the port to be protected. Subsequently the VoIP pack providing the protection circuit requests from the COMDAC to setup the metallic protection path via the UART link. The request specifies the protection port and the port to be protected. The COMDAC as the master of the metallic test bus will either reject the request or grant the request for the metallic protection path.

□

Activate service over ICAPs

Provisionable items to activate service over ICAP (LPI600)

Introduction

Provisionable items include:

- Shelf type, pack type, group
- General, including the system configuration, timing source control and IP interface.
- Profiles, including the digit map, RTP, switch, numbers, and emergency call.
- Network, including the network protocols SIP, H.248 or MGCP defined from customer key code with the appropriate network protocol parameters.
- Ports, including the port configuration, profiles, ID´s, XConnects and media monitoring.
- Downstream TDM configuration: *AnyMedia* RT aggregation, standard V5.2 aggregation, and/or R2 (PBX) or GR-303 (DS1).

All provisionable items in detail and provide default values and ranges where applicable see *Commands and Procedures for IP-based Services*.

□

Service activation provisioning for VDSL services

Provisionable items for VDSL services

Introduction

Provisionable items for VDSL services include:

- Parameters on pack level
- Parameters on port level

Provision pack parameters

When the pack type has been provisioned on shelf level, the provisionable items for VDSL services on pack level include:

- Pack type
- Enable or disable Flow Control as required
- Enable or disable Broadcast Storm Control as required

For provisioning the pack type in the system, set the pack type for the individual slot to the correct type (e.g. LPV417).

Provision port parameters

For provisioning the port parameters on a VSIM AP proceed as follows:

- Set the service state to ″In Service″.
- Select the default transmission profile or create a new transmission profile.
- Select the default PM profile or create a new PM profile.

Profiles

Profiles are a common feature of systems that are managed and using SNMP. A profile is a fixed set of parameters which specifies values that need to be provisioned only once but then can be used by any number of system entities of the same type.

The following profile types apply to VSIM APs:

- VSIM transmission profiles
- VSIM PM profiles.

The library of profiles always includes predefined profiles which cannot be modified or deleted.

All provisionable items in detail and provide default values and ranges where applicable see *Commands and Procedures for IP-based Services*.

□

Turn-up of IP-AFMs and service activation

Provisionable items for IP-AFMs

Introduction

From a high-level perspective, the turn-up provisioning of an ATM AFM and an IP-AFM differs in the following:

- On the ATM AFMs the turn-up provisioning includes the provisioning of
  - Subscriber lines
  - ATM feeders
  - QoS for ATM cells (4 service classes)
  - and the cross-connections between both sides.
- On the IP-AFMs the turn-up provisioning includes the provisioning of
  - Subscriber lines
  - ATM bridge port profiles
  - ATM bridge ports

    ATM bridge ports bridge the ATM functionality to the Ethernet functionality. The ATM feeders are hidden.
  - cross-connections between both sides
  - VLANs
  - Layer 2 interworking system parameters
  - QoS for ATM cells (4 service classes)
  - Ethernet ports towards the network
  - QoS for Ethernet frames.

Provisionable items for IP-AFMs include items that are provisionable on system level, on pack level or on port level.

Provisionable items on system level include similar parameters as for an ATM-AFM, such as

- Transmission mode
- Protection mode
- Timing source
- MAC table aging interval

Provisionable items on pack level include:

- ATM QoS provisioning
- VLANs provisioning
  - VLAN identification -

    The VLAN Id is a required parameter for the configuration of an ATM bridge port. The allowed range is [1 - 4092]. VLAN Ids 0 and 4093-4095 are reserved for internal use. A VLAN Id is rejected if this Id is assigned to a VLAN group as an NSP-VLAN Id or if this VLAN Id belongs to a VLAN group which has an NSP-VLAN assigned.

    VLAN Id 1 is the default VLAN and cannot be modified or removed from the system
  - VLAN description
  - IGMP snooping

    This parameter specifies if IGMP Snooping is enabled or disabled for this VLAN. Default value is disable.
  - Direct port communication

    This parameter specifies if direct communication between port members of the same VLAN is allowed. If not explicitly enabled, the default value will be disable.
- NSP-VLANs and User-VLANs
  These VLANs can be used for configuring ATM Bridge Ports. If it does not exist, this VLAN Id will be created by the IP-AFM automatically during the ATM Bridge Port provisioning and is deleted automatically when that ATM Bridge Port is deleted. The relation between an ATM Bridge Port and VLAN Id is 1 : 1. For NSP-VLANs and User-VLANs no IGMP snooping and Direct Port Communication is available.
- Broadcast storm control - can be enabled or disabled per pack
  If enabled, the broadcast storm control recovery mechanism will be activated whenever the broadcast traffic on any Ethernet port exceeds a provisioned high-threshold percentage of the link speed. The switch will block (discard) broadcast traffic until this percentage returns to a provisioned low-threshold percent or less.
- Provisioning of the Ethernet ports
  - Four Gigabit Ethernet (GbE) ports

    GbE1 is used to connect the IP-AFM to the network or to the next shelf in a daisy-chain. GbE2 is used to connect two IP-AFMs operating in duplex mode. GbE3 is used to connect the IP-AFM to a subtending shelf in a daisy-chain. GbE4 is reserved for future use.
  - Two Fast Ethernet (FE) ports FE1 and FE2
  - Uplink ports

    The system (IP-AFM) does not allow the operator to disable the ports used as uplink. This behavior prevents the system from loosing the inband management channel connectivity during maintenance operations.
- IGMP snooping global parameters (including IGMP fast leave)

- Provisioning of an inband management channel (optional)
  The IP-AFM can be accessed via an inband management channel. This inband channel terminates an IP address which is used typically for OAM&P functions.
- ATM bridge port provisioning
  - ATM bridge port administration
  - ATM bridge port profile – including provisioning data likely to be shared across ATM bridge ports
  - Port specific ATM bridge port parameters – provisioning data not likely to be shared across ATM bridge ports.

ATM QoS provisioning

ATM QoS provisioning on the IP-AFM is performed similarly to the QoS provisioning on the ATM AFMs. It needs to be taken into account that:

- The ATM internal feeder bandwidth of the IP-AFM is hard-coded at 280 Mbps for upstream and 280 Mbps for downstream flow.
- The remaining bandwidth is used for the OAM&P channel and internal communication.

Ethernet port provisioning

Provisioning of the Ethernet ports applies to

- four Gigabit Ethernet (GbE) ports
  - GbE1 is used to connect the IP-AFM to the network or to the next shelf in a daisy-chain.
  - GbE2 is used to connect two IP-AFMs operating in duplex mode.
  - GbE3 is used to connect the IP-AFM to a subtending shelf in a daisy-chain.
  - GbE4 is reserved for future use.
- two Fast Ethernet (FE) ports FE1 and FE2
  - Auto Negotiation – The ″Auto Negotiation″ capability for FE ports can be enabled or disabled.
  - Auto Negotiation Forced Restart – An ″Auto Negotiation Forced Restart″ forces the restart of the auto negotiation capability for this port.
  - Duplex mode – this parameter indicates if the port will work in half duplex or full duplex mode.
  - Flow Control (enable/disable) – this parameter indicates if the port will generate an 802.3x pause frame to the far end interface in case of congestion.
  - Flow Control Announce – this parameter indicates the 802.3x flow control capability announce mode during auto-negotiation.

  General the administrative status of the Ethernet ports can be enabled or disabled.

ATM bridge port provisioning

The ATM bridge ports represent the subscriber’s ingress/egress points of the layer 2 interworking system implemented in the IP-AFM controller pack.

For the provisioning, data likely to be shared across ATM bridge ports are grouped as instances of profile entries. Provisioning data not likely to be shared across ATM bridge ports are treated as specific parameters of the port.

The provisioning of an ATM bridge port requires the following parameters:

- Internal feeder VPI/VCI
- ATM bridge port profile to be associated to the ATM bridge port
  As other profiles the ATM bridge port profiles can be created, edited and deleted - assuming that they are not used by any ATM bridge port. The maximum number of ATM bridge port profiles that can be created is 15.
  The IP-AFM provides a default ATM bridge port profile.
- Specific ATM bridge port parameters such as VLAN Id and static MAC entries.

Daisy-chain uplink port provisioning

The IP-AFM can be deployed in daisy-chain configurations – in simplex or in duplex mode – similarly to the ATM AFMs.

The provisioning of IP-AFMs in a daisy-chain is in principle identical to the provisioning of single IPFMs, but additionally the Gigabit Ethernet (GbE) port of the previous IP-AFM in the daisy-chain used to connect subtending shelves (GbE3) has to be enabled .

Note that daisy chaining via the Fast Ethernet (FE) ports is not supported.

Constraints for provisioning uplink ports in *Dual Path Protection* mode

- In simplex and duplex configuration using the protection mode *Link_State*, the port selected as uplink is automatically enabled by the system and can not be disabled by the operator.
- In duplex configuration using the protection mode *RSTP*, the ports GbE1 and GbE2 are automatically enabled by the system and can not be disabled by the operator.

□

IP-AFM deployment engineering rules

Rules

The following parameters need to be considered when engineering an IP-AFM shelf:

- Internal feeder upstream shelf peak cell rate (*USPCR*)
  As in traditional legacy AFMs, this parameter represents the upstream peak cell rate that the ATM internal feeder provides towards the network.
- Internal feeder upstream bandwidth (*IFUPB*)
  This parameter specifies the upstream bandwidth allocated in the IP-AFM internal feeder. It defines the maximum upstream rate that the IP-AFM provides towards the IP network. The total bandwidth of the internal feeder is hard-coded at 281,25 Mbps. It must be considered as the upper limit for the internal upstream shelf peak cell rate.
- Upstream FE required bandwidth (*FEUPB*)
  This parameter is a non user provisioned parameter. It specifies the upstream bandwidth required for the FE ports, which connect the IP-AFM either to an ICAP or to another source of IP traffic. This parameter must be considered for the calculation of the maximum upstream traffic generated by this shelf.

Note that the maximum downstream bandwidth supported by the current IP-AFM hardware is 311,25 Mbps.

Maximum upstream bandwidth – single shelf

In case of a single shelf, the *ShelfMaxUpStreamRate* is defined as the maximum upstream rate generated by this shelf. This is a non provisionable parameter and is calculated as follows:

ShelfMaxUpStreamRate = *FEUPB* + (*USPCR* Mbps / 1.10)

In this formula, the factor (1.10) represents the ATM overhead which needs to be removed when converting the ATM traffic to Ethernet.

Maximum upstream bandwidth – daisy-chain

The maximum upstream rate in a daisy-chain is defined as the maximum upstream rate generated by a set of daisy-chained shelves. This is a non provisioned parameter and it is defined as the sum of each shelf's individual *ShelfMaxUpStreamRate*. This parameter cannot exceed the bit rate of the IP-AFM port used for the uplink (1Gbps).

□

IP-AFM Inband Management Channel to transport OAM&P Information for NB (Telephony)

Overview

Operations, administration, and maintenance messages may be sent to and from the COMDAC on the *AnyMedia*® Access System via the inband management channel. The inband management channel is part of an internal feeder connected to the IP-AFM on the appropriate *AnyMedia* Shelf. Using the inband management channel as a communications link provides an alternative to a LAN connection.

There are a number of requirements for the inband management channel:

- IP address assignment for the PC running the GSI or AEM
- IP assignment for the PC gateway
- IP assignment for the inband management channel (BB Operations channel)
- An Ethernet (LAN) crossover cable for 10Base-T connection
- IP assignment for the IP-AFM 10Base-T local management port
- IP assignment for the COMDAC Ethernet (LAN) port (IP address and default gateway).

NOTE: In IP-AFM duplex mode configurations, the communication to the COMDAC via inband management channel is not yet supported at the issue date of this information product.

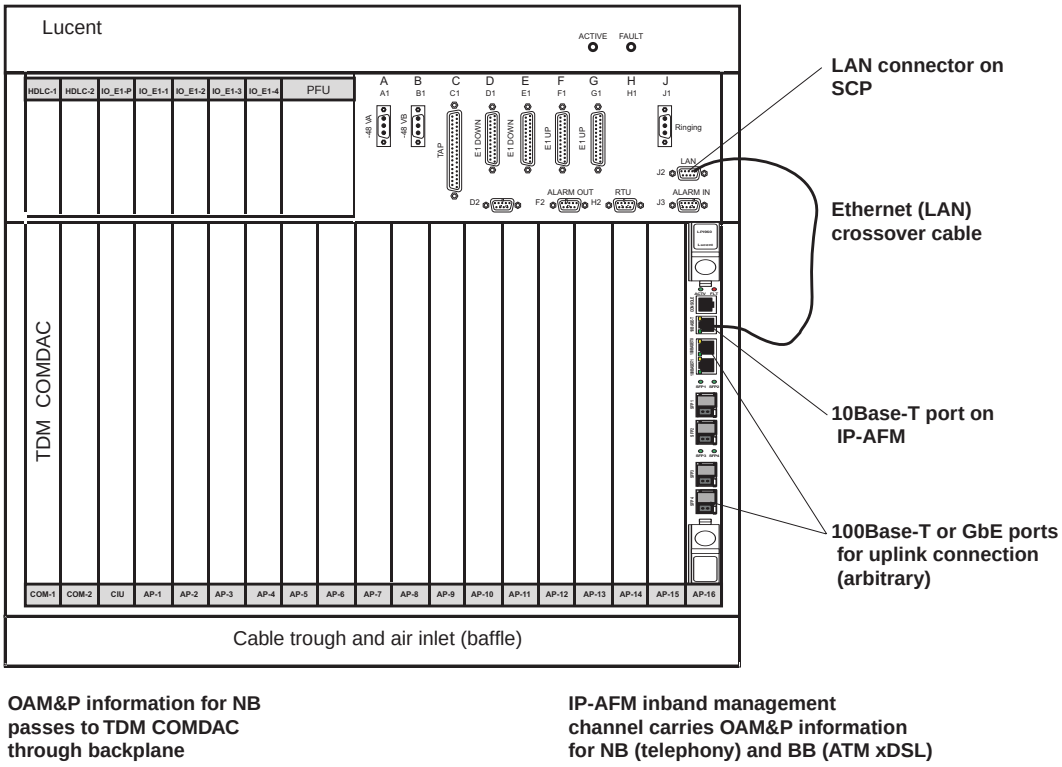
Physical requirements

An Ethernet (LAN) crossover cable or Ethernet hub is used to connect the IP-AFM console port (10Base-T) to the appropriate LAN connector on the shelf connection panel (field) or shelf backplane.

The location of the LAN connector depends on the used *AnyMedia*® Shelf type as follows:

- For ETSI V5 Shelf on the SCP with LAN connector designation J2
- For FAST Shelf on the backplane with LAN connector designation J107
- For LAG 1900 Shelf on the shelf connector field with LAN connector designation J104
- For LAG 2300 Shelf on the backplane with LAN connector designation J107
- For LAG 4300 Shelf on the connector field with LAN connector c designation J107

The example in the figure below shows a physical connection for the IP-AFM inband management channel in an *AnyMedia*® ETSI V5 Shelf



Special duplex cabling is required when two IP-AFMs are installed. For details on this cabling, see the *AnyMedia*® Access System *Commands and Procedures for ATM xDSL services* online documentation (363-211-133).

IP assignments

The IP assignments in the next figure are examples. The IPs that are used in each subnet must be assigned to work with the local IP/Ethernet network configuration. The IP assignments are made using several different mechanisms and have to be included in the Management-VLAN.

The PC's IP and gateway are assigned using the *Windows* (Windows is a registered trademark of Microsoft Corporation) operating system *Network* input screens. Router IP addresses are entered using the router's operations interface. The *AnyMedia*® Shelf IPs are entered using the GSI or AEM. In the next figure, the IPs designated are as follows:

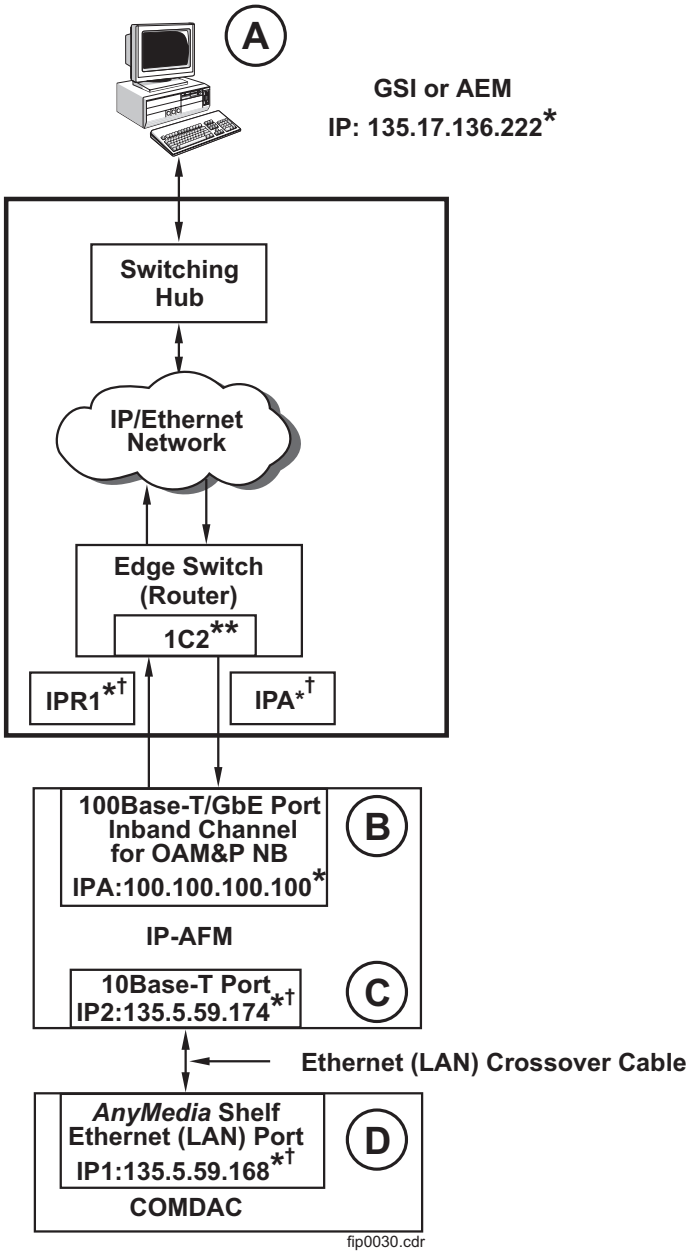
A is the IP address of the PC on which the GSI or AEM is installed.

B is the IP address of the IP-AFM inband management channel (IPA). The IP address of the router port connected to the shelf (IPR1) used for the uplink connection must be in the same subnet as IPA. Note that IPR1 is the default gateway of IPA, and in the router there is a static route to Subnet_1 with IPA as the gateway.

C is the IP address of the IP-AFM 10Base-T port (IP2).

D is the IP address of the shelf Ethernet (LAN) port (IP1) for the COMDAC. The COMDAC's default gateway is IP2 (IP address of IP-AFM 10Base-T).

The example in figure below shows an IP assignments for network configuration including IP-AFM inband management channel



*** - IPs are examples; network planning will supply these.**

† - IP1 and IP2 are part of the same subnet (Subnet_1)
- IPA and IPR1 are part of the same subnet (Subnet_R1)

**** - 1C2 - name of router port connected to *AnyMedia* Shelf**

IPA : IP address of the IP-AFM inband management channel

IPR1 : IP address of the router port connected to the shelf 1

Note that the IP-AFM static routing functions specify that *Subnet_1* is reached via *Subnet_R1*.

Provisioning

For the provisioning of the inband management channel (optional) see *AnyMedia*® Access System *Commands and Procedures for ATM xDSL services* online documentation (363-211-133).

□

Service activation provisioning for IPADSL2 services

Provisionable items for IPADSL2 services

Introduction

Provisionable items for IPADSL2 services include:

- Parameters on pack level
- Parameters per port (line provisioning)
- ATM bridge port
- Performance management.

Provision parameters on pack level

Provisionable items for IPADSL2 services on pack level include:

- Pack type
- GbE ports on the faceplate
- Layer 2 Interworking parameters
- VLAN Provisioning
- IGMP snooping global parameters

When IGMP snooping is enabled on a VLAN, the behavior of the system is to discard all unknown multicast traffic. The IPADSL2+ allows the operator to provision static multicast groups which will never be discarded when IGMP snooping is enabled on the VLAN.

Provisioning static multicast groups requires a multicast address and a mask. This approach allows the operator to specify a broad range of multicast addresses with a single addition to the multicast group list. For example: If the IP-Address 224.10.10.0 and mask 225.225.225.0 is provisioned in the system, all multicast addresses within the range 224.10.10.0 through 224.10.10.225 will be considered statically provisioned for the given VLAN. Well-known multicast groups will be statically provisioned by default when the system is initialized.

All provisionable items in detail and provide default values and ranges where applicable see *Commands and Procedures for IP-based Services*.

Provision port provisioning parameters

Provisionable items for IPADSL2 services per port include:

- IPADSL2+ port number
- Service state
- Transmission/DMT profiles

- Line provisioning
  - ADSL line type

    This field defines the type of ADSL physical line by specifying whether and how the line is channelized.
  - ADSL2+ Line configuration profile

    Each line of the IPADSL2+ pack must be associated to one ADSL2+ line configuration profile
  - ADSL2+ Line startup mode

    It depends on the CPE used by the subscriber.
  - ADSL2 performance management profile

    Each line of the IPADSL2+ pack must be associated to one ADSL2 PM profile. This profile defines thresholds associated to data collections intervals. When these thresholds are crossed alarm traps will be sent to the management system.

    Setting the thresholds to the value 0 disables the generation of the associated alarm trap.

ATM bridge port provisioning

ATM bridge ports represent the subscriber's ingress/egress points of the layer 2 interworking system implemented in the IPADSL2+ pack. This provisioning model assumes that data likely to be shared across ATM bridge ports can be grouped together as entries in profile tables. On the other hand, provisioning data not likely to be shared across ATM bridge ports will be treated as specific parameters of the port.

Provisioning of an ATM bridge port requires the following parameters:

- Pack port number where the ATM Bridge port will be created
- VPI/VCI configured in the ADSL2+ modem connected to the port.
  The VPI/VCI and the port number are the fields that uniquely identify the ATM bridge port. For a given ADSL2+ port, multiple ATM bridge ports can be provisioned.
- Traffic Profile to be associated to the ATM bridge port.
  This profile includes the ATM service category and corresponding upstream/downstream parameters (policing parameters, etc.).
- ATM bridge port profile to be associated to the ATM bridge port.
  This profile includes Layer 2 parameters that will define the behavior and characteristics of the port
- IP Statistics Traffic profile to be associated to the ATM bridge port.
  This profile contains the traffic statistics thresholds for the 15-minute intervals and/or 24-hour interval.
- Specific ATM bridge port parameters such as VLAN id, static MAC provisioning etc.
- Filtering
- Policing/Scheduling.

Performance management

Performance management of the IPADSL2+ faceplate ports contains attributes that allow for the monitoring of several traffic statistics for a port.

Performance management can be enabled/disabled on a per face port basis:

- ATM Bridge Port Performance Management
- EtherNet Port Performance Management.

Profiles

Profiles are a common feature of systems that are managed and using SNMP. A profile is a fixed set of parameters which specifies values that need to be provisioned only once but then can be used by any number of system entities of the same type.

The following profile types apply to IPADSL2 APs:

- ADSL2 Transmission profiles
- ADSL2 performance management profiles
- ADSL2 DMT profiles
- ATM bridge port profiles
- ATM bridge port traffic profiles
- Bridge port PM profiles.

The library of profiles always includes predefined profiles which cannot be modified or deleted.

All provisionable parameters for the profiles and provide their setting options see *Commands and Procedures for IP-based Services*.

□

Provisioning of L2 and L3 functionality

VLAN provisioning

Overview

The *AnyMedia*® Access System system supports three types of VLANs:

-
  - ″Normal″, port-based VLANs, including shared VLANs
  - Layer 3 VLANs
  - Tunnel VLANs (also known as QinQ or stacked VLANs).
- Each VLAN is linked with an ingress and an egress rule.
- Additionally to the ingress rules, classifying and policing is supported (see “Quality of Service provisioning for the IP subsystem” (p. 4-17))
- VLANs must be provisioned separately on every single pack.
- VLAN configuration must be carefully planned through the whole network, or data loss might occur.
- VLANs support MAC learning and broadcast storm control
- n PVCs to 1 VLAN mapping supported by IP-AFM
  Multiple PVCs from xDSL ports and/or trunk ports can be mapped into a single VLAN
- There is no distinction between upstream or downstream. All ports (except in case of tunnel VLANs) are treated identically. Only the physical connection makes a difference.

Not all packs support all VLAN types. The table below shows which VLAN types are supported by the individual pack types.

Pack type	VLAN types			
	Port-based VLANs		L3 VLAN	Tunnel-VLAN
	Normal VLANs	Shared VLANs		
IPFM	×	×	×	×
VoIP AP			×([1]), ([2])	
ICAP			×([1]), ([2])	
VSIM AP	×			([3])
ESIM	×	×	×	×
IP-AFM	×			×
IPADSL2_32 AP	×			×

Notes:

1. VoIP APs and ICAPs support only exactly one VLAN for all AP ports. With release R3.3 the ICAP support at least two VLANs, one for the RTP data stream and one for the signaling.
2. VLAN provisioning on a VoIP AP and on ICAPs is done differently to VLAN provisioning on other packs.
3. Frames with double-tagged VLAN IDs won't be dropped, but they will be treated as normal tagged frames if their first tagged field value is 0 x 8100. Otherwise, they will be treated as untagged frames.

Port-based VLANs

- Port-based VLANs form broadcast domains:
  - Broadcast messages are forwarded to all members of a VLAN, but not to other ports.
  - Unicast messages with a known MAC address are only sent to the corresponding port.
  - Unicast messages with unknown MAC address are broadcasted.
  - Multicast messages are only sent to all ports which have members of this multicast group. Membership is learned by IGMP snooping.
- The VLANs are identified by their VLAN ID
- The *AnyMedia*® Access System supports VLAN 1 to 4092. VLAN 4093 and 4094 are reserved for internal use.
- Up to 256 VLANs can be provisioned.
- Ports are assigned to a VLAN with egress rules:
  - Untagged
  - Tagged
  - Shared.
- Each port can be member of many VLANs, but only one can be untagged.
- Each port has a PVID (port VLAN ID). This VLAN ID is used to tag untagged packets for internal use. Default PVID for all ports is ″1″.
- Each port has ingress rules. A filter, which is enabled or disabled can be defined.

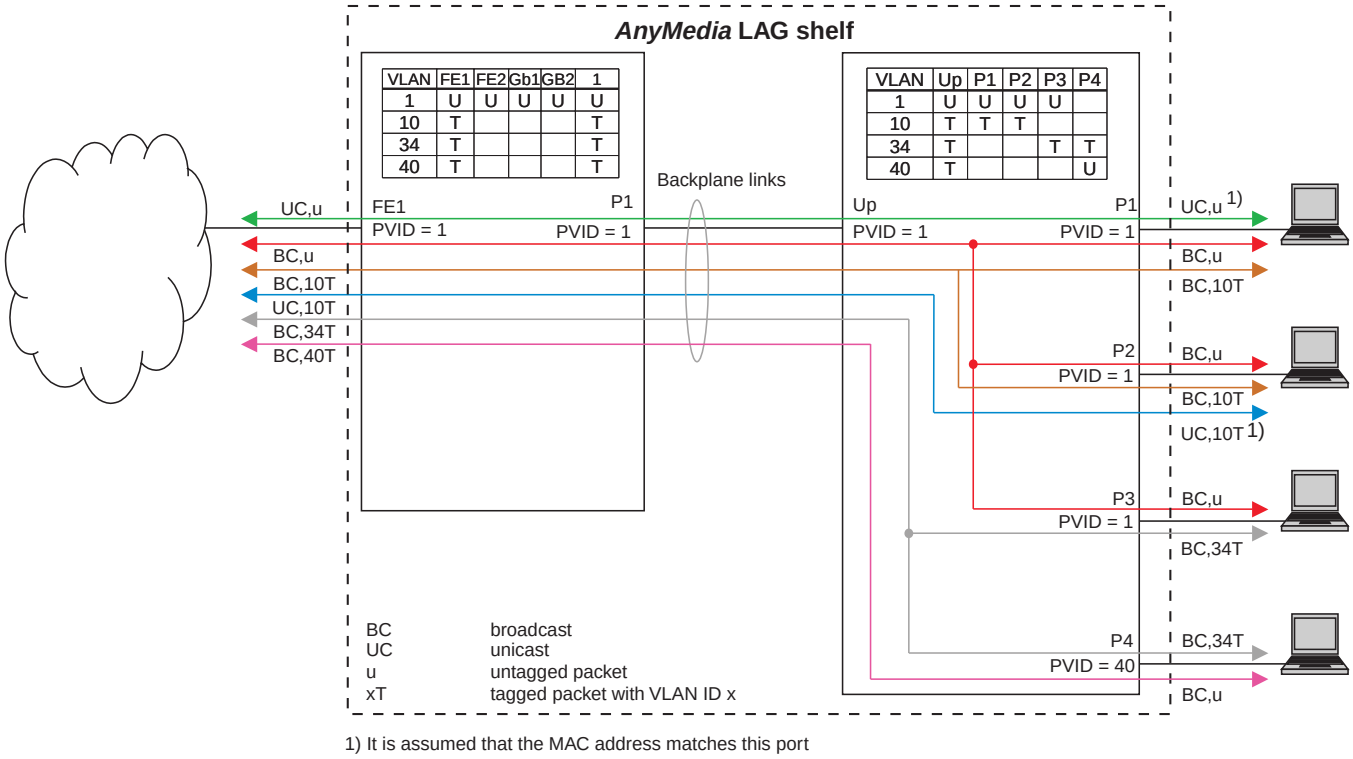
Ingress filter	Accepted frames	Result
Disabled	All	All received packets are accepted at the port. However they might be dropped later by subsequent policies
	Tagged only	

Ingress filter	Accepted frames	Result
Enabled	All	Untagged and/or tagged packets with a valid VLAN ID are accepted[1]
	Tagged only	Only tagged packets with a valid VLAN ID are accepted[1]

Notes:

1. A VLAN ID is valid, when the port is a member of this VLAN.

The figure below shows how different packet types (broadcast, unicast, tagged, untagged) are handled by port-based VLANs provisioned on packs of the *AnyMedia*® Access System.



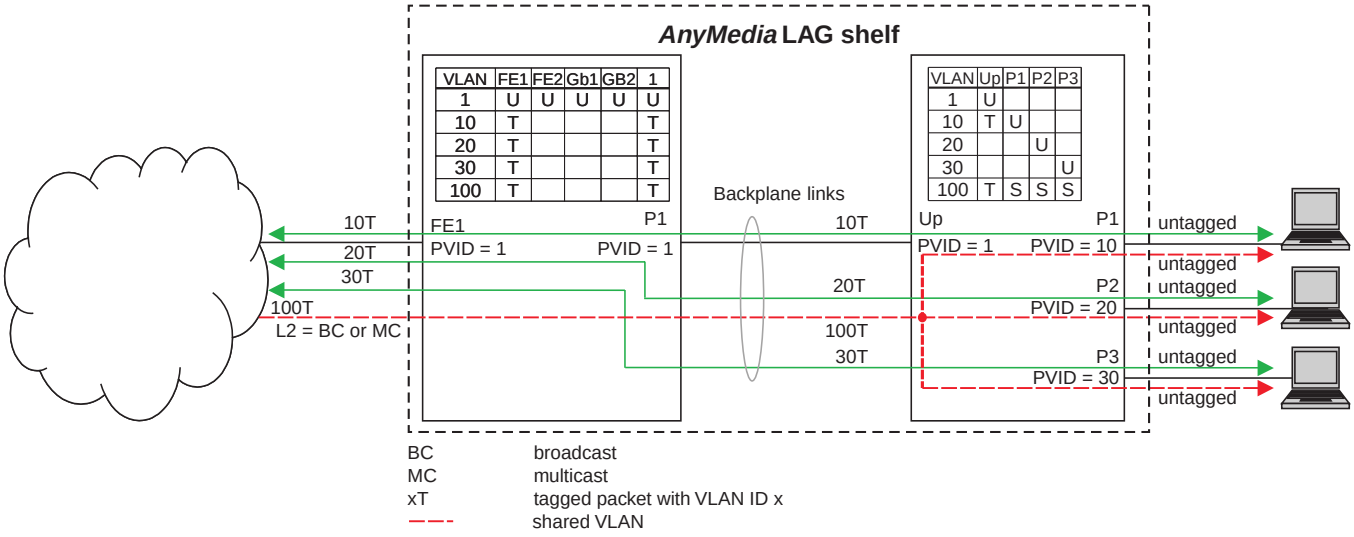
Multicast messages are distributed like broadcast packages. The are only sent to all ports which have members of this multicast group. Membership is learned by IGMP snooping.

Shared VLANs

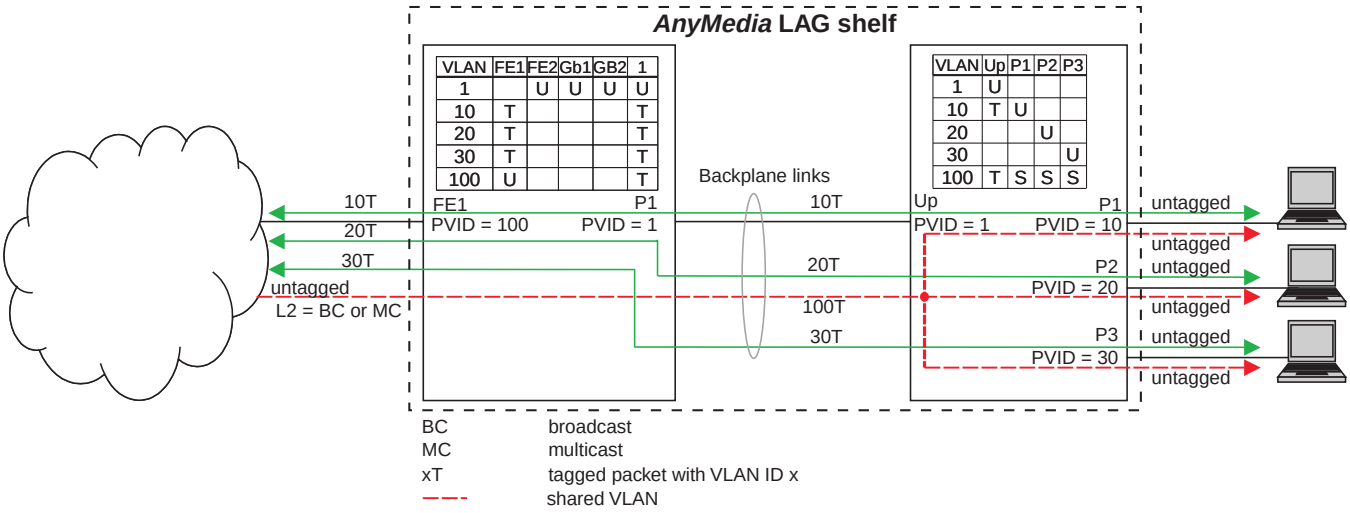
There are applications (e.g. video broadcast), where it might be helpful to split protocols in different VLANs (e.g. control data and video stream).

- VLAN unaware subscribers connected to a port can only be member of one untagged VLAN. To allow splitting traffic into different VLANs, a shared VLAN must be used (or better: the port must be a shared member of a VLAN).
- A shared VLAN is unidirectional (not unicast), but is expected to transport broadcast or multicast traffic.
- Broadcast traffic (e.g. video) from the ISP can be sent tagged (preferred) or untagged, but it will be untagged at the subscriber ports.
- Control traffic is expected always to be tagged at network side.
- Untagged traffic from the subscribers will be sent tagged with the corresponding VLAN ID (via a normal port-based VLAN) to the ISP.

The figure below shows how packets are handled in the *AnyMedia*® Access System in a shared VLAN tagged with VLAN ID 100 in the network.



The next figure shows how packets are handled in the *AnyMedia*® Access System in an untagged shared VLAN in the network.

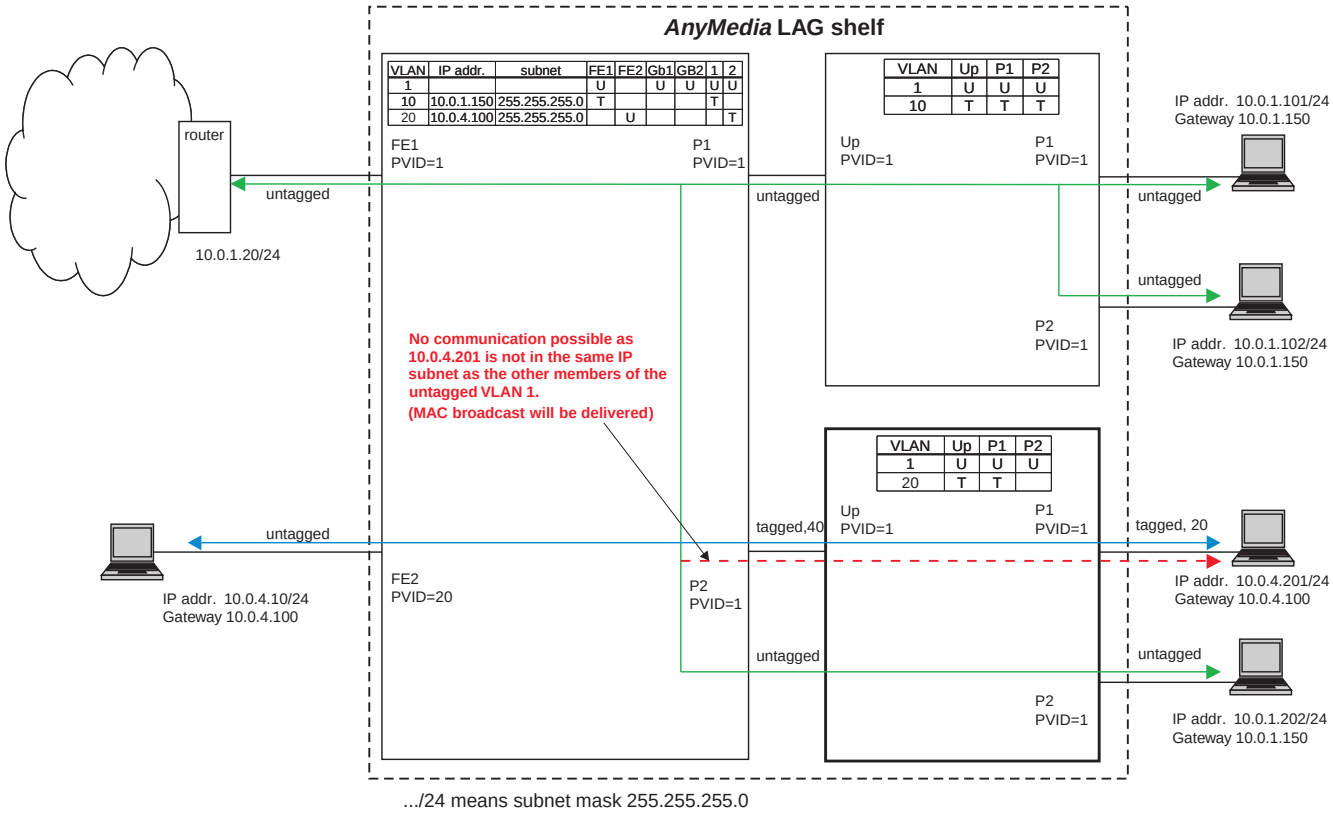


Layer 3 VLANs

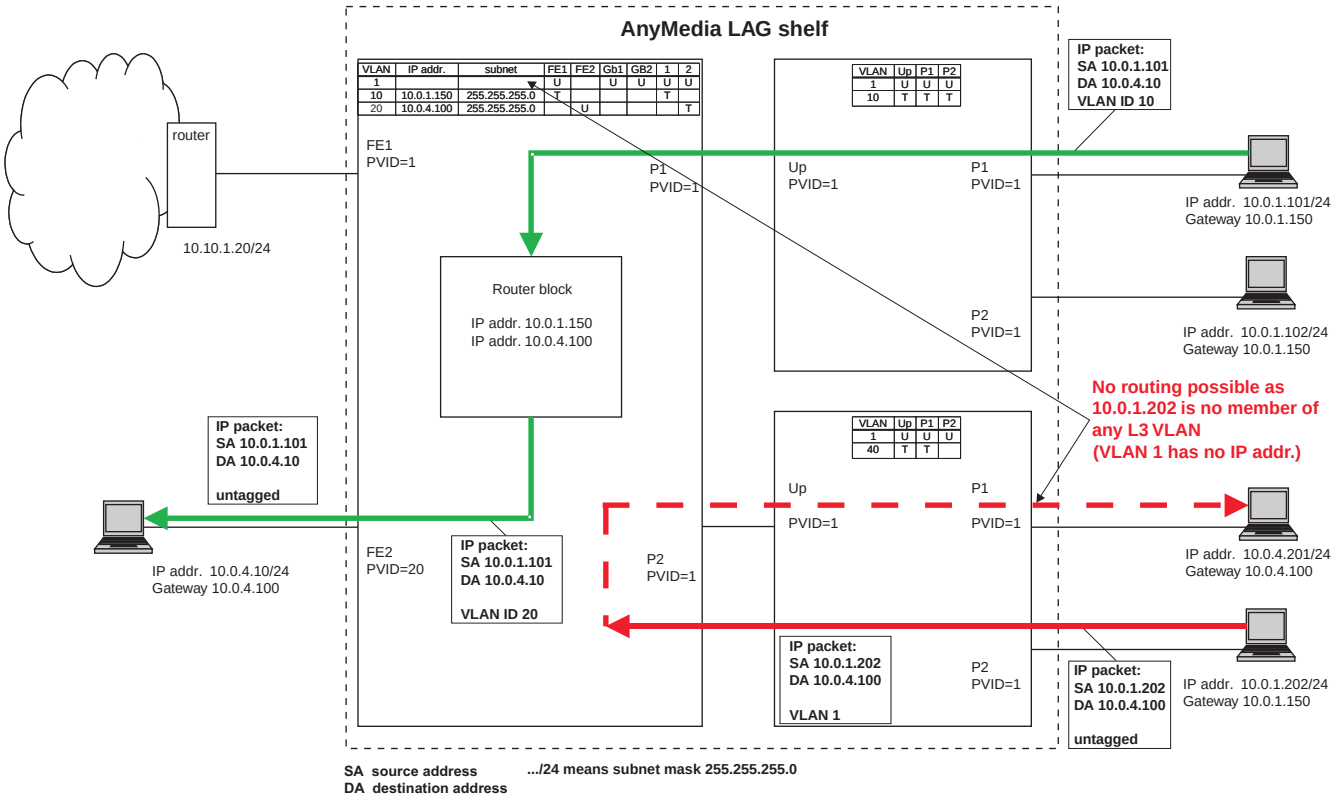
Layer 3 VLANs (L3 VLANs) allow routing in the packs of the *AnyMedia*® Access System.

- For L3 VLANs the packs support routing on VLAN base, not on port base. Therefore the IP address is not assigned to a port, but to the VLAN.
- Only the management Ethernet interface port has an IP address. This IP address cannot be changed using the GSI or NAM.
- When an IP address (and subnet mask) is assigned to a VLAN, this VLAN becomes a L3 VLAN and is internally connected to the router.
- Routing is only supported between L3 VLANs
- If routing is done between tagged VLANs, the VLAN ID of a routed packet is changed.
- Subscribers on a L3 VLAN should have their default gateway set to the IP address of this VLAN.
- L3 VLANs support inband management on the IPFM. The IPFM can be managed with each VLAN IP address provisioned.

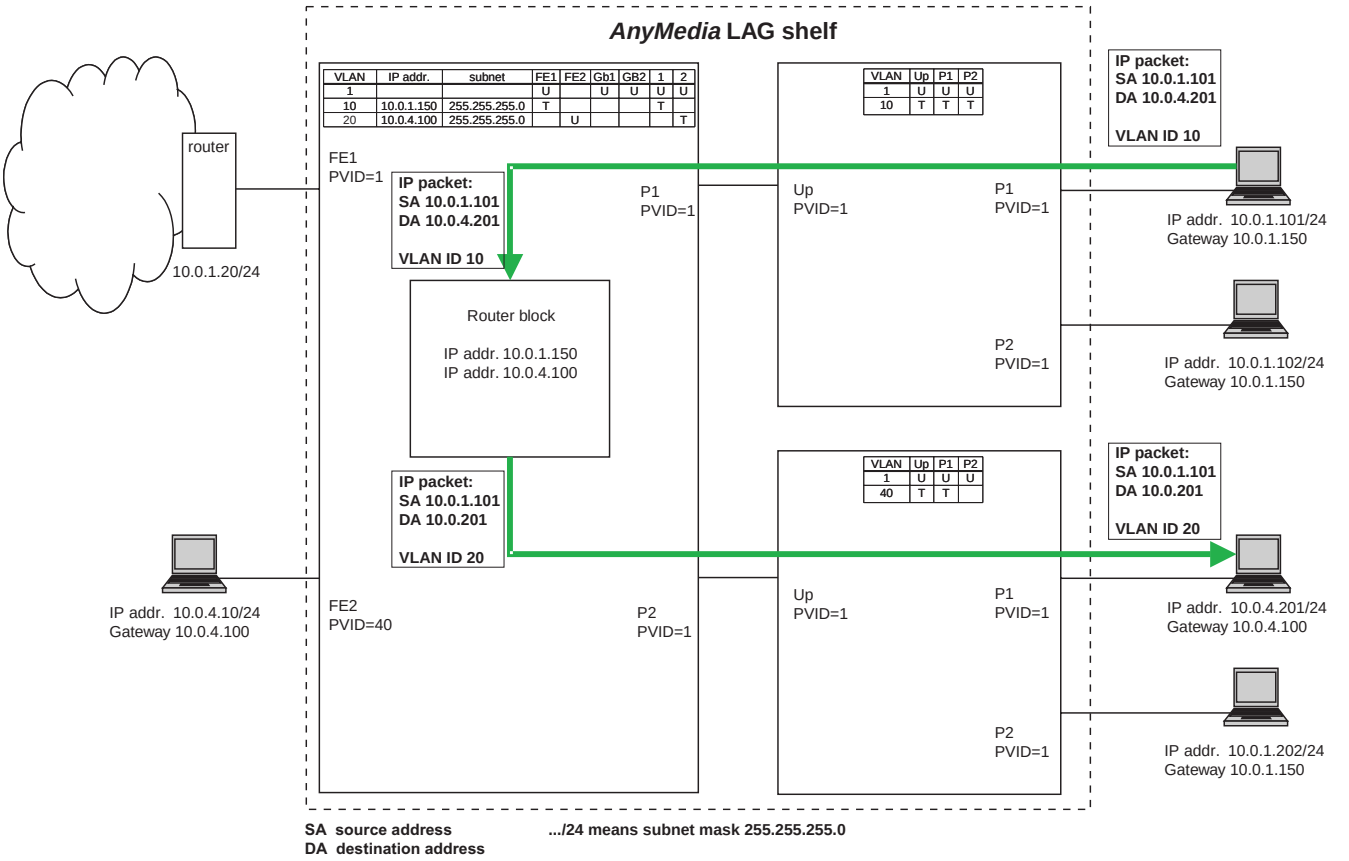
The figure below shows VLANs where source IP address and destination IP address are located in the same subnet. Therefore only L2 switching is done between source and destination. The subscriber at pack 2 port 1 is in a different IP subnet than the other members of this VLAN, so IP communication is not possible.



The next figure shows L3 VLANs, where source IP address and destination IP address are not located in the same subnet. Therefore the routing capability of the packs in the *AnyMedia*® Access System is required. Shown is a possible route (note that the VLAN ID is being changed by the router block) and an example where no routing is possible because for VLAN ID 1 no IP address is specified.



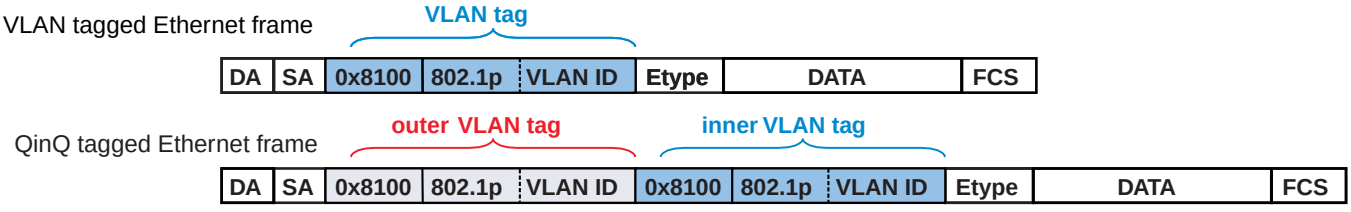
The following figure shows a routing between two subscribers connected to the *AnyMedia*® Access System. Again, the VLAN ID is being changed by the router block.



Tunnel-VLANs

Tunnel-VLANs (also called QinQ or stacked VLANs) support an additional (outer) VLAN tag on a packet.

The figure below shows a VLAN tagged Ethernet frame compared to a QinQ tagged Ethernet frame with the additional outer VLAN tag.



- The additional tag is the VLAN ID of the tunnel-VLAN.
- A port can be member of a tunnel-VLAN being a QinQ port or QinQ access port.
- Packets at QinQ ports have the additional outer VLAN tag, QinQ access port do not.
- Packets received at a QinQ access port are forwarded to a QinQ port by adding the additional tag.

- Packets received at a QinQ port are forwarded to an access port by deleting the additional tag.
- Packets received at a QinQ port are forwarded unchanged to QinQ ports.
- If a port is member of a tunnel-VLAN, it cannot be member of normal port-based or L3 VLAN.
- It is strongly recommended to only send tagged frames to a port, which is member of a tunnel-VLAN, because there is no way to distinguish between a tunneled untagged packet and a tagged not tunneled packet.

VLAN provisioning

When creating a VLAN, the following provisionable items are required:

- VLAN Type
- VLAN ID (in the range of 1...4092)
- VLAN Name
- Broadcast Storm Control (optional)
- IP Address (only applicable for Layer 3 VLANs)
- Subnetmask (only applicable for Layer 3 VLANs)
- Associated ports and egress rule per port.
- Port VLAN ID (PVID) including Ingress Filter and type of Acceptable Frame.

In contrast to IPFM ports, VDSL ports can be untagged in multiple VLANs. The PVID is not necessarily the PVID of the VLAN in which the port is an untagged entity.

The following egress rules are provisionable for each port (for uplinks and for backplane spokes to the APs):

- Egress tagged mode (for standard VLANs only)
  In *Egress tagged* mode, packets transmitted in the outgoing direction of a certain port have to be sent tagged. If the packet, when it came in, was already tagged, this tag will not be modified. If the packet, when it came in, was untagged, it has to be tagged with the PVID of the ingress port.
  To frames that are transmitted from these ports, a 4-byte tag including the VLAN ID is added to the MAC frame header.
- Egress untagged mode (for standard VLANs only)
  In *Egress untagged* mode, packets transmitted in outgoing direction will not be tagged. If the packet is tagged, this tag will be removed. The system automatically uses exactly that VLAN ID, whose tag has to be removed, as PVID to handle the ingress traffic. Untagged packets received (ingress), at that port will be tagged according to that PVID value.
  Ports can only be member of exactly one VLAN with the rule *Egress untagged*.
  An arriving packet that already contains a tag will not be modified.
  A given port can only be defined as Egress Untagged in one standard VLAN.
  Note: Tagged packets may be discarded if the port they arrive has engress filtering enabled and is not member of the VLAN indicated by packet's tag.

- Egress Shared (for standard VLANs only)
  Egress shared refers to overlapping VLAN domains. It is used to share MAC address tables across VLANs.
- QinQ Port (for tunnel-VLANS only)
  This is a tagged port of a tunnel-VLAN. Actually these tagged ports are the switch-to-switch ports of tunnel-VLANs. Any packet received by the port should be double tagged. The VLAN ID of the outer tag should be the same as the VLAN ID of the tunnel-VLAN.
  If an untagged packet is received on the port, the packet will belong to the VLAN associated with the PVID of the port.
  If a tagged packet is received on the port and the VLAN ID in the outer tag is not the VLAN ID of a tagged VLAN and is different to the VLAN ID of the tunnel-VLAN, then the packet will be discarded.
  Any packet to be forwarded from the tunnel-VLAN to the tagged port will be transmitted as double tagged packet and the VLAN ID in the outer tag will be defined by the VLAN ID of the tunnel-VLAN.
- QinQ Access Port (for tunnel-VLANS only)
  QinQ is the short name for tunneling 802.1q VLANs inside 802.1q VLANs. This is an untagged port of a tunnel-VLAN. Actually, these ports are the ingress/egress ports for the tunnel-VLANs. Any packet received on the port will be tagged with a second 802.1q tag regardless of the tagged/untagged type of the original packets. The VLAN ID in the outer tag will be defined by the VLAN ID of the tunnel-VLAN. Any packet to be forwarded from the tunnel-VLAN to the port will be transmitted with the second IEEE 802.1Q tag removed. So the original tagged or untagged packets will appear. These untagged ports can not be overlapped among other normal VLANs. (for tunnel-VLANs only).
  A given port can only be defined as QinQ Access Port in one tunnel-VLAN. A port can only be provisioned as a QinQ Access port if it is not in any non-default standard VLAN or any tunnel-VLAN.

If a port is not part of any user defined VLAN as egress untagged, it is part of the default VLAN (VLAN ID 1).

Modifying VLANs

VLANs can be modified regarding the following settings:

- Ingress filters
  As described in "Port-based VLANs" (p. 4-88), an ingress filter for the incoming packets can be enabled or disabled on an IPFM port or on a VSIM port.
  If enabled, the filter restricts incoming frames to the provisioned VLANs, all others are discarded. If disabled, all incoming frames are allowed.
- Acceptable frames (on an IPFM port or on a VSIM port)
  As also described in "Port-based VLANs" (p. 4-88) it can be selected whether all frames will be accepted or only tagged ones.
- PVID for individual ports
  All frames are internally handled as tagged frames. Untagged frames get a PVID. For all packs except the VSIM AP the PVID for any port is automatically set to the VLAN ID which this port is untagged member of.
  For the VSIM AP, the PVID is provisionable. It is not automatically set to the VLAN ID of the untagged VLAN. It is strongly recommended that the PVID is set to the VLAN ID of the untagged VLAN.

Broadcast storm control per VLAN

Currently broadcast storm control per VLAN is supported on the IPFM, on the ESIM and on the IPADSL2 AP.

For provisioning broadcast storm control the following is required:

- First enable broadcast storm control on the pack. After that all per VLAN configured broadcast storm control thresholds are activated
- Then set the threshold in the VLAN configuration window. The value assigned for broadcast storm is the maximum number of broadcast packets per second allowed to access this VLAN

MAC address learning

MAC addresses can be:

- Dynamic MAC addresses that are automatically learned by the system and deleted when for a provisionable time frame no packets are sent to it or
- Static MAC addresses.
  To provision a static MAC address, the VLAN ID, the port and the MAC address is required.

The IPFM and the ESIM support the following MAC address learning features:

- Up to 64 static MAC addresses provisionable per VLAN ID (downlinks only)
- MAC addresses can be learned per port (uplinks and downlinks)
- Learned MAC addresses can be deleted
- Max 4096 dynamic MAC addresses per pack
- Max. 250 dynamic MAC addresses per VLAN on pack
- Max 512 dynamic MAC addresses per port.

The IP-AFM controller pack supports the following MAC entries learning features:

- Dynamic learning and aging of MAC entries into/out of the forwarding table
- MAC entries can be learned or provisioned per ATM bridge port
- A limit of 1...35 is provisionable per port for dynamic MACs
- An aging timer is provisionable per IP-AFM pack
- Provisioning of static MAC entries, that is entries added to the forwarding table during provisioning time
- A limit of 1...20 is provisionable per port for static MACs.

The VSIM AP and the IPADSL2_32p AP support the following MAC address learning features:

- MAC addresses can be learned per VDSL/ADSL port
- MAC addresses can be provisioned per VDSL/ADSL port
- A limit of 1...35 is provisionable per port for dynamic MAC addresses
- A limit of 1...20 is provisionable per port for static MAC addresses
- Dynamic entries can be declared static

Note, that in the VSIM AP the actual time interval for deleting a MAC entry when no packets have been received may range from 1 to 2 times the provisioned interval. For example, if the MAC aging timer on a VSIM AP is set to 5 minutes, MACs will be deleted after 5 to 10 minutes of inactivity.

Static routes

Up to 256 static routes through the network can be provisioned on the IPFM. Provision the following items:

- Destination IP address
- Subnet mask
- One default gateway.

IGMP snooping/ IGMP fast leave

IGMP snooping is supported for the IPFM, the ESIM, the VSIM AP and the IPADSL2_32p AP. Enable IGMP snooping and forced aging if required, and enter a value for the aging timeout. This way, a client who sends regular join messages, will time out if the join messages are not sent and the leave message is missed by the pack.

The VSIM AP and the IPADSL2_32p AP support provisionable query parameters and a retrievable multicast forwarding table.

IGMP fast leave is supported and can be enabled/disabled per pack on the IPFM, the VSIM AP, the ESIM, the IP-AFM and on the IPADSL2_32p AP.

Trace route

For tracing route through the network to an IP address that can be routed to, enter the IP address. A table will display the number of hops to the IP address, and the response times.

This feature is supported by the IP controller and by all stand-alone IP APs including the ICAP.

Multiple IP addresses within the ICAP

There are 3 types of data stream from/to the ICAP:

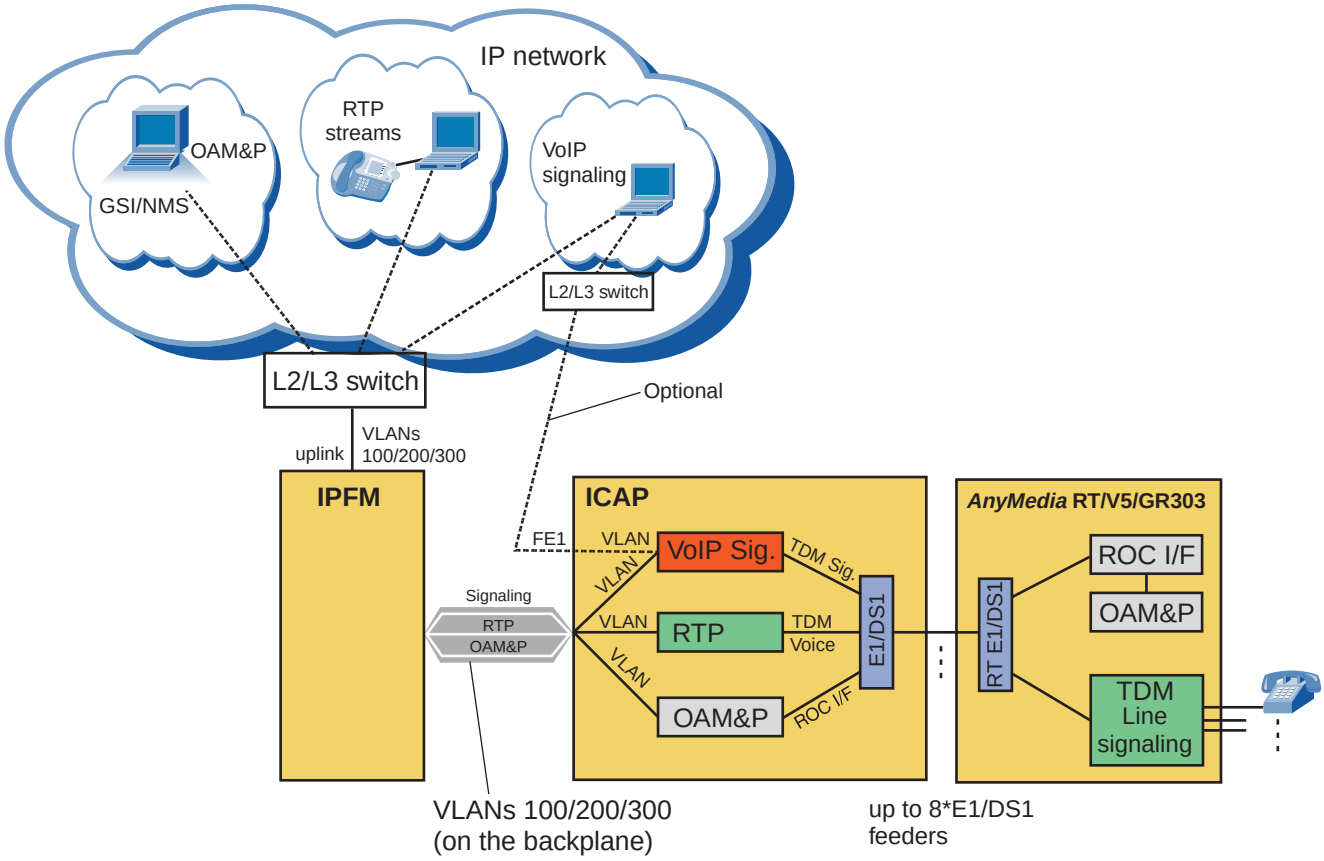
- RTP
- Signaling
- OAM&P.

These data can be sent to the next network node (IPFM, L2/L3 switch) via one line. But for avoiding bugging it is wise to separate these data over two or three different ways.

In order to achieve that, a way has to be found to assign to each data stream a dedicated IP address. That is, each data stream can have a dedicated IP address, which can be assigned to a dedicated VLAN ID. Tables in the ICAP (created by the operator) define the assignment IP address – VLAN ID.

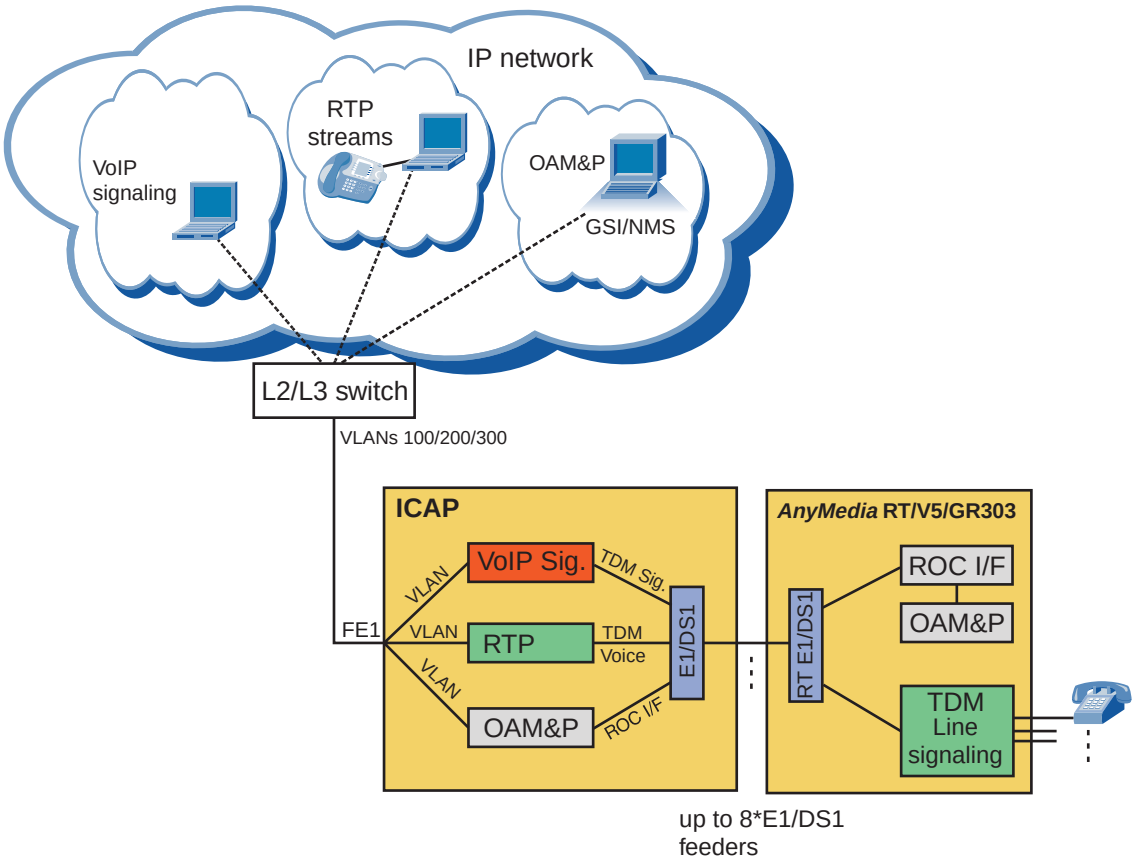
The diagram below shows the data stream in controlled mode (IPFM is available and will be used by the ICAP). In this configuration the three data streams are forwarded to the IPFM via the backplane. Each data stream belongs to a separate VLAN.

Note: Also the FE1 port on the ICAP front plate can be used to carry one, two or all three types of traffic instead of using the backplane as shown here.



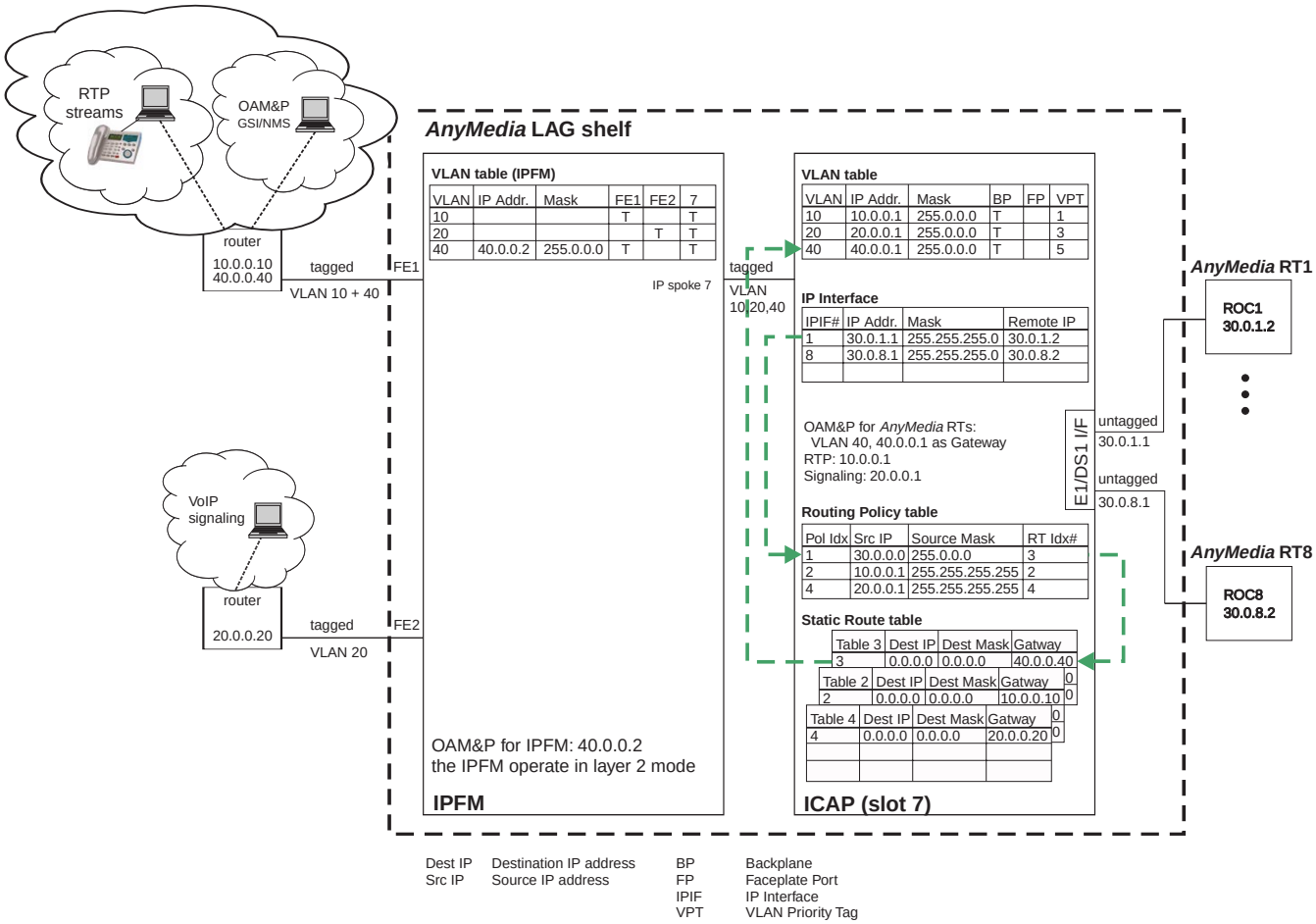
The diagram below shows the stand-alone mode (The ICAP is not controlled by the IPFM).

In this configuration the three data streams are forwarded to the FE1 port of the ICAP. Each data stream belongs to a separate VLAN.



Layer 3 VLAN provisioning via ICAP for multiple IP addresses

The next figure shows L2/L3 VLANs, where RTP, Signaling and OAM&P data streams of the ICAP in controlled mode can be sent to the next network node (IPFM, L2/L3 switch) via one line. To separate these data over two or three different ways each data stream can have a dedicated VLAN ID, which can be assigned to a dedicated IP address.



The following is a brief description of the example diagram above.

IP Interface Table (ICAP Subsystem turnup):

If a Remote Operations Channel is to be supported towards *AnyMedia* RTs then a unique IP subnet for each *AnyMedia* RT ROC must be set up. In the example above the first *AnyMedia* RT uses the ROC IP Interface 1 with the IP address 30.0.1.1 at the ICAP side and 30.0.1.2 at the *AnyMedia* RT side. All OAM traffic from the subtending *AnyMedia* RT will then be L3 routed in the OAM VLAN 40 upstream to the network.

Routing Policy Table:

All IP packets having a source IP address 30.x.x.x (30.0.0.0 / 255.0.0.0) will use the static route table 3. (RT Idx# 3).

Static Route Table: All IP packets (0.0.0.0 / 0.0.0.0) that are associated with RT Idx# 3 are routed to the gateway IP address 40.0.0.40. That is, in order to establish a connection between the ICAP and the gateway 40.0.0.40 an IP address in the same subnet has to be chosen.

VLAN Table (ICAP Subsystem turnup): Since there is only one physical interface (one MAC address) but several IP addresses on the ICAP, VLANs have to be assigned to the chosen IP addresses. In this example an IP address 40.0.0.1 with the Mask 255.0.0.0 will be assigned to a VLAN ID 40. This VLAN 40 is tagged forwarded to the IPFM over the backplane (BP) with the priority 5 (VPT).

VLAN Table (IPFM Subsystem turnup): Tagged ethernet frames with VLAN 40 arrive the IPFM on spoke 7 and go to the gateway through FE1. OAM&P packets for the IPFM get the IP address 40.0.0.2 that is also assigned to the VLAN 40.

□

Migration scenarios

Overview

Migration types

In this context, migration scenarios include the following:

- Migration from simplex to duplex IPFM mode
- Migration from duplex to simplex IPFM mode
- Migration of IP APs from controlled mode to stand-alone mode
- Migration of IP APs from stand-alone mode to controlled mode.
- Migration of IP APs from simplex to duplex mode
- Migration of IP APs from duplex to simplex mode
- Migration from an ATM xDSL system to an IP system (ATM AFM to IP-AFM).

□

Migration from simplex to duplex IPFM mode and vice versa

Migration from simplex to duplex IPFM mode

This procedure requires the attendance of a maintenance technician for inserting the second IPFM into the IPFM protection slot and, if the management port on the faceplate(MGMT) is used instead of an inband management channel, to replace the cable to the management port by a Y-cable.

After inserting the second IPFM and making the necessary cable changes, provision the system for duplex and then save the change to NVDS.

Migration from duplex to simplex IPFM mode

When migrating from duplex to simplex IPFM mode it is not necessarily required to have a maintenance technician on site, because the cable and the protection IPFM may be removed at a later point in time.

Check whether the IPFM in the preferred IPFM slot is the active one. If it is the active one, provision it for simplex mode. If it is not the active one, perform a manual side switch and then provision the active IPFM for simplex mode.

□

Migration of IP APs from controlled to stand-alone mode and vice versa

Overview

By default, IP APs come configured in controlled mode. When stand-alone mode is required, the controlled mode has to be changed during turn-up. Note that not all IP APs support stand-alone mode.

Migration from controlled mode to stand-alone mode

This migration requires attendance of a maintenance technician to connect the uplink cable to the faceplate and to enter data for the IP connection via the console port.

The control mode of an IP AP is changed from controlled mode to stand-alone mode via provisioning.

Two migration scenarios from controlled to stand-alone mode are possible:

- In configurations where an IP controller is present in the shelf, the IP controller with its connection to the GSI allows to easily provision the service parameters and to set the communications parameters, for example IP address, subnet mask, default gateways and routes. After reboot the pack is in stand-alone mode and is ready to connect to the GSI. Note that this migration scenario is currently only supported by ICAP and VoIP AP.
- In configurations where no IP controller is present in the shelf, the migration to stand-alone mode is based on running a script that supports you to set the management IP address, the mask and routes on the pack via its serial port. After execution of the script the system reboots in order to activate the new configuration. The rebooted pack is in stand-alone mode and is ready to connect to the GSI.

Note that after a system initialization the IP AP will come up in controlled mode because this is the default mode.

Migration from stand-alone mode to controlled mode

Here the presence of a maintenance technician is not required at the time of migration. The uplink cable can be disconnected at a later point in time.

The control mode of an IP AP is changed from stand-alone mode to controlled mode via provisioning.

Associated to the changed control mode, the pack reboots. Once the pack comes up in controlled mode, it is not accessible as an independent NE any longer via the configured management IP address. Do a ″Save to NVDS″ at the IPFM to store the AP configuration on the IPFM.

□

Migration of IP APs from simplex to duplex mode and vice versa

Migration of IP APs from simplex to duplex mode

Some IP AP types (e.g. the ICAP), may be protected.

The following scenarios may apply:

- Both IP APs in the future protection group are inserted and provisioned for simplex.
- One IP AP is inserted and provisioned for simplex mode, the protection slot is empty.

Migration of IP APs from duplex to simplex mode

For the migration of IP APs from duplex to simplex mode, it is assumed that both IP APs in the protection group are inserted and provisioned for duplex.

□

Migration from an ATM xDSL system to an IP system via IP-AFM

Migration from ATM AFM to IP-AFM

The IP-AFM supports the migration of ATM xDSL services to IP while preserving APs and shelves that are already in use. Note that this procedure is *service-affecting*.

Following steps are required for the migration scenario:

- Backup the database NVDS for ATM xDSL services on the ATM AFM
- Disconnect all cables from the ATM AFM
- Remove the ATM AFM(s) and insert the new IP-AFM(s) into the ATM AFM slots
- Perform a database restore from the NVDS on the IP-AFM via GSI
- Reconnect the cables and install the appropriate Ethernet uplink cables for the IP-AFM
- Verify software load for the IP-AFM
- Provision the IP-AFM and save this new configuration to the NVDS.

The IP-AFM supports also the uplink protection. In this case a second IP-AFM is required (active/standby) in a duplex mode configuration. The standby IP-AFM provides the redundant link for protection.

□

5 Technical specifications

Overview

Purpose

The *AnyMedia*® Access System in general complies with all standards and specifications listed in the APOG part *Overview*. This section provides the additional standards the IP-part of the *AnyMedia*® Access System complies with.

Contents

Standards compliance

IP-based standards compliance

The IP-part of the *AnyMedia*® Access System complies with standards from the following sources:

- Request for Comments (RFC)
- Institute of Electrical and Electronics Engineers (IEEE).

RFC specifications

Within the *AnyMedia*® Access System the applicable sections of the following Requests for Comments (RFCs) are considered:

- RFC854 Telnet Protocol Specification, J. Postel, J.K. Reynolds, May-01-1983. IETF Standard #8 STANDARD
- RFC1157 Simple Network Management Protocol (SNMP), J.D. Case, M. Fedor, M.L. Schoffstall, C. Davin, May-01-1990. IETF Standard #15 STANDARD
- RFC1901 Introduction to Community-based SNMPv2, SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996. Experimental
- RFC1905 Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996. Draft
- RFC1906 Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996. Draft
- RFC1907 Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996. Draft
- RFC2236 Internet Group Management Protocol, Version 2, W. Fenner, November 1997. Proposed
- RFC2327 SDP: Session Description Protocol, M. Handley, V. Jacobson, April 1998. Proposed
- RFC2328 OSPF Version 2, J. Moy, April 1998. IETF Standard #54 STANDARD
- RFC2396 Uniform Resource Identifiers (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L. Masinter, August 1998. Draft
- RFC2402 IP Authentication Header, S. Kent, R. Atkinson, November 1998. Proposed
- RFC2576 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, R. Frye, D. Levi, S. Routhier, B. Wijnen, March 2000. Proposed
- RFC2578 Structure of Management Information Version 2 (SMIv2), K. McCloghrie, D. Perkins, J. Schoenwaelder, April 1999. IETF Standard #58 STANDARD
- RFC2579 Textual Conventions for SMIv2, K. McCloghrie, D. Perkins, J. Schoenwaelder, April 1999. IETF Standard #58 STANDARD

- RFC2580 Conformance Statements for SMIv2, K. McCloghrie, D. Perkins, J. Schoenwaelder, April 1999. IETF Standard #58 STANDARD
- RFC2617 HTTP Authentication: Basic and Digest Access Authentication, J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, June 1999. Draft
- RFC2819 Remote Network Monitoring Management Information Base, S. Waldbusser, May 2000. IETF Standard #59 STANDARD
- RFC2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, H. Schulzrinne, S. Petrack, May 2000. Proposed
- RFC3164 The BSD syslog Protocol, C. Lonvick, August 2001. Informational
- RFC3261 SIP - Session Initiation protocol (SIP), June 2002.
- RFC3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP), June 2002.
- RFC3264 An Offer/Answer Model with the Session Description Protocol (SDP), June 2002.
- RFC3310 Hypertext Transfer Protocol (HTTP) Digest Authentication using Authentication and Key Agreements (AKA), September 2002.
- RFC3311 The Session Initiation Protocol UPDATE Method, September 2002.
- RFC3323 A Privacy Mechanism for the Session Initiation Protocol (SIP), November 2002.
- RFC3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, November 2002.
- RFC3550 RTP: A Transport protocol for Real-Time Applications, July 2003.

IEEE specifications

Within the *AnyMedia*® Access System the applicable sections of the following IEEE specifications are considered:

- IEEE Std 802.1d IEEE Standard for Local and metropolitan area networks: Media access control (MAC) Bridges
- IEEE Std 802.1p IEEE Standard for Local and metropolitan area networks—Supplement to Media access control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering
- IEEE Std 802.1q IEEE Standard for Local and metropolitan area networks: Virtual Bridged Local Area Networks
- IEEE Std 802.1w Common Specifications - Part 3: Media Access Control (MAC) Bridges: Amendment 2 - Rapid Reconfiguration
- IEEE Std 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

□

Glossary

Numerics

1N / 3N

Formats of packs which define the height according to the One GPN standard hardware requirement.

10Base-T

IEEE 802.3 standard for Ethernet transmission over unshielded twisted pair.

100Base-T

IEEE 802.3 standard for Ethernet transmission over unshielded twisted pair. 100Base-T or Fast Ethernet, supports data transfer rates of 100 Mbps.

100Base-FX

Version of Fast Ethernet (100 Mbps) over optical fiber.

A

a-wire

One of the two wires of a twisted a/b copper pair. The a/b copper pairs are used for subscriber lines connected for example with Z interfaces. The a-wire is sometimes called tip-wire.

AC

Alternating Current

Active pack

The IPFM performing the operational work. The active pack can reside in the preferred slot or the protected slot.

Active status condition message

Each status condition message contains access identifier, condition type, condition effect, and condition description. Currently active status conditions are listed chronologically (see also status condition).

ADM

Add/Drop Multiplexer

Administrative State

A nominal service state typically set by the operator. The administrative state is non-volatile data. It survives system crashes when saved to NVDS.

ADSL

Asymmetric Digital Subscriber Line

AID

Access identifier - AID is the address within a TL1 command that is used to identify the physical or logical entity (or entities) within a network element to which the command applies. It has the format of a unique component identifier followed by hierarchical addresses of components. For example, drop-{1}-{3}-{8} is an object representing the physical subscriber line #8 of the application pack in slot #3 in the *AnyMedia* Shelf #1.

AN

Access Node

ANSI

American National Standards Institute

***AnyMedia*® Access System**

The *AnyMedia*® Access System is an access network element which supports various narrowband, ATM xDSL and IP services, digital as well as analog.

AnyMedia LAG Shelf

The term *AnyMedia LAG Shelf* is generally used for an *AnyMedia* shelf with a high capacity backplane, independently of the physical design of the shelf. It houses COMDAC(s), CIU/CTU, AFM(s) IPFM(s) and application packs.

AP

Application pack - A 3N-sized pack which is located in any of the AP slots of the *AnyMedia*® Access System.

APOG

Applications, Planning, and Ordering Guide

Apparatus code (APP)

The apparatus code is an 8-byte item of ASCII information stored in the nonvolatile data storage (NVDS) of a pack (for example LPZ100, DTP500,...). It is a unique identifier which specifies the function of the pack.

Application pack (AP)

A circuit pack which is located in any of the AP slots and supports subscriber interfaces for certain services. Some examples for application packs are LPZ100, LPA416, LPU430.

Authentication

Process used to verify the integrity of transmitted data, especially that of a message.

Availability

The probability that a system is in operable state at a given instant in time.

B

b-wire

One of the two wires of a twisted a/b copper pair. The a/b copper pairs are used for subscriber lines. The b-wire is sometimes called ring-wire.

BORSCHT

BORSCHT is an abbreviation for interface functions provided by Z ports for POTS.

- Battery (Subscriber loop feeding)
- Overvoltage/Overcurrent protection
- Ringing (Ringing signal provided for subscriber's terminal)
- Supervision (Loop signaling)
- Coding/Decoding (PCM)
- Hybrid (2- to 4-wire conversion)
- Test (provide a test access to subscriber's line and line circuit).

Bridge

A network layer device that passes packets between two or more network segments that use the same data link communications protocol (OSI layer 2). The network segments appear as one segment to protocol levels higher than the data link layer.

Bridging

Port and subscriber line are connected during a test session.

C

CE

Communauté Européenne

Circuit pack

A general term for any plug-in unit that is determined > to be inserted into the slot of a shelf, regardless of the slot size (1N-sized or 3N-sized) and the functionality. Common packs and application packs are subsets of circuit packs.

Circuit testing

Verifies the ability of an AP port to provide proper transmission and signaling.

CIT

Craft Interface Terminal - The Craft Interface Terminal is used to enter and receive messages. A CIT emulation is running on the GSI.

CIT interface

Interface for the Craft Interface Terminal - A serial EIA-232C interface (9-pin Dsub) on the faceplate of the communication interface unit (CIU/CTU) where a craft interface terminal (CIT) or a graphical system interface (GSI) is connected to the *AnyMedia*® Access System.

CIU

Communication interface unit - This is a pack used to provide several OAM&P interface terminations to the *AnyMedia*® Access System.

CKC

Customer key code

C_L channel

Used to transfer information concerning operation, maintenance and activation/deactivation of the access transmission system (ATS) in both directions between the LT and the NT.

CLEI

Common language equipment ID code - The CLEI is a 10-character code assigned by Bellcore identifying each pack. The CLEI information relates to the function of the pack, the condition of use, the source document used in creating the CLEI code etc. If two packs have the same first seven characters in the CLEI code, then the packs are electrically and mechanically interchangeable. Knowledge of CLEI is useful in planning, engineering and provisioning.

CLI

Command line interpreter

CLIP

Calling line identification presentation - A supplementary service which provides the called party with the possibility of receiving identification of the calling party.

CLIR

Caller ID restriction

CN

Change Notification

CO

Central Office

Collocation

Grouping entities in the same physical location.

Comcode

The comcode is a unique nine-digit code with the ECI being represented by the digits 2 through 7. The comcode is used by various Alcatel-Lucent organizations for the ordering of components.

COMDAC

Common data and control - Pack which provides the central control and transmission fabric for the *AnyMedia*® Access System. The COMDAC supports multiple system applications, including V5.x switched services and analog and digital leased lines (ALL and DLL) and a variety of application packs.

Common pack

A circuit pack providing system functionality that is not limited to a specific application like POTS or ADSL. All circuit packs that are not defined as application packs, are common packs. Some examples for common packs are COMDAC, CIU, AFM, RGUs.

Configuration management

Consists of a set of functions to exercise control over elements in the network, including initialization, parameter setting, starting and stopping, and collection of information about the configuration.

Controlling entity

A controlling entity has a control relationship to another entity where the operational condition of the other (controlled) entity depends on the operational condition of the entity concerned.

CPE

Customer premises equipment - CPE covers the subscriber's installation and the subscriber's terminal.

CR

Critical

CRC-4 procedure

Cyclic redundancy check-4 procedure - A multiplication/division process, specified in ITU-T G.704, to provide additional protection against simulation of the frame alignment signal and capability for enhanced error monitoring.

Cross-connection

A term for a logical association between two objects, for example between a subscriber port and a network interface. A physical cross-connection may additionally be established in the case of a network interface where bandwidth allocation is done on a provisioning basis.

CTU

Craft test unit

Customer key code

The provisionable customer key code defines which customer specific settings are used by the *AnyMedia*® Access System.

D

DC

Direct Current

DDI

Direct dialing in

Degrowth

The removal of circuit packs or traffic from a system via a provisioning operation (may be accompanied by the physical removal of associated equipment, but this is not required).

Device

Any electrical part (IC, diode, capacitor, resistor, etc.) with distinct electrical characteristics. This term is used interchangeably with component.

DHCP

Dynamic Host Control Protocol (Defined in RFC 1541)
DHCP allows IP addresses to be assigned in three ways:
1) Manual Allocation: The network administrator keeps complete control over addresses by specifically assigning them to clients.
2) Automatic Allocation: The DHCP server permanently assigns an address from a pool of addresses.
3) Dynamic Allocation: The DHCP server assigns an address to a DHCP client for a limited period of time.

Distance-to-open

For deciding whether a line is broken (open), a distance-to-open measurement is to be implemented. Such a measurement could be based upon several techniques: capacitance or impedance measurement, or even pulse-reflection. TAP10x may produce parameters, with which the operator can decide on the location of the cable-fault (based on the operator's knowledge of the applied cable type).

DoS

Denial of service.

Downlink, uplink

In the *AnyMedia*® IP subsystem, any interfaces carrying IP traffic which are oriented towards the network are termed uplinks. Those interfaces which are oriented towards the subscriber (end-user) are termed downlinks. Typical uplinks are the GbE and FE interfaces of the IPFM. Typical downlinks are the VDSL lines. Whether a link is a downlink or uplink may depend on the relative viewpoint: From an AP point of view the backplane spokes are uplinks. From an IPFM point of view the same spokes are downlinks.

Download

A binary data transfer from the GSI to the *AnyMedia*® Access System.

Downstream, upstream

Those terms denote a direction relative to the network or the subscriber. Upstream is towards the network, downstream is towards the subscriber.

Downtime

Used to describe the time during which a system is not available for service. In engineering applications downtime is associated with unavailability.

Downtime per port

Downtime, in minutes per year, for a single bidirectional path terminating on an interface port on an add/drop multiplexer or a digital cross connect system. Any service interruption longer than 50 milliseconds contributes to this measure.

Drop

See subscriber loop.

Drop testing

Checks for opens, shorts, leakages to ground, foreign voltages, or other faults on the subscriber loop.

DS1

DS1 is a GR-303-like format

DSCP

Differentiated Services Code Point

DSP

Digital signal processor

DTE

Data Terminal Equipment

DTP500

Communication interface unit (CIU)

Duplex mode

A facility protection scheme in which two identical facilities (packs or feeders) are installed on a shelf; one is running in the active mode, the other is in the standby mode. The standby facility takes over when the active one fails or on an external command. Such a take-over (″protection switch″) guarantees that a facility failure does not disrupt the services. In the duplex IPFM context ‘Duplex Mode’ means, that the Protection Slot is provisioned in the IPFM data base to contain an IPFM.

E

E1

E1 is the standard acronym for the 2.048-Mbps interface defined in the ITU standards G.703/G.704.

ECI

Equipment catalog item - Equipment catalog item code is a 6-character code assigned by Bellcore identifying each pack. This code corresponds to the bar-coded label on the faceplate of the pack, and is uniquely equivalent to the CLEI code - for a given CLEI there is a unique ECI. It is used internally in the databases of external inventory systems for cataloging of equipment and is useful in accounting and inventory control.

Edge switch

A switch that is located at the meeting point between the access and the core network.

EIA-232C

American Standard for Serial Interface (the same as EIA-RS-232C; similar to V.24)

EIDR

Enhanced inventory data record - Enhanced inventory data record is a set of parameters that are stored in the non-volatile memory of packs. The parameters relate to the function performed by the pack, the manufacturing information, ordering information etc. that is of importance in provisioning a new service, maintaining the service, and in restoring the service quickly in event of a failure.

EMC

Electromagnetic Compatibility

End of life

The instant when a device parameter reaches a specified failure threshold. The failure threshold is device-dependent. For instance, an aluminum electrolytic capacitor reaches its end of life when its equivalent series resistance (ESR) exceeds twice its initial value.

EOC

Embedded Operations Channel

Equipment pair

The equipment pair of the TAP-B interface consists of the 2 wires towards the customer premises equipment (outward direction).

ES

Errored Seconds

ESIM

Ethernet subscriber interface module (LPE408)

ETS

European Telecommunication Standard

ETSI

European Telecommunication Standards Institute

External interface

Any operations or user interface system connected locally or remotely to the *AnyMedia*® Access System. For example: CIT, GSI, EMS.

F

Facility pair

The facility pair of the TAP-B interface consists of the 2 wires towards the application pack circuitry (inward direction).

Facility protection

The capability for a system to choose which signal from two facilities to pass along to the internal, unprotected transmission paths. A system switches from one facility to the other, for example, when the facility being used fails or when an administrator issues an OAM&P command.

Far end

The transmission termination or network element terminating the remote end of a feeder connected to the system. Examples include the edge switch and another *AnyMedia* shelf within a daisy chain. The far end is also referred to as remote end.

Fault management

Consists of a set of functions, such as testing, that enable the detection, isolation, and correction of abnormal operation of the telecommunications network and its environment.

FDI

Feeder Distribution Interface

FE

Fast Ethernet

FFU

Fan Filter Unit

FITL

Fiber In The Loop

Forced mode

Refers to the mode of changing to administrative primary service state OOS. In forced mode the resources are freed immediately and the administrative primary service state OOS is entered.

Forward direction

The direction followed by monitored user cells. Unlike the definition of upstream and downstream direction, the forward and backward directions are relative to a reference point (e.g., the point where a failure occurs).

FTP

File Transfer Protocol

Full duplex

Refers to the transmission of data in two directions simultaneously.

Full split

With full-split test access, transmission is interrupted in both the transmit and receive directions at the test access point and the tester is allowed to inject and look at the transmitted and received signals both in the equipment (towards the end-customer) and in the facility (towards the network) directions simultaneously.

G

GbE

Gigabit Ethernet

GND

Ground - Synonym for electrical potential of 0V.

GSI

Graphical System Interface - A user friendly front-end for communicating with a system. In the *AnyMedia*® Access System the GSI is installed on a Windows based Personal Computer and used for entering and receiving TL1 (Transaction Language 1) messages for narrowband applications and SNMP messages for ATM xDSL and IPFM applications. The GSI provides support for managing the *AnyMedia*® Access System in the following functional areas:

- Configuration management
- Fault management
- Performance management

- Security management
- Inventory management.

H

Half simplex

Refers to the transmission of data in just one direction at a time.

Half split

With half-split test access, transmission is interrupted in both the transmit and receive directions at the test access point, exactly as in full-split access. However, the tester is allowed to inject and look at the transmitted and received signals either in the equipment (towards the end-customer) direction or in the facility (towards the network) direction, but not in both directions simultaneously.

High-impedance state

This state refers to the Z interface and implies that the physical Z port circuit is disabled. Consequently no feeding current can flow from the Z interface to the subscriber's terminal, no loop scanning will be performed and no AC signal transmission is possible.

Hold-up time

The time during which a power supplies output voltage remains within specification following the loss of input power.

Hook flash

Hook flash is a signal of POTS. A hook flash signal is a short interruption of subscriber's loop, which is generated at subscriber's terminal. Hook flash signals are used to request additional service features (for example establishing a three party telephone conference).

HST

Hold service tone

I

ICAP

IP COMDAC application pack

ICC

Interchangeability code - The ICC is of the form Sm:n, where ″m″ is the issue number and ″n″ is the series number. This is used to accurately indicate the interchangeability among packs with the same pack name and apparatus code, but different manufacturing versions. In general, a pack can be replaced by another pack that has the same apparatus code and the same issue number regardless of the series number.

ICV

Integrity check value.

ID

Identification

IEEE

Institute of Electrical and Electronic Engineers

IGMP

Internet group management protocol

IIT

Incoming identification tone

IM

Installation Manual

Inbound, outbound

From a VoIP AP perspective outbound signaling messages are messages sent towards the network. In traditional telephony those messages are termed outgoing messages. Inbound messages are messages received from the network. In traditional telephony those messages are termed incoming messages.

Incoming, outgoing

In the traditional call context of a local exchange (LE), incoming calls are calls coming in from the network and being destined for a subscriber connected to this LE directly or via an access node (AN). Correspondingly, outgoing calls are calls initiated by subscribers being connected to the LE directly or via an AN and being forwarded towards the trunk network.

Inrush current

Inrush current is the current flowing at the moment when the power is switched on.

Installation time

The period of time beginning when the transfer of software to the peripheral pack starts. The interval ends at the point when the transfer of the peripheral image to the pack is completed for both peripheral processors and field programmable gate array (FPGAs). Peripheral SW version switch over is not included.

Inventory

Inventory is the summary of data stored on a pack in the NVDS during manufacturing which is used to identify the pack and its functionality.

Inventory management

Consists of a set of functions to track, report, and ensure adequate supplies of equipment.

Inward direction

See facility pair.

IP

Internet Protocol

IP Subsystem

IP subsystem is the part of the system to provide IP services. It consists of the IPFM, which is the controller of the IP subsystem, hosting the IP feeder interfaces also, the IP application packs and the associated parts of the backplane.

IP-AFM

IP ATM feeder multiplexer

IPFM

IP forwarding module

IS

In Service

ISP

Internet Service Provider

IT

IT is the synonym for a power distribution system having no direct connection to earth, the exposed conductive parts of the electrical installation are connected to a local earth.

ITU

International Telecommunication Union

J

Jabber

In this document Jabber is defined as condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Jitter

Short-term noncumulative variations of the significant instants of a digital signal from their ideal positions in time.The most significant form of jitter arises from imperfections in the circuitry, for example quantizing distortions in phase locked loops (PLL).

L

LACP

Link aggregation control protocol.

LAG

Line Access Gateway

LAN

Local Area Network

Latency

The minimum amount of time it takes for a token to circulate around the LAN token ring or FDDI ring in the absence of a data transmission. Latency is selected when provisioning data service in the *AnyMedia*® Access System.

LBO

Lightguide Buildout; the LBO is an optical attenuator used between ATM circuit packs in an ATM switch or multiplexer and the AFMOs in an *AnyMedia* shelf, or between separate AFMOs in multiple *AnyMedia* shelves in a daisy chain. LBO guarantees the proper signal level.

LCS

Local Customer Support

LE

Local Exchange

LED

Light Emitting Diode

Load

The total number of call attempts offered to a telecommunication system during a given interval of time.

Load set

The load image plus the site-dependent configuration data.

Local login

Login into the *AnyMedia*® Access System via the CIT or External System LAN 10BaseT interface from the collocated GSI or dumb terminal.

LOF

Loss of frame - A LOF condition is declared when an out of frame (OOF) condition persists for t seconds.

LOP

Loss of pointer - A LOP is declared when a valid pointer can not be obtained using the pointer interpretation rules for SONET/SDH.

LOS

Loss of signal

M

MAC

Media Access Control

Mainshelf

See *AnyMedia* Mainshelf.

MDF

Main Distribution Frame

MEA

Mismatch of Equipment

Megaco

Media gateway control protocol

MG

Media gateway

MGC

Media gateway controller

MGCP

Media gateway control protocol according to RFC3435

MIB

Management information base - Declaration of a collection of objects that defines the network or network element for a given interface protocol. For example, there is a MIB defined for access using the simple network management protocol (SNMP) and a different MIB defined for access using the protocol of the GR-303 Embedded Operations Channel (EOC).

MJ

Major

MMH

Media monitor host

MN

Minor

Monitoring

The operator can hear to the subscriber while the circuit is still operational and in bridged state. Additionally a speech connection can be established to allow to talk to the customer.

MSG

Message

N

NAM

Navis AnyMedia Element Management System - Represents computing facilities, specialized software and data storage facilities used to administer and maintain multiple network elements (NEs) distributed over a wide geographical area from a centralized location. Communication in both directions is accomplished via TL1 messages.

NCP

Network connection point - NCP is the point at subscriber site on which subscriber's installation and subscriber's line are connected.

NE

Network Element

NE name

The network element (NE) name is a unique provisioned name given to an AnyMedia shelf. This name is identified by the GSI as the site ID.

Non-revertive mode

Means, that a certain protected working system resource which has become faulty and thus caused a switch to or replacement by another resource is NOT reused automatically as working resource if the (temporarily) faulty resource returns back to operation. Instead of this the (former) protection resource is used further on as working resource. A switch back may take place later on, but is independent from the recovery of the

(temporarily) faulty resource.

Non-service-affecting

Refers to a condition not affecting the service at the time it is detected.

NSA

Non-Service Affecting

NT

Network termination - The equipment that terminates the access transmission system on the customer side. The most known network termination device is the NT1, that provides only physical layer functionality. Other network termination devices with more functionality are NT-N or NT-a/b.

NTP

Network Time Protocol

NVDS

Nonvolatile data storage - NVDS refers to that part of the database which is retained even after a power failure, for example provision parameters.

NVPS

Nonvolatile program storage - NVPS refers to nonvolatile memory used to store the load image.

O

OAM&P

Operations, Administration, Maintenance, and Provisioning

Off-hook

In the off-hook state the telephone is picked up. The off-hook state indicates the busy state.

On-demand tests

On-demand tests will be executed only by an operator TL1 command.

On-hook

In the on-hook state the telephone is not picked up. The on-hook state indicates the idle state.

OOS

Out Of Service

Operational condition

Reflects whether the entity concerned is able to take over operation or not. It depends on the service state.

Operational State

The operational state is determined autonomously by the system, often but not exclusively relative to an administrative state. It is volatile and is re-determined in case of recoveries.

Originating call

Originating call is the type of call initiated at the subscriber side.

Outgoing

See *Incoming*.

Overload

Any load which is greater than the nominal load for which the system is required to work without any performance degradation.

P

Pack

See circuit pack

PCM

Pulse Code Modulation

PDU

Protocol Data Unit - A PDU is a message of a given protocol comprising payload and protocol-specific control information, typically contained in a header. PDUs pass over the protocol interfaces which exist between the layers of protocols (per OSI model).

Performance management

Consists of a set of functions to evaluate and report on the behavior of telecommunication equipment and the effectiveness of the network and/or network elements (NEs).

Planned Side Switch

Planned side switches are side switches that are jointly and carefully prepared by both the active and protection IPFMs. I.e., there is some time to prepare the side switch in order to accomplish it with a minimum impact on service. Events that cause planned side switches include administrator command and software upgrade.

Platform

Items and functions in SW, HW and FW which are independent of the application.

PLC

Packet loss concealment

Port

Refers to the devices and functions built on or provided by a pack for one subscriber or line interface; sometimes referenced as circuit.

POTS

Plain old telephone service - Analog telephony service via a copper pair.

PP

Point-to-Point

ppm

parts per million

PPPoE

Point-to-Point Protocol over Ethernet

Preferred slot

In the IPFM context, the Preferred Slot is the slot to be used for simplex mode. For more details see “Slot designations” (p. 4-8)

Profiles

Profiles are a common feature of systems that are managed using SNMP. A profile is a fixed set of parameters with specific values that needs to be provisioned only once but that can be used by any number of system entities of the same type.

Protected configuration

The protection pack is provisioned but may be faulty or moved to OOS by the operator.

Protection pack

The mate of the active pack. The protection pack can reside in the preferred slot or the protection slot.

Protection slot

In the duplex IPFM context, the Protection Slot is the slot to be used by the second IPFM in duplex mode. For more details see “Slot designations” (p. 4-8)

Protection status

An indication which reflects the actual state of the pack protection.

Protection switch

A switch of the service from the service pack to the protection pack. A protection switch can be requested manually or driven by pack fault.

Protection switching

A reliability feature that causes service to switch to the backup equipment during faults or testing.

Provisioning

The process of providing the system with parameters needed to realize a specific customer and site specific behavior.

PSTN

Public Switched Telephone Network

Q

QMS

Quality Management System

Quality of service (QoS)

An indicator of the performance of a transmission system on the Internet and other networks. QoS is measured in transmission rate, error rates, latency, and other characteristics.

R

RAM

Random Access Memory

Regenerator

A transmission device between LT and NT. It enhances the transmission distance between LT and the NT. The regenerator is remote powered from the LT and is powering the NT. In ETR080 the number of regenerator between LT and NT is due to reasons of powering limited to one.

Relationship

A dependence between two entities concerning the operational condition where the operational condition of one entity depends on the operational condition of another entity. The relationship may be of two types:

- hierarchical relationship according to the provisioning and resource view where upperlying entities depend on underlying entities; that is underlying entities have to be provisioned first. This also implies that the operational condition of an upperlying entity depends on the operational condition of an underlying entity. If a pack is in a protected configuration, the EQUIPMENT-layer entity has more than one relationship to underlying PACKS-layer entities. The operational condition of the upperlying EQIPMENT layer entity is ″operational″, if at least one underlying entity is also ″operational″ and available for a protection switch.
- control relationship not necessarily a relationship between entities of different layers as the hierarchical relationship. It is a relationship of two entities where the operational condition of one of the entities (controlled entity) depends on the operational condition of the other (controlling) entity in such a way that the operational condition of the controlled entity is only ″operational″ if the operational condition of the controlling entity is also ″operational″.

Remote login

Login into the *AnyMedia*® Access System via LAN or External System LAN (over TCP/IP DCN) from NAM or GSI.

RGP

Ringing Generator Pack - The RGP is a dual slot ringing generator pack, which may be plugged in slot 40/41 and slot 42/43 of the AnyMedia LAG Shelf. The RGP in slot 40/41 drives ringing bus 0, while the RGP in slot 42/43 drives ringing bus 1.

Ringing protection mode

Two ringing sources (external or internal) on the AnyMedia LAG System are working in active/active protection mode. Each one provides a ringing voltage to a separate ringing bus. The power ringing is taken by the POTS APs from the ringing bus according to the load sharing scheme. If one ringing voltage on one ringing bus fails, all POTS AP take the ringing voltage from the remaining operational ringing bus.

Router

A LAN/WAN device that operates at OSI layers 1 (physical), 2 (data link), and 3 (network). Distinguished from a bridge by its capability to switch and route data based upon network protocols such as IP.

RSTP

Rapid spanning tree protocol.

RTP

Real time protocol

RTU

Remote Test Unit - An RTU is a testing equipment for subscriber lines. An RTU-2 is collocated to the system and performs test functions (application of test signals and measurements) under the control of a test system controller. An RTU-1 is collocated to the central office and not used in the 30 channel market.

S

SA

Service Affecting

SC

Station clock - An external 2048 kHz synchronization signal, according to ITU-T G.703.

SCC

Serial communication controller - Part of the communication processor module of the micro-controller MPC860. The SCC can be configured to implement different protocols. For most protocols, this corresponds to portions of the link layer (OSI layer 2). For a ROC (64-kbps timeslot of an E1 link), the SCC is configured to implement HDLC protocol in QMC-mode (QUICC multichannel controller mode).

SDP

Session description protocol

Security management

Consists of a set of functions that protect telecommunications networks and systems from unauthorized access by persons, acts, or influences, and to track and report access attempts.

Serial number

The serial number is a 12-character code uniquely identifying each pack and indicating the date and place of manufacture.

Service-affecting

Refers to a condition affecting the service at the time it is detected.

SFTP

Secure File Transfer Protocol

SID

System Identification

Side switch

The operation of deactivating an active pack and activating the stand-by pack.

Simplex mode

In the duplex IPFM context ‘Simplex Mode’ means, that the Protection Slot is not provisioned in the IPFM data base to contain an IPFM. In normal simplex operation, per convention the IPFM resides in the Preferred Slot. For more details see “Slot designations” (p. 4-8)

SIP

Session initiation protocol

SN

Serial Number

SNMP

Simple network management protocol - Used by the GSI/NAM for the *AnyMedia*® Access System subsystem for accessing the MIB objects.

SNMP TRAP

See TRAP.

Soft switch

In this information product used as a generic term to denote H.248 media gateway controllers as well as SIP Proxies.

Software package

At the architectural level, software packages are the primary vehicle for functional partitioning of the system. Software packages are configuration units of the system.

Software upgrade

Installing newer system software.

SPI

Security parameters index.

Standby pack

The protection pack is up-to-date with the provisioning information of the active pack and ready to take over operation with minimum service interruption. Its operational state is STBY. As long as this state is not left the protection pack will be kept up-to-date with the provisioning information.

Status condition

Report of a type of standing condition that reflects abnormal conditions or other anomalies that are not assigned a severity. Status conditions are necessary to indicate to the EMS or the operator that the system is in an unusual state, or is performing an action that may interfere with system operations, such as loop-back, software installation, or a forced or inhibited protection switch. A status condition is reported via a report-event TL1 message or an SNMP trap. Two kinds of status conditions are supported: Set/clear status conditions, which are active as long as the abnormal condition persists, and transient status conditions, which indicate a single abnormal event which is already cleared again.

STP

Spanning tree protocol.

Subscriber

Represents one customer entity on the LINES-layer.

Subscriber line

The a/b copper pair between a local exchange (LE) or access network system (AN) and the network connection point (NCP) (see ITU G.101).

Subscriber loop

Contains subscriber's line, subscriber's installation and subscriber's terminal; sometimes referenced as drop.

Subscriber loop feeding

Subscriber loop feeding will be provided for POTS to supply subscriber's terminal with power and for supervisioning of subscriber's loop.

SVGA

Super Video Graphics Adapter

SW

Software - Software is program data which is downloadable into the system.

T

TA

Terminal Adapter

TAP

Test access path - Two metallic test access paths, one consisting of two pairs (TAP-B) and the other of six pairs (TAP-A), provide both internal and external metallic test access to the ports and drops of the application packs.

TAP-B

Test Access Path B

TAP10x

Test Application Pack - TAP10x (that is TAP100, TAP100B, or TAP101) is the internal test head executing the measurements required for the drop.

TC

TAP Connected

TCA

Threshold Crossing Alert

TCP/IP

Transmission control protocol/Internet protocol - The combination of a network and transport protocol developed by ARPANET for internetworking IP-based networks.

TELNET

A remote terminal interface protocol which allows remote login capability into a system on a network from any other node on that network that is also running TELNET. TELNET is a TCP/IP application.

Terminating call

Terminating call is the type of call initiated at the network side of the network user interface. It comprises the build-up, speech and the tear-down phase. For a POTS call for example it starts with a message from the LE to the *AnyMedia*® Access System to seize a given subscriber and to supply ringing current.

Test session

A test session is the procedure including all necessary functions to test a subscriber. This includes the setup of the test path as well as the release of the test equipment. The test session runs in the *AnyMedia*® Access System.

Threshold crossing alert

A threshold is a value assigned by the system user to a certain desired level (for example errored seconds); when the level is exceeded, a threshold crossing alert is issued.

TID

Target Identifier

Tier 2 NMS

A generic term for a network management system (NMS) that can manage multiple kinds of network elements as a connected network. Tier 3 refers to element managers and Tier 1 refers to customer service support systems.

TRAP

An autonomous report in the simple network management protocol (SNMP), sent out by a network element towards an SNMP network manager, indicating an exceptional event.

Turn-up

The process of bringing the system or a system component to an operational state (it includes HW and SW installation as well as self diagnostics). After that the system can be provisioned for service and other operational functionality.

U

UART

Universal Asynchronous Receiver/Transmitter

UAS

Unavailable Second

UDP

User datagram protocol

Unavailability

In general, steady-state unavailability is defined as the fraction of time that the system is not available, or equivalently as the average downtime per year. Unavailability is often

expressed in minutes per year of downtime. In engineering applications, unavailability is frequently expressed in terms of its complement, that is the availability. For a digital channel, unavailability or downtime begins when the first 10 consecutive severely error seconds (SESs) occur, and it ends when the first of 10 consecutive non-SESs occur.

Unplanned side switch

Unplanned side switches are side switches that occur autonomously without any special preparation by the active and protection IPFMs. Events that cause unplanned side switches include software failure, hardware failure, pack removal.

Unprotected configuration

No protection pack is provisioned.

Uplink, downlink

See *Downlink*.

Upload

A binary data transfer from the *AnyMedia*® Access System to the GSI.

Upstream

The bitstream direction from the NT towards the network.

URI

Uniform resource identifier
Uniform resource identifiers are defined in RFC 2396. This RFC replaces the older definitions of the uniform resource locators URL per RFCs 1738 and 1808.

URL

See URI.

User identifier (login)

A unique character string consisting of up to 20 alphanumeric characters (ASCII) used by the system to identify a particular person or user.

V

VBD

Voice band data

VDSL

Very High Speed Digital Subscriber Line.

VID

VLAN Identifier

VLANs

Virtual local area networks

VSIM

VDSL subscriber interface module.

W **WAN**

Wide area network - A network that operates over a large region and commonly uses carrier facilities and services.

WFHBD

Weighted fair hashed bandwidth distributor.

WRR

Weighted round robin scheduling

Z **Z interface**

A 2-wire analog subscriber interface. It is used for connection of analog subscriber lines and will carry signals such as speech, voice-band analog data and multi-frequency push button signals, etc. In addition the Z interface must provide the DC feeding of subscriber's terminal and ordinary functions such as DC signaling, ringing, metering, etc., where appropriate (see ITU Q.551 2.1.1).

Index