IP over NBMA Working Group
Internet Draft
Expires: January 2000
draft-ietf-ion-multiprotocol-atm-04.txt

Dan Grossman
Motorola, Inc.
Juha Heinanen
Telia
July 1999

Multiprotocol Encapsulation over ATM Adaptation Layer 5

Status of this Memo

Abstract

This memo updates RFC 1483. It describes two encapsulations methods for carrying network interconnect traffic over AAL type 5 over ATM. The first method allows multiplexing of multiple protocols over a single ATM virtual connection whereas the second method assumes that each protocol is carried over a separate ATM virtual connection.

Copyright Notice

Applicability

This specification is intended to be used in implementations which use ATM networks to carry multiprotocol traffic among hosts, routers and bridges which are ATM end systems.

1. Introduction

Asynchronous Transfer Mode (ATM) wide area, campus and local area networks are used to transport IP datagrams and other connectionless traffic between hosts, routers, bridges and other networking devices. This memo describes two methods for carrying connectionless routed and bridged Protocol Data Units (PDUs) over an ATM network. The "LLC Encapsulation" method allows multiplexing of multiple protocols over a single ATM virtual connection (VC). The protocol type of each PDU is identified by a prefixed IEEE 802.2 Logical Link Control (LLC) header. In the "VC Multiplexing" method, each ATM VC carries PDUs of exactly one protocol type. When multiple protocols need to be transported, there is a separate VC for each.

The unit of transport in ATM is a 53 octet fixed length PDU called a cell. A cell consists of a 5 octet header and a 48 byte payload. Variable length PDUs, including those addressed in this memo, must be segmented by the transmitter to fit into the 48 octet ATM cell payload, and reassembled by the receiver. This memo specifies the use of the ATM Adaptation Layer type 5 (AAL5), as defined in ITU-T Recommendation I.363.5 [2] for this purpose. Variable length PDUs are carried in the Payload field of the AAL5 Common Part Convergence Sublayer (CPCS) PDU.

This memo only describes how routed and bridged PDUs are carried directly over the AAL5 CPCS, i.e., when the Service Specific Convergence Sublayer (SSCS) of AAL5 is absent. If Frame Relay Service Specific Convergence Sublayer (FR-SSCS), as defined in ITU-T Recommendation I.365.1 [3], is used over the CPCS, then routed and bridged PDUs are carried using the NLPID multiplexing method described in RFC 2427 [4]. The RFC 2427 encapsulation MUST be used in the special case that Frame Relay Network Interworking or transparent mode Service Interworking [9] are used, but is NOT RECOMMENDED for other applications. Appendix A (which is for information only) shows the format of the FR-SSCS-PDU as well as how IP and CLNP PDUs are encapsulated over FR-SSCS according to RFC 2427.

This memo also includes an optional encapsulation for use with Virtual Private Networks that operate over an ATM subnet.

If it is desired to use the facilities which are designed for the Point- to-Point Protocol (PPP), and there exists a point-to-point relationship between peer systems, then RFC 2364, rather than this memo, applies.

2. Conventions

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in RFC 2119 [10].

3. Selection of the Multiplexing Method

The decision as to whether to use LLC encapsulation or VC-multiplexing depends on implementation and system requirements. In general, LLC encapsulation tends to require fewer VCs in a multiprotocol environment. VC multiplexing tends to reduce fragmentation overhead (e.g., an IPV4 datagram containing a TCP control packet with neither IP nor TCP options exactly fits into a single cell).

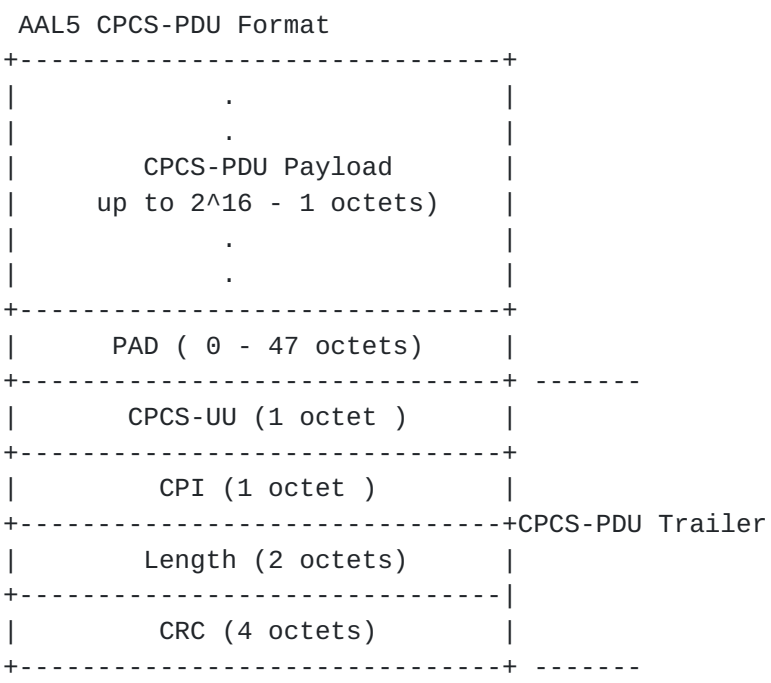
When two ATM end systems wish to exchange connectionless PDUs across an ATM Permanent Virtual Connection (PVC), selection of the multiplexing method is done by configuration. ATM connection control signalling procedures are used to negotiate the encapsulation method when ATM Switched Virtual Connections (SVCs) are to be used. [5] and [8] specify how this negotiation is done.

4. AAL5 PDU Format

For both multiplexing methods, routed and bridged PDUs MUST be encapsulated within the Payload field of an AAL5 CPCS-PDU.

ITU-T Recomendation I.363.5 [2] provides the complete definition of the AAL5 PDU format and procedures at the sender and receiver. The AAL5 message mode service, in the non-assured mode of operation MUST be used. The corrupted delivery option MUST NOT be used. A reassembly timer MAY be used. The following description is provided for information.

The format of the AAL5 CPCS-PDU is shown below:



The Payload field contains user information up to 2^16 - 1 octets.

The PAD field pads the CPCS-PDU to fit exactly into the ATM cells such that the last 48 octet cell payload created by the SAR sublayer will have the CPCS-PDU Trailer right justified in the cell.

The CPCS-UU (User-to-User indication) field is used to transparently transfer CPCS user to user information. The field is not used by the multiprotocol ATM encapsulation described in this memo and MAY be set to any value.

The CPI (Common Part Indicator) field aligns the CPCS-PDU trailer to 64 bits. This field MUST be coded as 0x00.

The Length field indicates the length, in octets, of the Payload field. The maximum value for the Length field is 65535 octets. A Length field coded as 0x00 is used for the abort function.

The CRC field is used to detect bit errors in the CPCS-PDU. A CRC-32 is used.

5. LLC Encapsulation

LLC Encapsulation is needed when more than one protocol might be carried over the same VC. In order to allow the receiver to properly process the incoming AAL5 CPCS-PDU, the Payload Field contains information necessary to identify the protocol of the routed or bridged PDU. In LLC Encapsulation, this information MUST be encoded

in an LLC header placed in front of the carried PDU.

Although this memo only deals with protocols that operate over LLC Type 1 (unacknowledged connectionless mode) service, the same encapsulation principle also applies to protocols operating over LLC Type 2 (connection-mode) service. In the latter case the format and contents of the LLC header would be as described in IEEE 802.1 and IEEE 802.2.

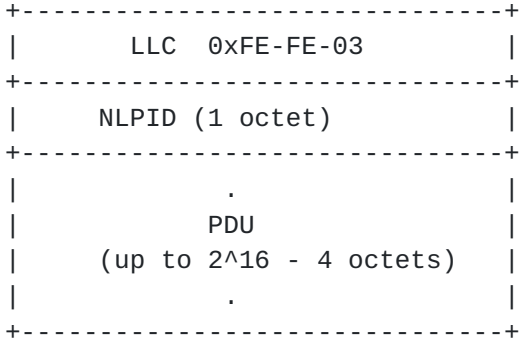
5.1. LLC Encapsulation for Routed Protocols

In LLC Encapsulation, the protocol type of routed PDUs MUST be identified by prefixing an IEEE 802.2 LLC header to each PDU. In some cases, the LLC header MUST be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. In LLC Type 1 operation, the LLC header MUST consist of three one octet fields:

In LLC Encapsulation for routed protocols, the Control field MUST be set to 0x03, specifying a Unnumbered Information (UI) Command PDU.

The LLC header value 0xFE-FE-03 MUST be used to identify a routed PDU in the ISO NLPID format (see [6] and Appendix B). For NLPID-formatted routed PDUs, the content of the AAL5 CPCS-PDU Payload field MUST be as follows:

Payload Format for Routed NLPID-formatted PDUs



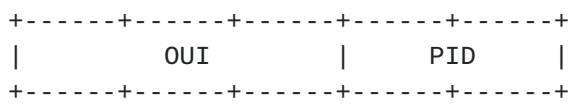
The routed protocol MUST be identified by a one octet NLPID field that is part of Protocol Data. NLPID values are administered by ISO and ITU-T. They are defined in ISO/IEC TR 9577 [6] and some of the currently defined ones are listed in Appendix C.

An NLPID value of 0x00 is defined in ISO/IEC TR 9577 as the Null Network Layer or Inactive Set. Since it has no significance within

the context of this encapsulation scheme, a NLPID value of 0x00 MUST NOT be used.

Although there is a NLPID value (0xCC) that indicates IP, the NLPID format MUST NOT be used for IP. Instead, IP datagrams MUST be identified by a SNAP header, as defined below.

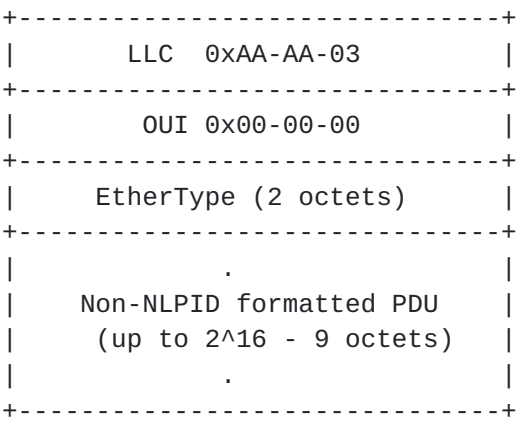
The presence of am IEEE 802.1a SNAP header is indicated by the LLC header value 0xAA-AA-03. A SNAP header is of the form



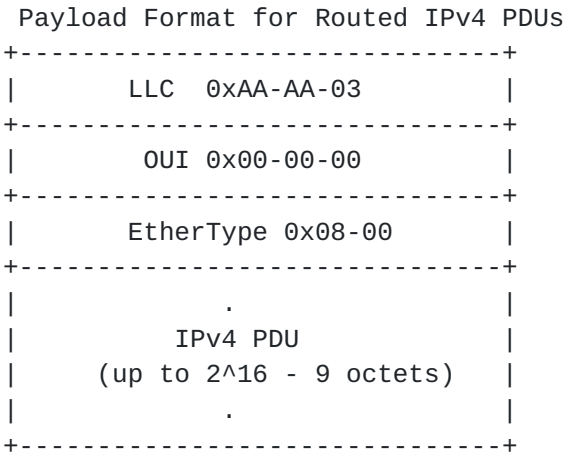
The SNAP header consists of a three octet Organizationally Unique Identifier (OUI) and a two octet Protocol Identifier (PID). The OUI is administered by IEEE and identifies an organization which administers the values which might be assigned to the PID. The SNAP header thus uniquely identifies a routed or bridged protocol. The OUI value 0x00-00-00 indicates that the PID is an EtherType.

The format of the AAL5 CPCS-PDU Payload field for routed non-NLPID Formatted PDUs MUST be as follows:

Payload Format for Routed non-NLPID formatted PDUs



In the particular case of an IPv4 PDU, the Ethertype value is 0x08-00, and the payload format MUST be:



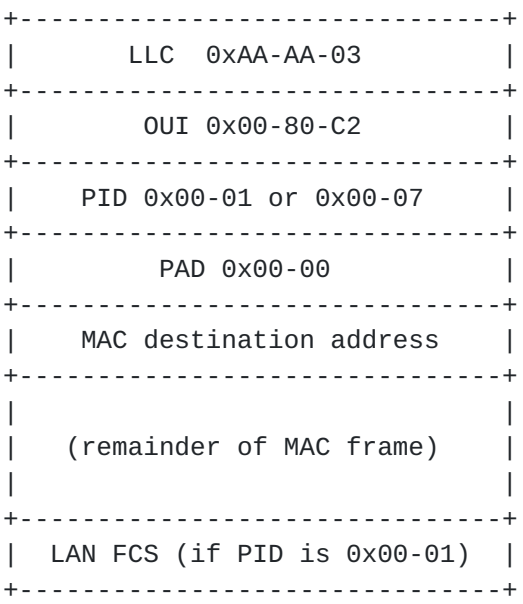
This format is consistent with that defined in RFC 1042 [7].

5.2. LLC Encapsulation for Bridged Protocols

In LLC Encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. The presence of the SNAP header MUST be indicated by the LLC header value 0xAA-AA-03. The OUI value in the SNAP header MUST be the 802.1 organization code 0x00-80-C2. The type of the bridged media MUST be specified by the two octet PID. The PID MUST also indicate whether the original Frame Check Sequence (FCS) is preserved within the bridged PDU. Appendix B provides a list of media type (PID) values that can be used in ATM encapsulation.

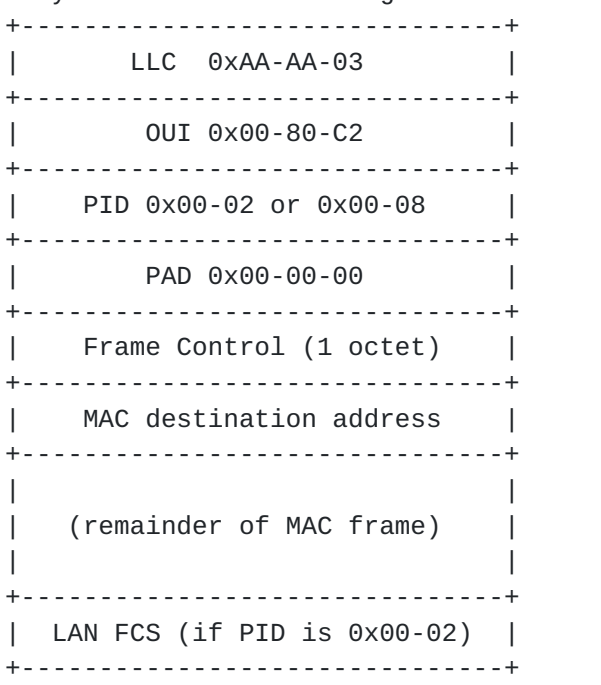
The AAL5 CPCS-PDU Payload field carrying a bridged PDU MUST have one of the following formats. The necessary number of padding octets MUST be added after the PID field in order to align the Ethernet/802.3 LLC Data field, 802.4 Data Unit field, 802.5 Info field, FDDI Info field or 802.6 Info field (respectively) of the bridged PDU to begin at a four octet boundary. The bit ordering of the MAC address MUST be the same as it would be on the LAN or MAN (e.g., in canoncial form for bridged Ethernet/IEEE 802.3 PDUs, but in 802.5/FDDI format for bridged 802.5 PDUs).

Payload Format for Bridged Ethernet/802.3 PDUs

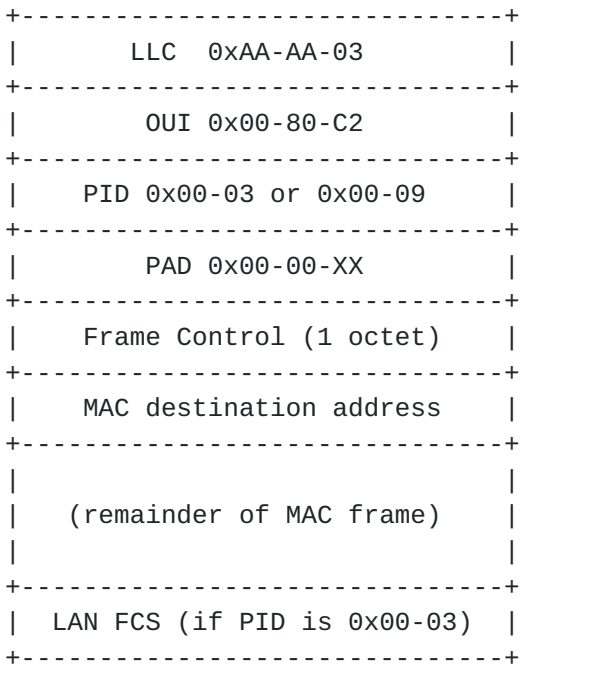


The Ethernet/802.3 physical layer requires padding of frames to a minimum size. A bridge that uses uses the Bridged Ethernet/802.3 encapsulation format with the preserved LAN FCS MUST include padding. A bridge that uses the Bridged Ethernet/802.3 encapsulation format without the preserved LAN FCS MAY either include padding, or omit it. When a bridge receives a frame in this format without the LAN FCS, it MUST be able to insert the necessary padding (if none is already present) before forwarding to an Ethernet/802.3 subnetwork.

Payload Format for Bridged 802.4 PDUs

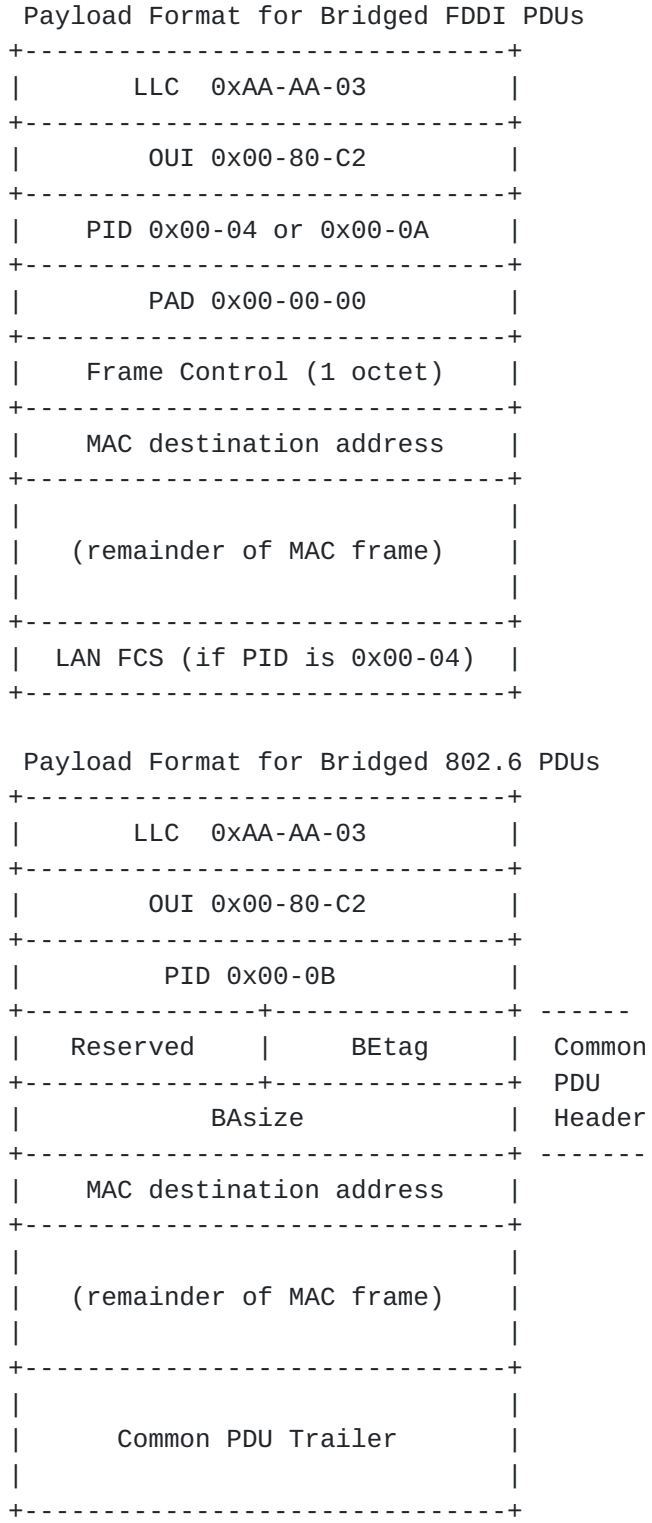


Payload Format for Bridged 802.5 PDUs



Since the 802.5 Access Control (AC) field has no significance outside the local 802.5 subnetwork, it is treated by this encapsulation as the last octet of the three octet PAD field. It MAY be set to any value by the sending bridge and MUST be ignored by the receiving

bridge.



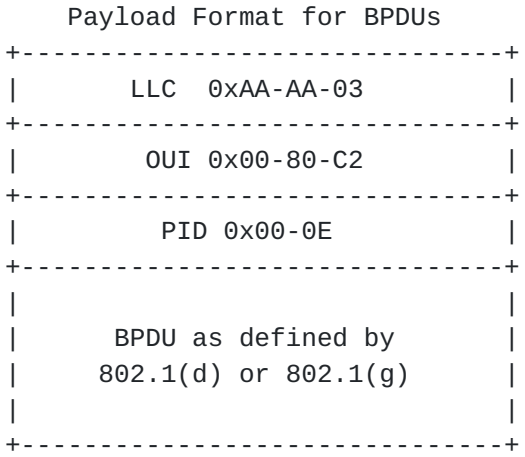
In bridged 802.6 PDUs, the presence of a CRC-32 is indicated by the CIB bit in the header of the MAC frame. Therefore, the same PID

value is used regardless of the presence or absence of the CRC-32 in the PDU.

The Common Protocol Data Unit (PDU) Header and Trailer are conveyed to allow pipelining at the egress bridge to an 802.6 subnetwork. Specifically, the Common PDU Header contains the BAsize field, which contains the length of the PDU. If this field is not available to the egress 802.6 bridge, then that bridge cannot begin to transmit the segmented PDU until it has received the entire PDU, calculated the length, and inserted the length into the BAsize field. If the field is available, the egress 802.6 bridge can extract the length from the BAsize field of the Common PDU Header, insert it into the corresponding field of the first segment, and immediately transmit the segment onto the 802.6 subnetwork. Thus, the bridge can begin transmitting the 802.6 PDU before it has received the complete PDU.

Note that the Common PDU Header and Trailer of the encapsulated frame should not be simply copied to the outgoing 802.6 subnetwork because the encapsulated BEtag value may conflict with the previous BEtag value transmitted by that bridge.

An ingress 802.6 bridge can abort an AAL5 CPCS-PDU by setting its Length field to zero. If the egress bridge has already begun transmitting segments of the PDU to an 802.6 subnetwork and then notices that the AAL5 CPCS-PDU has been aborted, it may immediately generate an EOM cell that causes the 802.6 PDU to be rejected at the receiving bridge. Such an EOM cell could, for example, contain an invalid value in the Length field of the Common PDU Trailer.



6. VC Multiplexing

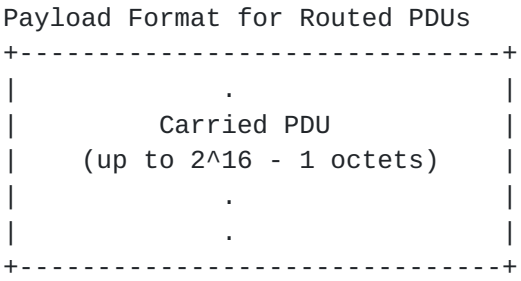
VC Multiplexing creates a binding between an ATM VC and the type of the network protocol carried on that VC. Thus, there is no need for protocol identification information to be carried in the payload of

each AAL5 CPCS-PDU. This reduces payload overhead and can reduce per-packet processing. VC multiplexing can improve efficiency by reducing the number of cells needed to carry PDUs of certain lengths.

For ATM PVCs, the type of the protocol to be carried over each PVC MUST be determined by configuration. For ATM SVCs, the negotiations specified in RFC 1755 [5] MUST be used.

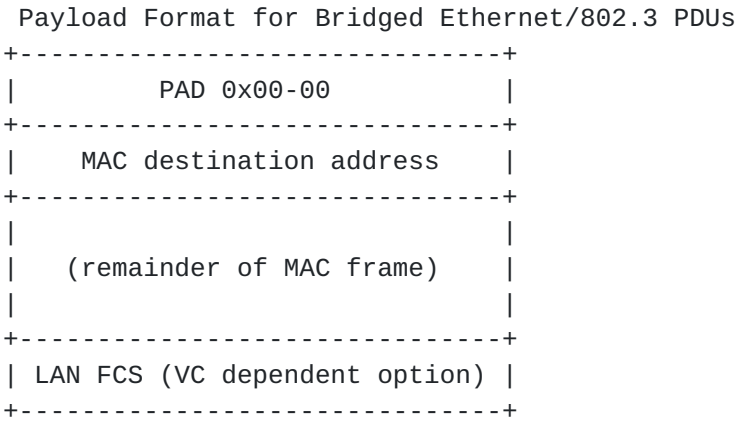
6.1. VC Multiplexing of Routed Protocols

PDUs of routed protocols MUST be carried as the only content of the Payload of the AAL5 CPCS-PDU. The format of the AAL5 CPCS-PDU Payload field thus becomes:

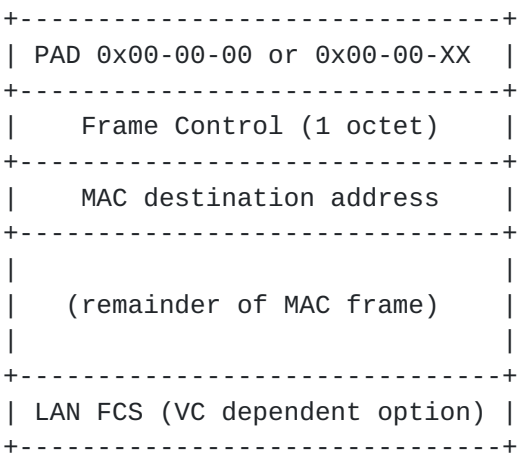


6.2. VC Multiplexing of Bridged Protocols

PDUs of bridged protocols MUST be carried in the Payload of the AAL5 CPCS-PDU exactly as described in section 5.2, except that only the fields after the PID field MUST be included. The AAL5 CPCS-PDU Payload field carrying a bridged PDU MUST, therefore, have one of the following formats.

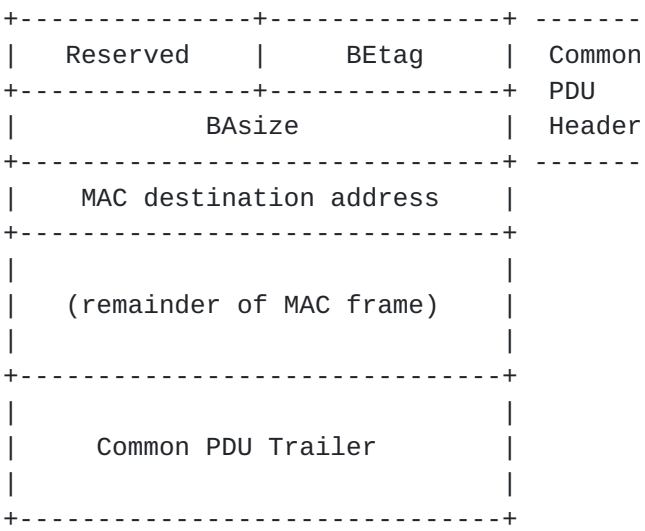


Payload Format for Bridged 802.4/802.5/FDDI PDUs

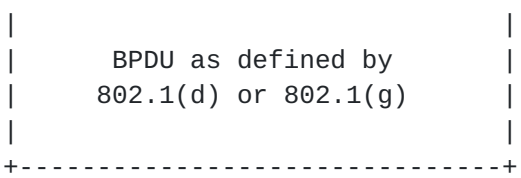


Note that the 802.5 Access Control (AC) field has no significance outside the local 802.5 subnetwork. It can thus be regarded as the last octet of the three octet PAD field, which in case of 802.5 can be set to any value (XX).

Payload Format for Bridged 802.6 PDUs



Payload Format for BPDUs



In case of Ethernet, 802.3, 802.4, 802.5, and FDDI PDUs the presense or absence of the trailing LAN FCS shall be identified implicitly by

the VC, since the PID field is not included. PDUs with the LAN FCS and PDUs without the LAN FCS are thus considered to belong to different protocols even if the bridged media type would be the same.

7. Bridging in an ATM Network

A bridge with an ATM interface that serves as a link to one or more other bridge MUST be able to flood, forward, and filter bridged PDUs.

Flooding is performed by sending the PDU to all possible appropriate destinations. In the ATM environment this means sending the PDU through each relevant VC. This may be accomplished by explicitly copying it to each VC or by using a point-to-multipoint VC.

To forward a PDU, a bridge MUST be able to associate a destination MAC address with a VC. It is unreasonable and perhaps impossible to require bridges to statically configure an association of every possible destination MAC address with a VC. Therefore, ATM bridges must provide enough information to allow an ATM interface to dynamically learn about foreign destinations beyond the set of ATM stations.

To accomplish dynamic learning, a bridged PDU MUST conform to the encapsulation described in section 4. In this way, the receiving ATM interface will know to look into the bridged PDU and learn the association between foreign destination and an ATM station.

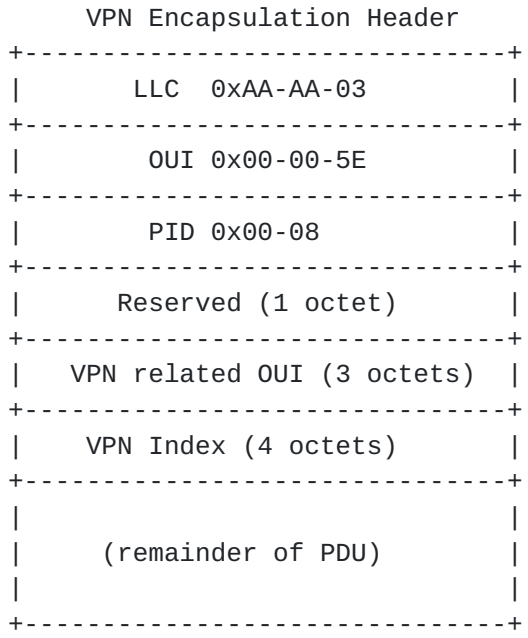
8. Virtual Private Network (VPN) identification

The encapsulation defined in this section applies only to Virtual Private Networks (VPNs) that operate over an ATM subnet.

A mechanism for globally unique identification of Virtual Private multiprotocol networks is defined in [11]. The 7-octet VPN-Id consists of a 3-octet VPN-related OUI (IEEE 802-1990 Organizationally Unique Identifier), followed by a 4-octet VPN index which is allocated by the owner of the VPN-related OUI. Typically, the VPN-related OUI value is assigned to a VPN service provider, which then allocates VPN index values for its customers.

8.1 VPN Encapsulation Header

The format of the VPN encapsulation header is as follows:



When the encapsulation header is used, the remainder of the PDU MUST be structured according to the appropiate format described in section 5 or 6 (i.e., the VPN encapsulation header is prepended to the PDU within an AAL5 CPCS SDU).

8.2 LLC-encapsulated routed or bridged PDUs within a VPN

When a LLC-encapsulated routed or bridged PDU is sent within a VPN using ATM over AAL5, a VPN encapsulation header MUST be prepended to the appropriate routed or bridged PDU format defined in sections 5.1 and 5.2, respectively.

8.3 VC multiplexing of routed or bridged PDUs within a VPN

When a routed or bridged PDU is sent within a VPN using VC multiplexing, the VPN identifier MAY either be specified a priori, using ATM connection control signalling or adminstrative assignment to an ATM interface, or it MAY be indicated using an encapsulation header.

If the VPN is identified using ATM connection control signalling, all PDUs carried by the ATM VC are associated with the same VPN. In this case, the payload formats of routed and bridged PDUs MUST be as defined in sections 6.1 and 6.2, respectively. If a PDU is received containing a VPN encapsulation header when the VPN has been identified using ATM signalling, the receiver MAY drop it and/or take other actions which are implementation specific. Specification of the mechanism in ATM connection control signalling for carrying VPN

identifiers is outside the scope of this Memo.

If a VPN identifier is administratively assigned to an ATM interface, then all PDUs carried by any ATM VCs within that interface are associated with that VPN. In this case, the payload formats of routed and bridged PDUs MUST be as defined in sections 6.1 and 6.2, respectively. If a PDU is received containing a VPN encapsulation header when the VPN identifier has been administratively assigned, the receiver MAY drop it and/or take other actions which are implementation specific. Specification of mechanisms (such as MIBs) for assigning VPN identifiers to ATM interfaces is outside the scope of this Memo.

If the VPN identifier is to be indicated using an encapsulation header, then a VPN encapsulation header MUST be prepended to the appropriate routed or bridged PDU format defined in sections 6.1 and 6.2, respectively.

9. Security Considerations

This memo defines mechanisms for multiprotocol encapsulation over ATM. There is an element of trust in any encapsulation protocol: a receiver must trust that the sender has correctly identified the protocol being encapsulated. There is no way to ascertain that the sender did use the proper protocol identification (nor would this be desirable functionality). The encapsulation mechanisms described in this memo are believed not to have any other properties that might be exploited by an attacker. However, architectures and protocols operating above the encapsulation layer may be subject to a variety of attacks. In particular, the bridging architecture discussed in section 7 has the same vulnerabilities as other bridging architectures.

System security may be affected by the properties of the underlying ATM network. The ATM Forum has published a security framework [12] and a security specification [13] which may be relevant.

Acknowledgements

This memo is an update of RFC 1483, which was developed by the IP over ATM working group, and edited by Juha Heinanen (then at Telecom Finland, now at Telia). The update was developed in the IP-over-NBMA (ION) working group, and Dan Grossman (Motorola) was editor and also contributed to the work on RFC 1483.

This material evolved from RFCs [1] and [4] from which much of the material has been adopted. Thanks to their authors Terry Bradley, Caralyn Brown, Andy Malis, Dave Piscitello, and C. Lawrence. Other

key contributors to the work included Brian Carpenter (CERN), Rao Cherukuri (IBM), Joel Halpern (then at Network Systems), Bob Hinden (Sun Microsystems, presently at Nokia), and Gary Kessler (MAN Technology).

The material concerning VPNs was developed by Barbara Fox (Lucent) and Bernhard Petri (Siemens).

References

[1] Piscitello, D. and Lawrence, C., "The Transmission of IP Datagrams over the SMDS Service". RFC 1209, Bell Communications Research, March 1991.

[2] ITU-T Recommendation I.363.5, "B-ISDN ATM Adaptation Layer (AAL) Type 5 Specification", August, 1996.

[3] ITU-T Recommendation I.365.1, "Frame Relaying Service Specific Convergence Sublayer (SSCS), November, 1993

[4] Brown, C., and Malis, A., "Multiprotocol Interconnect over Frame Relay". RFC 2427, September 1998.

[5] Perez-Maher et al, "ATM Signalling Support for IP over ATM", RFC 1755, February 1995

[6] Information technology - Telecommunications and Information Exchange Between Systems, "Protocol Identification in the Network Layer". ISO/IEC TR 9577, October 1990.

[7] Postel, J. and Reynolds, J., "A Standard for the Transmission of IP Datagrams over IEEE 802 Networks". RFC 1042, ISI, February, 1988.

[8] Maher, M, "IP over ATM Signalling - SIG 4.0 Update", RFC 2331, ISI, April 1998

[9] ITU-T Recommendation I.555, "Frame Relay Bearer Service Interworking", September, 1997.

[10] S. Bradner., "Key words for use in RFCs to Indicate Requirement Levels", RFC-2119, USC/Information Sciences Institute, March 1997.

[11] Fox, B. and Gleeson, B. "Virtual Private Networks Identifier",

work in progress.

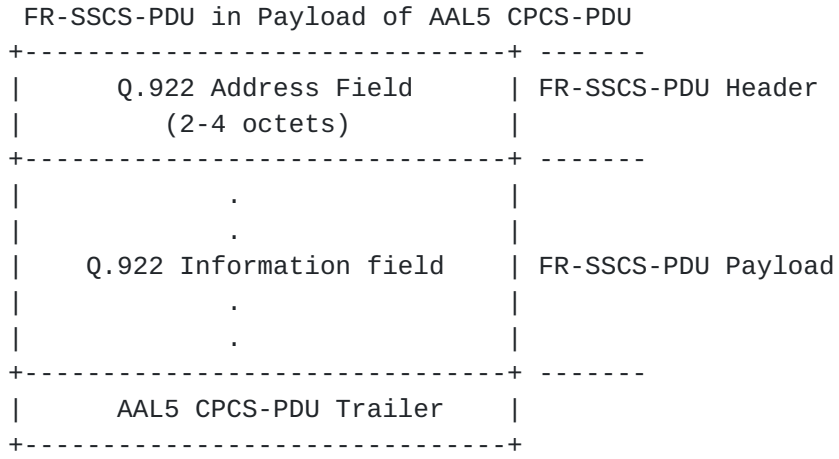
[12] The ATM Forum, "ATM Security Framework Version 1.0", af-sec-0096.000, February 1998

[13] The ATM Forum, "ATM Security Specification v1.0", af-sec-0100.001, February 1999

Appendix A. Multiprotocol Encapsulation over FR-SSCS

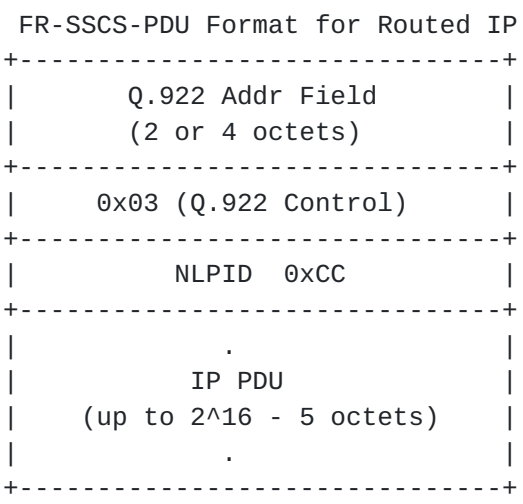
ITU-T Recommendation I.365.1 defines a Frame Relaying Specific Convergence Sublayer (FR- SSCS) to be used on the top of the Common Part Convergence Sublayer CPCS) of the AAL type 5 for Frame Relay/ATM interworking. The service offered by FR-SSCS corresponds to the Core service for Frame Relaying as described in I.233.

An FR-SSCS-PDU consists of Q.922 Address field followed by Q.922 Information field. The Q.922 flags and the FCS are omitted, since the corresponding functions are provided by the AAL. The figure below shows an FR-SSCS-PDU embedded in the Payload of an AAL5 CPCS-PDU.



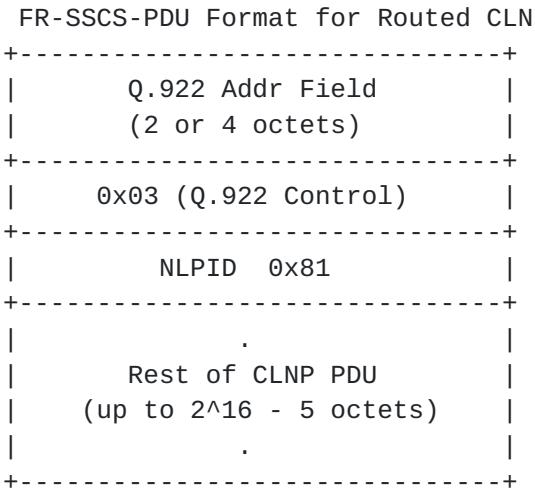
Routed and bridged PDUs are encapsulated inside the FR-SSCS-PDU as defined in RFC 2427. The Q.922 Information field starts with a Q.922 Control field followed by an optional Pad octet that is used to align the remainder of the frame to a convenient boundary for the sender. The protocol of the carried PDU is then identified by prefixing the PDU by an ISO/IEC TR 9577 Network Layer Protocol ID (NLPID).

In the particular case of an IP PDU, the NLPID is 0xCC and the FR-SSCS-PDU has the following format:



Note that according to RFC 2427, the Q.922 Address field MUST be either 2 or 4 octets, i.e., a 3 octet Address field MUST NOT be used.

In the particular case of a CLNP PDU, the NLPID is 0x81 and the FR-SSCS-PDU has the following format:



Note that in case of ISO protocols the NLPID field forms the first octet of the PDU itself and MUST not be repeated.

The above encapsulation applies only to those routed protocols that have a unique NLPID assigned. For other routed protocols (and for bridged protocols), it is necessary to provide another mechanism for easy protocol identification. This can be achieved by using an NLPID value 0x80 to indicate that an IEEE 802.1a SubNetwork Attachment Point (SNAP) header follows.

See RFC 2427 for more details related to multiprotocol encapsulation over FRCS.

Appendix B. List of Locally Assigned values of OUI 00-80-C2

with preserved FCS	w/o preserved FCS	Media
0x00-01	0x00-07	802.3/Ethernet
0x00-02	0x00-08	802.4
0x00-03	0x00-09	802.5
0x00-04	0x00-0A	FDDI
0x00-05	0x00-0B	802.6
	0x00-0D	Fragments
	0x00-0E	BPDUs

Appendix C. Partial List of NLPIDs

0x00	Null Network Layer or Inactive Set (not used with ATM)
0x80	SNAP
0x81	ISO CLNP
0x82	ISO ESIS
0x83	ISO ISIS
0xCC	Internet IP

Appendix D. Applications of multiprotocol encapsulation

Mutiprotocol encapsulation is necessary, but generally not sufficient, for routing and bridging over the ATM networks. Since the publication of RFC 1483 (the predecessor of this memo), several system specifications were developed by the IETF and the ATM Forum to address various aspects of, or scenarios for, bridged or routed protocols. This appendix summarizes these applications.

1) Point-to-point connection between routers and bridges -- multiprotocol encapsulation over ATM PVCs has been used to provide a simple point-to-point link between bridges and routers across an ATM network. Some amount of manual configuration (e.g., in lieu of INARP) was necessary in these scenarios.

2) Classical IP over ATM -- RFC 2225 (formerly RFC 1577) provides an environment where the ATM network serves as a logical IP subnet (LIS). ATM PVCs are supported, with address resolution provided by INARP. For ATM SVCs, a new form of ARP, ATMARP, operates over the ATM network between a host (or router) and an ATMARP server. Where servers are replicated to provide higher availability or performance, a Server Synchronization Cache Protocol (SCSP) defined in RFC 2335 is used. Classical IP over ATM defaults to the LLC/SNAP encapsulation.

3) LAN Emulation -- The ATM Forum LAN Emulation specification provides an environment where the ATM network is enhanced by LAN Emulation Server(s) to behave as a bridged LAN. Stations obtain

configuration information from, and register with, a LAN Emulation Configuration Server; they resolve MAC addresses to ATM addresses through the services of a LAN Emulation Server; they can send broadcast and multicast frames, and also send unicast frames for which they have no direct VC to a Broadcast and Unicast Server. LANE uses the VC multiplexing encapsulation foramts for Bridged Etherent/802.3 (without LAN FCS) or Bridged 802.5 (without LAN FCS) for the Data Direct, LE Multicast Send and Multicast Forward VCCS. However, the initial PAD field described in this memo is used as an LE header, and might not be set to all '0'.

4) Next Hop Resolution Protocol (NHRP) -- In some cases, the constraint that Classical IP over ATM serve a single LIS limits performance. NHRP, as defined in RFC 2332, extends Classical to allow 'shortcuts' over a an ATM network that supports several LISs.

5) Multiprotocol over ATM (MPOA) -- The ATM Forum Multiprotocol over ATM Specification integrates LANE and NHRP to provide a generic bridging/routing environment.

6) IP Multicast -- RFC 2022 extends Classical IP to support IP multicast. A multicast address resolution server (MARS) is used possibly in conjunction with a multicast server to provide IP multicast behavior over ATM point-to-multipoint and/or point to point virtual connections.

7) PPP over ATM -- RFC 2364 extends multiprotocol over ATM to the case where the encapsulated protocol is the Point-to-Point protocols. Both the VC based multiplexing and LLC/SNAP encapsulations are used. This approach is used when the ATM network is used as a point-to-point link and PPP functions are required.

Appendix E Differences from RFC 1483

This memo updates RFC 1483. It was intended to remove anachronisms, provide clarifications of ambiguities discovered by implementors or created by changes to the base standards, and advance this work through the IETF standards track process. A number of editorial improvements were made, the RFC 2119 [10] conventions applied, and the current RFC boilerplate added. The following substantive changes were made. None of them is believed to obsolete implementations of RFC 1483:

-- usage of NLPID encapsulation is clarified in terms of the RFC 2119 conventions

-- a pointer to RFC 2364 is added to cover the case of PPP over ATM

-- RFC 1755 and RFC 2331 are referenced to describe how encapsulations are negotiated, rather than a long-obsolete CCITT (now ITU-T) working document and references to work then in progress

-- usage of AAL5 is now a reference to ITU-T I.363.5. Options created in AAL5 since the publication of RFC 1483 are selected.

-- formatting of routed NLPID-formatted PDUs (which are called "routed ISO PDUs" in RFC 1483) is clarified

-- clarification is provided concerning the use of padding between the PID and MAC destination address in bridged PDUs and the bit ordering of the MAC address.

-- clarification is provided concerning the use of padding of Ethernet/802.3 frames

-- a new encapuslation for VPNs is added

-- substantive security considerations were added

-- a new appendix D provides a summary of applications of multiprotocol over ATM

Author's Addresses

Dan Grossman
Motorola, Inc.
20 Cabot Blvd.
Mansfield, MA 02048
Email: dan@dma.isg.mot.com

Juha Heinanen
Telia Finland
Myyrmaentie 2
01600 Vantaa, Finland
Email: jh@telia.fi

Full Copyright Statement