AF-MPOA-0129.000

TITLE: Final Ballot Version of MPOA-VPN

EDITOR: Bernhard Petri, Siemens
Phone: +49 89 722-34578
Fax: +49 89 722-62366
E-mail: bernhard.petri@icn.siemens.de

DATE: July 26-30, 1999; New Orleans, Louisiana

ABSTRACT: This specification provides for the letter ballot version of the

"MPOA v1.1 Addendum on Virtual Private Network Support"

(MPOA-VPN).

NOTICE: This contribution has been prepared to assist the ATM Forum. This proposal is made by Siemens as a basis of discussion. This contribution should not be construed as a binding proposal on Siemens. Specifically, Siemens reserves the right to amend or modify the statements contained herein.

This page is intentionally blank.

The ATM Forum

Technical Committee

MPOA v1.1 Addendum on VPN Support

AF-MPOA-VPN-0129.000

Final Ballot

August, 1999

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and The ATM Forum is not responsible for any errors. The ATM Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither The ATM Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by The ATM Forum or the publisher as a result of reliance upon any information contained in this publication.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

- Any express or implied license or right to or under any ATM Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
- Any warranty or representation that any ATM Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
- Any form of relationship between any ATM Forum member companies and the recipient or user of this document.

Implementation or use of specific ATM standards or recommendations and ATM Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in The ATM Forum.

The ATM Forum is a non-profit international organization accelerating industry cooperation on ATM technology. The ATM Forum does not, expressly or otherwise, endorse or promote any specific products or services.

NOTE: The user's attention is called to the possibility that implementation of the ATM interoperability specification contained herein may require use of an invention covered by patent rights held by ATM Forum Member companies or others. By publication of this ATM interoperability specification, no position is taken by The ATM Forum with respect to validity of any patent claims or of any patent rights related thereto or the ability to obtain the license to use such rights. ATM Forum Member companies agree to grant licenses under the relevant patents they own on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. For additional information contact:

The ATM Forum
Worldwide Headquarters
2570 West El Camino Real, Suite 304
Mountain View, CA 94040-1313
Tel: +1-650-949-6700
Fax: +1-650-949-6705

Acknowledgement

Much work went into the development of this specification. It could not have been completed without the ATM Forum contributions and the participation of many people in the LANE/MPOA working group. In particular, the Editor would like to recognize the following members who made significant contributions.

Barbara Fox

Neil Lacey

Jim Logan

Scott Brim

Matt Squire (LANE/MPOA-chair)

Hiroshi Suzuki

Shigeki Yamano

Srinivasan Balaji

Rohit Chhapolia

Kedar Deshpande

Ali Kujoory

Brenda O'Shaunessey

Kuo-Hui Liu

Vijay Srinivasan

John Drake

Joel Halpern

Sung Hei Kim

Jim Luciani

The assistance by these members and all that participated in the LANE/MPOA working group is greatly appreciated.

Bernhard Petri, Editor.

Contents

1. INTRODUCTION..6
1.1 REFERENCES 6
2. TERMS AND DEFINITIONS 7
2.1 DEFINITIONS..7
2.2 ACRONYMS AND ABBREVIATIONS 7
3. DESCRIPTION OF MPOA VPN SUPPORT 8
3.1 INTRODUCTION 8
3.2 METHODS TO IDENTIFY TRAFFIC AS BELONGING TO A VPN..9
3.3 CONFIGURATION 9
3.4 MPOA OPERATION..9
3.5 INTEROPERABILITY WITH DEVICES WITHOUT VPN SUPPORT 10
3.6 THE DEFAULT ROUTING INSTANCE..11
4. VPN SUPPORT SPECIFICATION..12
4.1 CONFIGURATION PARAMETERS 12
4.2 MPC-MPS DEVICE DISCOVERY..12
4.3 MPOA RETRY MECHANISM 12
4.4 DETAILED MPC BEHAVIOR 13
4.4.1 Introduction..13
4.4.2 Inbound Data Flow..13
4.4.3 Outbound Data Flow 14
4.5 DETAILED MPS BEHAVIOR..15
4.6 KEEP-ALIVE PROTOCOL..15
4.7 CACHE MAINTENANCE 16
4.8 CONNECTION MANAGEMENT 16
4.9 ERROR HANDLING PROCEDURES 16
5. FRAME FORMATS..17
5.1 MPOA DEVICE CAPABILITIES TLV..17
5.2 NHRP DEVICE CAPABILITIES EXTENSION..17
5.3 VPN KEEP-ALIVE EXTENSION..18
5.4 ADDITIONAL MPOA ERROR CODES..18
6. USE OF THE GIT IE FOR INDICATION OF THE VPN-ID DURING ATM CONNECTION ESTABLISHMENT 19
ANNEX A: VIRTUAL PRIVATE NETWORKS IDENTIFIER..22
ANNEX B: VPN ENCAPSULATION..28
APPENDIX 1: EXAMPLE FRAME FORMATS FOR VPN ENCAPSULATION 31

List of Figures

Figure 1: An Example of a Multi Layer VPN 8
Figure 2: MPOA Support for VPNs 10
Figure 3: MPOA Device Capabilities TLV Format 17
Figure 4: NHRP VPN Capability Extension Format 17
Figure 5: VPN Keep-Alive Extension Format 18
Figure 6: Coding of the GIT Information Element 19
Figure 7: Coding of the ATM Forum MPOA VPN Identifier 21
Figure 8: VPN Encapsulation 31
Figure 9: VPN Encapsulation of MPOA Control Messages 31
Figure 10: VPN Encapsulation for IP Packets 32
Figure 11: VPN Encapsulation for MPOA Tagged Encapsulation 32

List of Tables

Table 4-1: Ingress Cache Entries for VPN-aware MPCs 13
Table 4-2: Egress Cache Without Tags 14
Table 4-3: Egress Cache With Tags 14

1. Introduction

[Informative]

This document addresses the support of a Virtual Private Network (VPN) service in an MPOA network ("MPOA-VPN"). This Internetwork layer VPN may use a private address space which overlaps with that of another VPN or the Public Internet. In support of these private Internetwork layer address spaces, VPNs provide multiple virtual independent addressing and routing realms over the same physical network.

A major task of the MPOA VPN service is identifying the routing to be used for forwarding a particular control or data PDU. A globally unique identifier will be used to describe the instance. This document describes the transfer and processing of the VPN Identifier which identifies a VPN in a globally unique manner.

This MPOA VPN specification is developed in parallel and in cooperation with a number of related specifications:

- The basic concept for a generic VPN identification based on a globally unique ID (cf. Annex A).
- A per packet LLC/SNAP based transfer of the VPN-ID via an ATM connection (cf. Annex B)
- NHRP support for VPNs
- Transfer of the VPN-ID via signalling is specified for DSS2, and for ATM Forum UNI 4.0 signalling.

1.1 References

[LANE] "LAN Emulation over ATM Version 2.0", ATM Forum. af-lane-0084.000, John D. Keene, Dated: July 1997.

[MPOAv1.1] "Multiprotocol over ATM Version 1.1", ATM Forum. af-mpoa-0114.000, B. Petri, Dated: May 1999.

[Q.2941.1] ITU-T Recommendation Q.2941.1, "DSS2 Generic Identifier Transport", Part 1

[RFC 1483] "Multiprotocol Encapsulation over ATM Adaptation Layer 5, IETF RFC 1483, J. Heinanen, Dated: July 1993.

[RFC 2332] "Next Hop Resolution Protocol", IETF RFC 2332, J. Luciani et al., Dated: April 1998

2. Terms and Definitions

[Informative]

2.1 Definitions

Virtual Private Network (VPN):

In the context of this specification, the term "Virtual Private Network" (VPN) is a method of emulating a private network over a shared infrastructure.

VPN-aware:

A "VPN-aware" MPOA device is an MPOA device that implements the MPOA enhancements as defined in this specification.

Non-VPN-aware:

A "Non-VPN-aware" MPOA entity is an MPOA entity which is deployed as part of a single VPN, but is not VPN-aware. Restrictions applying to non-VPN-aware entities are outlined in Section 3.5 below.

VPN encapsulation:

An LLC/SNAP based transfer of the VPN-ID via an ATM connection as specified in Annex B below.

VPN signalling:

An indication of the VPN-ID through signalling during the establishment of an ATM connection as outlined in Section 6 below.

2.2 Acronyms and Abbreviations

The acronyms and abbreviations of [MPOAv1.1] apply. In addition, the following acronyms and abbreviations are used:

ID	IDentifier
GIT	Generic Identifier Transport
OUI	Organizationally Unique Identifier (see IEEE 802:1990)
VPN	Virtual Private Network

3. Description of MPOA VPN Support

[Informative]

3.1 Introduction

This specification adds VPN support to MPOA. Figure 1 illustrates the reference model for VPN support. In the model, there are multiple VPNs on a single ATM network. An MPC may be shared by multiple users of multiple VPNs. The edge device is responsible for mapping traffic into a particular VPN. The most straightforward method is to map a set of access interfaces (e.g. physical interface for Ethernet or Token Ring, DLCIs for Frame Relay, VCCs for ATM) into a VPN. Other methods of mapping traffic to a VPN may be used, and the choice of a particular algorithm is outside the scope of this specification.

Each VPN is represented at the edge device by a set of logical interfaces to the ATM network. The edge device maintains logically independent forwarding databases for each VPN. Similarly, routers on the ATM network which support multiple VPNs must maintain independent forwarding databases for each VPN, and must run separate instances of their routing protocols. When an edge device is connected to one or more router(s) supporting multiple VPNs, there is a default data path for each VPN. The default data paths may or may not traverse the same ATM VCC.

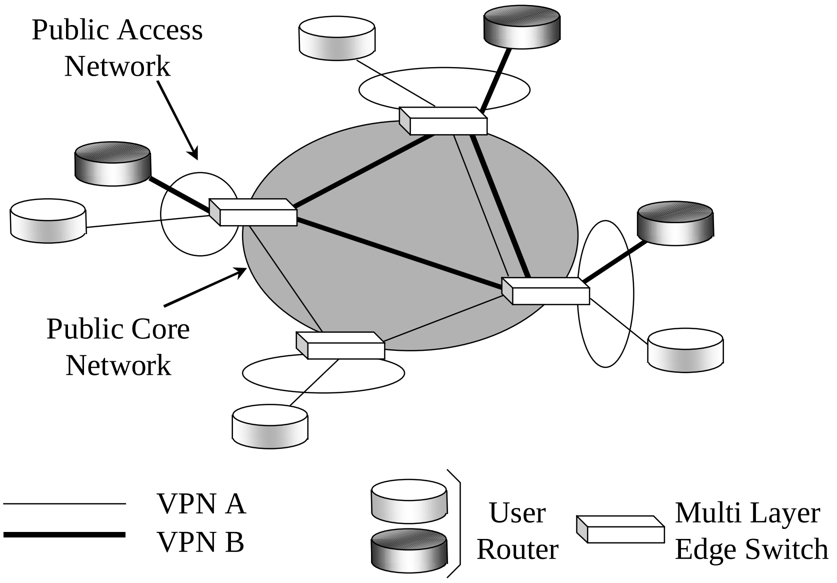

Figure 1: An Example of a Multi Layer VPN

An MPC normally performs flow identification based on the (destination internetwork address, MPS) combination. When there are multiple VPNs between an MPC and MPS, this method of flow detection is not sufficient because internetwork addresses are not guaranteed to be unique across multiple VPNs. Standard MPOA resolution is insufficient for the same reason.

This specification defines enhancements to [MPOAv1.1] to support multiple VPNs in a single MPOA device. These enhancements are backward compatible and provide an easy migration from a non-VPN-aware MPOA network to a VPN-aware MPOA network. This specification builds on the ideas outlined in Annex A and Annex

B. Specifically, each VPN is assumed to have a unique VPN identifier (VPN-ID) that can be used to identify frames or VCCs as belonging to a particular VPN, and there exist methods for communicating this VPN-ID within NHRP.

3.2 Methods to Identify Traffic as Belonging to a VPN

Among other things, MPOA defines the procedures for transmitting MPOA control messages over control VCCs and transmitting data packets over shortcut VCCs. In a network with multiple VPNs, each control frame and each packet must be associated with a specific VPN. This specification defines three methods by which a frame (control or data) may be associated with a VPN.

a) Indication of the VPN via ATM signalling

The VPN-ID of the VPN may be indicated via ATM signalling at the establishment of an ATM connection. If the VPN-ID is indicated via ATM signalling, then the established ATM connection can only be used for the particular VPN identified by the VPN-ID. All PDUs received via that ATM connection must belong to that particular VPN.

b) Indication of the VPN via encapsulation

The VPN-ID of the VPN may be included in an LLC/SNAP based encapsulation header for each packet. The formats for VPN encapsulation are included and exemplified in Annex B and Appendix 1. This method allows packets from different VPNs to be multiplexed onto the same ATM connection.

c) Indication of the VPN via system administration

VPN-IDs may be administratively assigned. A VPN-ID may be assigned to an entire non-VPN-aware device or a specific portion of a VPN-aware device (e.g., to a local or peer ATM address or interface) that communicates with a non-VPN-aware device. All control and data traffic received from this entity (or on this interface, etc) is associated with the VPN given by the assigned VPN-ID. If this method is used, no specific indications of the VPN-ID by signalling or encapsulation are required when communicating with this entity.

A VPN-aware MPOA device must support both method (a) (indication of the VPN-ID via ATM signalling) AND method (b) (VPN encapsulation) .

3.3 Configuration

A VPN-aware MPC must be able to map received traffic to a particular VPN based on some administrative criteria. Definition of these administrative criteria is outside the scope of this specification and requires no configuration specific to MPOA.

Each VPN that exists in the ATM cloud is required to have a unique VPN-ID. Administration of VPN-IDs to MPOA devices is also outside the scope of this specification.

3.4 MPOA Operation

Referring to Figure 2, each MPC has a default path to the MPS per VPN. The default path is used to forward data frames not destined for an MPOA shortcut. An MPS identifies the VPN for a received frame by the default path on which it was received. The MPS resolves the next hop router by referring to the routing table dedicated to that VPN. The MPS then sends the packet to the next hop for that VPN.

MPC ingress cache entries include a VPN-ID, and ingress MPCs perform flow detection based on the combination (VPN-ID, destination internetwork address, MPS).

As usual, an MPS may perform flow detection and trigger an MPC to establish a shortcut for a particular (VPN-ID, destination internetwork address).

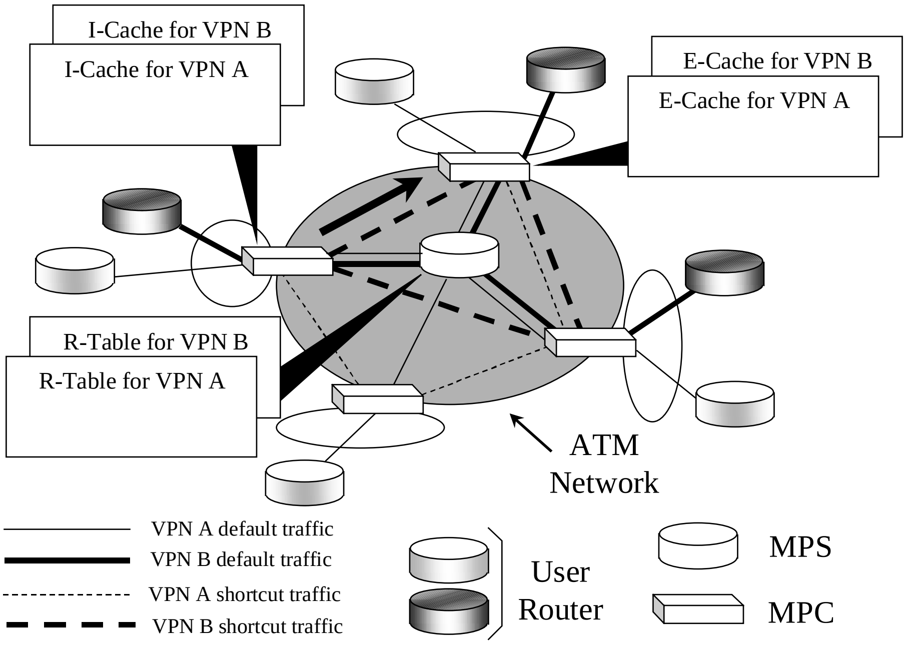

Figure 2: MPOA Support for VPNs

When supporting multiple VPNs, an MPC must indicate the VPN-ID for each transmitted data and control frame by one of the mechanisms specified in Section 3.2.

For the transfer of both control messages and data frames, the indication of the VPN-ID either via signalling (during the establishment of the ATM connection) or by VPN encapsulation is used. VPN encapsulation is required if multiple VPNs use the same ATM connection. Indication of the VPN-ID by signalling is recommended where it is important to avoid the per-frame overhead for the data packets, or when it is necessary for other reasons to separate traffic from different VPNs (for example, QoS requirements per VPN).

MPC egress cache entries include a VPN-ID, and egress MPCs perform forwarding based on the combination (VPN-ID, destination internetwork address, source ATM address).

3.5 Interoperability with Devices without VPN Support

Both VPN-aware and non-VPN-aware MPOA devices may participate in the same VPN; however, a specific non-VPN-aware MPOA device may only participate in the single VPN in which it is contained. This section describes the interaction between VPN-aware and non-VPN-aware devices.

MPCs may be associated with specific MPSs through administration. If an MPS is VPN-aware then that MPS may be configured with knowledge of the specific MPCs which may connect to that MPS and knowledge of the VPNs (i.e., the VPN-IDs) in which those specific MPCs are participating. Using configuration (instead of discovery) to determine which MPOA devices support which VPNs may be preferred in situations where security is a primary concern.

In some network configurations, VPNs may be deployed using non-VPN-aware MPOA devices. However, such a deployment is bound by the following additional requirements:

- Non-VPN-aware MPOA devices participating in a particular VPN may not interact with MPOA devices that do not share that VPN. That is, traffic from non-VPN-aware MPOA devices which are participating in a particular VPN must be contained within the bounds of that VPN.
- In the event that a VPN-aware MPC wishes to use a non-VPN-aware MPS, that MPC may do so even if that MPC is using the aforementioned MPS to “participate in a VPN.” However, that MPC must not use VPN encapsulation or VPN signalling on the control plane to that MPS. The MPC must use the NHRP device capability extension in its resolution requests, and it must use VPN signalling or VPN encapsulation for its shortcuts to a particular VPN-aware device.
- In the event that a VPN-aware MPS is serving a non-VPN-aware MPC, that MPS must act, as seen from the perspective of the MPC, as if VPNs were not involved with the control and data plane activity (e.g., resolution requests, etc.) Obviously, such an MPC will behave like any non-VPN-aware MPC and will not participate in any facet in VPN-aware behavior.

In addition to any configured knowledge about the peers' capabilities for VPN support, MPSs and their associated MPCs may also learn about each others' capabilities for VPN support by the mechanisms specified in Section 4.2 below.

An MPOA device may be capable of supporting VPNs, but must not use this capability when interoperating with non-VPN-aware MPOA devices. VPN-aware MPSs may serve both VPN-aware and non-VPN-aware MPCs. When a VPN-aware MPS serves a non-VPN-aware MPC, the MPS shall know the VPN in which that MPC is operating, if any, through administrative means. Such knowledge is required even without MPOA because the router (MPS) must forward packets from the edge device appropriately.

An extension to NHRP [RFC 2332] requests and responses is used between endpoints to indicate that a device is VPN-aware. MPOA messages may carry this extension as well (see Section 5.2 below). An ingress MPC will use this extension to learn whether a shortcut target is VPN-aware or not. The MPC may then use either signalling or VPN-encapsulation to indicate the VPN-ID for or on the new shortcut (the decision as to which method to use is outside the scope of this document). An egress MPC will use this extension to learn whether to expect a VPN-ID on a shortcut.

Detailed error handling procedures related to interactions with non-VPN-aware devices are provided in Section 4.9 below.

3.6 The Default Routing Instance

A VPN provides a virtual address space and routing realm to support a private network on a shared infrastructure. A control or data packet sent between VPN-aware MPOA devices without a VPN-specific association refers to the default routing instance supported by the shared infrastructure.

The public Internet or a particular VPN routing instance may be configured as the default routing instance. If no default routing instance is configured, control or data packets without an associable VPN-ID are discarded.

Configuration of the default routing instance is beyond the scope of this specification, and may introduce security issues.

4. VPN Support Specification

[Normative]

This section documents the changes required in [MPOAv1.1] to support VPNs. There are changes in the connection management, data frame encapsulation, and control frame encapsulation sections, and there are also changes in the ingress and egress cache structure and processing. The VPN-ID is used to identify the VPN for which the MPOA control message or data frame is intended. The following subsections describe the behavior of MPCs and MPSs with respect to VPNs. Behavior not mentioned in this section is unchanged from MPOA v1.1.

4.1 Configuration Parameters

Section 4.1 of MPOAv1.1 applies. As a default, the same set of configuration parameters applies to each VPN on a device.

The following parameters apply to each VPN-aware MPC in addition to those in [MPOAv1.1]:

Variable	Name	Description and Values
MPC-p7	Keep-Alive Time	The MPC must transmit MPOA Keep-Alives every MPC-p7 seconds. Minimum=1 second, Default=10 seconds, Maximum=300 seconds.
MPC-p8	Keep-Alive Lifetime	The length of time an MPS may consider a Keep-Alive valid in seconds. Minimum=3 seconds, Default=35 seconds , Maximum=1000 seconds (MPC-p8 must be at least three times MPC-p7)

4.2 MPC-MPS Device Discovery

MPSs and associated MPCs MAY be configured to know about each other's respective capabilities for VPN support. Such configuration SHOULD be used when security is a primary concern. In such situations, the MPOA device MAY be configured not to perform MPOA device discovery. Otherwise, MPOA devices use the basic device discovery mechanism as specified in Section 4.2 of [MPOAv1.1] and enhanced by the following paragraphs.

An additional Device Capabilities TLV is defined in Section 5.1. This TLV indicates whether the associated MPC or MPS is VPN-aware. The following paragraph assumes that the VPN-aware MPOA device is performing device detection.

VPN-aware MPCs or MPSs MUST include the Device Capabilities TLV along with the MPOA Device Type TLV within LANE control frames as described in [MPOAv1.1]. VPN-aware MPOA devices MUST detect this TLV in LANE control frames along with the MPOA Device Type TLV. When detected, VPN-aware MPOA devices MUST determine whether the source of the TLV is VPN-aware or not via the VPN-aware flag. When a device is detected but this TLV is absent, the VPN-aware MPOA device MUST consider the device as non-VPN-aware. All MPOA devices detected by a VPN-aware MPOA device MUST be flagged as either VPN-aware or non-VPN-aware.

4.3 MPOA Retry Mechanism

Section 4.3 of MPOA v1.1 applies.

4.4 Detailed MPC Behavior

4.4.1 Introduction

The MPOA extensions defined in this document assumes that traffic received and transmitted on the default data path can be classified into VPNs. The procedures of Section 4.4 in [MPOAv1.1] apply to MPOA VPN-aware devices except as noted in this section.

The MPOA configuration of a VPN-aware MPC does not differ from that of a non-VPN-aware MPC, except for those parameters defined in Section 4.1. As a default, the same set of configuration parameters applies to each VPN on a device.

4.4.2 Inbound Data Flow

VPN-aware MPCs MUST use the VPN-ID when making packet forwarding decisions. As such, the ingress cache entries of an MPC MUST include the VPN-ID as a part of the key that identifies a unique cache entry. The contents of an ingress cache entry for a VPN-aware MPC are given in Table 4-1.

Table 4-1 Ingress Cache Entries for VPN-aware MPCs

Keys			Contents		
MPS Control ATM Address	Internetwork Layer Destination Address	VPN-ID	Dest. ATM Address or VCC	Encapsulation Information	Other information needed for control (e.g. Flow Count and Holding Time)

Whether the ingress cache is composed of multiple tables, one per VPN, or a single table with a VPN-ID as part of the entry, is an implementation decision and is outside the scope of this specification.

Flow detection MUST be performed on the combination of internetwork layer destination address, VPN-ID, and MPS-control ATM address.

As detailed in Section 4.2, a VPN-aware MPC determines (either through discovery or administration) whether an MPS is VPN-aware. When communicating with a VPN-aware MPS, a VPN-aware MPC MUST use the VPN encapsulation of MPOA control frames or VPN signalling between itself and the MPS, except for the case of the default routing instance. VPN-encapsulation is defined in Annex B and the MPOA use of this encapsulation is described in Appendix 1. When an MPS is non-VPN-aware, the MPC MUST NOT VPN-encapsulate control frames or use VPN signalling to that MPS. If a VPN-aware MPC that is configured for multiple VPNs determines that its forwarding rules require it to forward traffic for *multiple* VPNs to a non-VPN-aware MPS, then the MPC MAY indicate a configuration error to system administration and SHOULD stop forwarding traffic to that MPS. Note that a VPN-aware MPC can communicate with a non-VPN-aware MPS when that MPS is being used for only a *single* VPN. Also, the decision whether to use VPN encapsulation or VPN signalling is made independently for each MPS serving the VPN-aware MPC.

When a VPN-aware MPC initiates an MPOA Resolution Request, it MUST include the NHRP Device Capabilities Extension as defined in Section 5.2. The VPN-aware bit MUST be set in the Source Capabilities field of that extension. A VPN-aware egress MPC MUST set the VPN-aware bit in the Target Capabilities field of that extension in the MPOA Cache Imposition Reply.

Upon receiving an MPOA Resolution Reply, the ingress MPC MUST use the NHRP Device Capabilities Extension to determine whether the egress device is VPN-aware. If the egress device is determined to be non-VPN-aware, then the MPC MUST NOT attempt to signal the egress using the VPN-ID in the signalling message and MUST NOT use VPN-encapsulation on the shortcut for this destination. If the egress device is VPN-aware as indicated by the NHRP Device Capabilities Extension, then the ingress MPC MUST forward VPN traffic either on a VPN-signalled shortcut or using VPN encapsulation on the resulting shortcut. It is a local decision whether the MPC uses VPN signalling or VPN encapsulation, but the general tradeoff is that the VPN signalling can provide QoS guarantees for individual VPNs while VPN encapsulation permits the sharing of a VCC between VPNs.

4.4.3 Outbound Data Flow

VPN-aware MPCs MUST also use the VPN-ID at the egress to map received shortcut traffic into a particular VPN. The possible contents of an egress cache entry on a VPN-aware MPC are given in Table 4-2 and Table 4-3.

Table 4-2 Egress Cache Without Tags

Keys			**Contents**		
Internetwork Layer Destination Address	Source/Dest. ATM Addresses	VPN-ID	LEC	DLL header	Other information needed for control (e.g. Holding Time)

Table 4-3 Egress Cache With Tags

Keys				**Contents**		
Internetwork Layer Destination Address	Source/Dest. ATM Addresses	Tag	VPN -ID	LEC	DLL header	Other information needed for control (e.g. Holding Time)

a) Determination of the VPN-ID for an MPOA Message

A VPN-aware MPC MUST determine the VPN-ID associated with an MPOA message from an egress MPS. It does so through administrative configuration, VPN encapsulation of the MPOA imposition request, or the VPN-ID signalled in the control VC. When the MPC gets a message from a non-VPN-aware MPS, it MUST determine the VPN-ID by adminstrative means.

If the VPN-ID in the VPN encapsulation header conflicts with the VPN-ID that was signalled or administratively configured, then the error-handling procedures in Section 4.9 apply.

If the egress MPC cannot determine the VPN-ID for an MPOA message from a VPN-aware MPS, it MUST treat this message request as belonging to the default routing instance.

b) Determination of the VPN-ID for PDUs received over a shortcut

When a packet is received on a shortcut, the VPN-ID for the packet MUST be determined.

To do so, the following procedures are used:

1. If the MPC has administrative means to associate a VPN-ID with a packet, it uses them first.
2. If the shortcut over which the packet was received indicated a VPN-ID during signalling, that VPN-ID is associated with all packets received over the shortcut.
3. If the packet used VPN-encapsulation, the VPN-ID is taken from the packet header. If this value conflicts with the VPN-ID that was signalled or configured for that VCC, the error handling procedures of Section 4.9 apply. The MPC SHOULD silently discard messages with incorrect or unknown VPN-IDs. If a data plane purge is used, it must use the incorrect or invalid VPN-ID.
4. If a non-VPN-encapsulated packet is received on a shortcut to which a VPN has not been bound and for which the ingress MPC is known to be VPN-aware, the packet is assumed to be for the default routing instance. If the ingress MPC is known to be non-VPN-aware, the VPN-aware MPC MUST be able to

determine the VPN-ID for the ATM address. One way to achieve this functionality would be for the VPN-aware MPC to maintain a new table mapping the ATM addresses to VPN-IDs. Entries would be added to this table when the VPN-aware MPC receives a Cache Imposition that indicates the source is non-VPN-aware (at least), and would be aged just like the egress cache entries. Other implementation alternatives are possible.

4.5 Detailed MPS Behavior

The MPOA configuration of a VPN-aware MPSs does not differ from that of a non-VPN-aware MPSs. As a default, the same set of configuration parameters applies to each VPN on a device.

MPOA control frames from a VPN-aware MPS to a VPN-aware MPC MUST be VPN-encapsulated or VPN-signalled. MPOA control frames from a VPN-aware MPS to a non-VPN-aware MPC MUST NOT be VPN-encapsulated or indicated through signalling.

On receiving an MPOA control frame from an MPC, a VPN-aware MPS MUST determine the VPN for the control frame. If the control frame is from a non-VPN-aware MPC, then the control frame is associated with the same VPN as that MPC.

In the case that the MPC is VPN-aware, the following applies: If the VPN-aware MPS has administrative measures that can be used to determine the VPN for a control frame, then these measures MUST be attempted to determine the appropriate VPN. If these measures fail and the control frame was VPN-encapsulated or VPN-signalled, then the VPN-ID MUST be taken from the VPN header or signalling message. Otherwise, the VPN-aware MPS MUST treat the packet as belonging to the default routing instance.

An MPS maintains an internetwork layer routing table per VPN and the routing function in the MPS node handles the internetwork layer packets based on the VPN on which the packets arrive. Forwarding of NHRP control frames MUST be based on both the VPN-ID and the destination internetwork address.

Data packets received over a default path are assumed to be handled by functions outside the scope of MPOA.

4.6 Keep-Alive Protocol

MPOA Servers need to know what VPNs are active on each MPC to maintain accurate routing and forwarding tables. MPOA Clients need to know that MPOA Servers that have supplied cache entries within a VPN are alive and able to maintain those cache entries.

All VPN-aware MPOA servers MUST add a non-compulsory VPN Keep-Alive extension to each MPOA Keep-Alive message. Rather than sending one Keep-Alive message per VPN, each Keep-Alive message MUST contain a VPN Keep-Alive extension with one VPN-ID for every active VPN.

A VPN-aware MPC that has cache entries from a VPN-aware MPS MUST periodically send Keep-Alive messages to that MPS with one VPN Keep-Alive extension containing a VPN-ID for every VPN that is operational on that MPC. A VPN-aware MPC MUST NOT send Keep-Alive messages to non-VPN-aware MPSs.

When a VPN-aware MPOA device has no active VPNs, it MAY exclude the VPN Keep-Alive extension, however, an MPOA client MUST still send Keep-Alive messages. A VPN-aware MPC MAY transmit the Keep-Alive frames over any LLC-encapsulated VCC to the MPS.

If a VPN-aware device does not receive a Keep-Alive message with a particular VPN-ID within Keep-Alive Lifetime seconds (specified in the previous Keep-Alive message), it MUST consider support for that VPN to have been removed by its peer. In response to a removed VPN-ID, an MPC MUST invalidate all cache entries which had been provided by that MPS for that VPN, and an MPS MUST send the appropriate purge requests for that VPN.

4.7 Cache Maintenance

Section 4.7 of MPOA v1.1 applies.

4.8 Connection Management

Section 4.8 of MPOA v1.1 applies with the following additions:

If an MPOA device chooses to indicate the VPN-ID via signalling, it is indicated via the GIT information element. If an MPOA device is aware that the network does not support the GIT IE, then it SHOULD not use VPN signalling.

The use of the GIT IE for the indication of the VPN-ID is specified in Section 6 below. Further information may be provided by future ATM Forum and ITU-T specifications.

UNI 3.0 / 3.1 considerations:

Although the support of the GIT IE is not specified for UNI 3.0/3.1, the use of the GIT IE by MPOA devices as an addition to the basic UNI 3.0/3.1 signalling is not precluded by this specification. If the GIT IE is used, the format specified in Section 6 is recommended.

Note:

If a VPN-aware ingress MPC tries to establish a call using VPN signalling through an ATM network that does not support the GIT IE or the specific VPN-codepoints therein, it should be aware that that network is not obligated to release such a call just because of the unrecognized GIT IE or its unrecognized contents. Instead, the related signalling procedures allow it to discard the GIT IE and possibly send a STATUS message; in either case, there is no guarantee that the ingress MPC is notified that the egress MPC might not have received the VPN indication.It is therefore required that ingress MPCs should not establish calls using VPN signalling without prior knowledge that the egress MPC is VPN-aware and the network supports the GIT IE.

4.9 Error Handling Procedures

If a PDU with a VPN encapsulation header is received on an ATM connection that was established with a VPN indication via signalling, the PDU MAY be dropped. If it is not dropped, the VPN identifiers MUST match. If the received PDU indicates a different VPN-ID, an MPOA Error Indication MUST be returned to the sender with an Error Code 16 (VPN mismatch). This error code is also returned, if an indicated VPN-ID conflicts with administratively configured information.

If a VPN-aware MPOA device receives a PDU for a VPN that it does not support, an MPOA Error Indication MUST be returned to the sender with an Error Code 17 (VPN not supported).

If an egress MPC receives a call setup message from an ingress MPC for a VPN it does not support, then it MUST reject the call establishment request.

If a VPN-aware MPS cannot find a route to forward an MPOA control message or data PDU within that VPN, it MAY send back an MPOA error indication with Error Code 6 (Protocol Address Unreachable).

5. Frame Formats

5.1 *MPOA Device Capabilities TLV*

The MPOA Device Capabilities TLV is a LANE TLV, and, if using device capability discovery, MUST be added along with the MPOA Device Type TLV in [LANE]-messages (see Section 4.2 of [MPOA v1.1]).

The format of the MPOA Device Capabilities TLV is as follows:

TLV Name	Type	Length	Value
MPOA Device Capabilities TLV	00-A0-3E-3D	4	Device Capabilities Bit 0x00000001 set implies source is VPN-aware Bit 0x00000001 clear implies source is non-VPN-aware Other bits must be clear on transmit, ignored on receipt.

Figure 3: MPOA Device Capabilities TLV Format

5.2 *NHRP Device Capabilities Extension*

The basic format of the NHRP Device Capabilities Extension is specified in the following Figure 4.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |C|u|        Type               |        Length                 |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                      Source Capabilities                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                      Target Capabilities                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: NHRP VPN Capability Extension Format

C-Bit: = 0 (compulsory bit, not a compulsory extension)
u-Bit: = 0 (unused)
Type: = 0x00 09
Length: = 8
Value: Two 32-bit fields indicating capabilities of source and target, respectively.
Bit 0x00000001 set implies the device is VPN-aware; Bit clear implies the device is non-VPN-aware.
Other bits must be cleared on transmit and ignored on receipt.

The NHRP Device Capabilities Extension MUST be included in the MPOA Resolution Requests originated by a VPN-aware MPC. The Source Capabilities field MUST have the VPN-aware bit set. If the NHRP Device

Capabilities Extension was included in the MPOA Cache Imposition Request, it MUST be included in the MPOA Cache Imposition Reply by a VPN-aware MPC with the Target Capabilities field having the VPN-aware bit set. The NHRP Device Capability Extension may only be carried in the following MPOA messages:

- MPOA Resolution Request / Reply
- MPOA Cache Imposition Request / Reply

5.3 VPN Keep-Alive Extension

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |C|u|        Type               |        Length                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   reserved    |             OUI                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     VPN index                                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                                  ...

   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   reserved    |             OUI                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     VPN index                                 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: VPN Keep-Alive Extension Format

C-Bit: = 0 (compulsory bit, not a compulsory extension)
u-Bit: = 0 (unused)
Type: = 0x00 0A
Length: = variable; n*8, where n is the number of indicated VPN-IDs
reserved field: value is 0x00 on transmit, and is ignored on receipt
OUI / VPN Index: see Annex A.

The number of VPN Identifiers within the extension can be determined from the length.

5.4 Additional MPOA Error Codes

The following error codes are used by MPOA VPN in addition to those specified in Section 5.3.14 of [MPOAv1.1]:

16 - VPN mismatch

This error code is returned by a VPN-aware MPOA device, if it receives a PDU with a VPN-ID in the VPN encapsulation header different from the VPN-ID which had been specified for that connection at its establishment.

17 - VPN not supported

This error code is returned by a VPN-aware MPOA device, if it receives a PDU for a VPN that it does not support.

6. Use of the GIT IE for Indication of the VPN-ID During ATM Connection Establishment

The indication of the VPN-ID via ATM signalling is based on the use of the "Generic Identifier Transport" (GIT) Information Element as specified in [Q.2941.1] during connection establishment.

The basic structure of the Generic identifier transport Information element is specified below. The specific codings for the transfer of the MPOA VPN identifier are then outlined.

<table>
<tr><th colspan="8">Bits</th><th></th></tr>
<tr><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octets</th></tr>
<tr><td colspan="8">Generic identifier transport
information element</td><td></td></tr>
<tr><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td rowspan="2">1
Ext</td><td colspan="2" rowspan="2">Coding
standard</td><td colspan="5">IE instruction field</td><td rowspan="2">2</td></tr>
<tr><td>Flag</td><td>Res.</td><td colspan="3">IE action ind.</td></tr>
<tr><td colspan="8" rowspan="2">Length of contents of information element</td><td>3</td></tr>
<tr><td>4</td></tr>
<tr><td colspan="8">Identifier related standard/applications</td><td>5</td></tr>
<tr><td colspan="8">Identifier type</td><td>6 (NOTE)</td></tr>
<tr><td colspan="8">Identifier length</td><td>6.1</td></tr>
<tr><td colspan="8" rowspan="2">Identifier value</td><td>6.2</td></tr>
<tr><td>6.m</td></tr>
<tr><td colspan="8"></td><td></td></tr>
<tr><td colspan="8">Identifier type</td><td>N*</td></tr>
<tr><td colspan="8">Identifier length</td><td>N.1*</td></tr>
<tr><td colspan="8" rowspan="2">Identifier value</td><td>N.2*</td></tr>
<tr><td>N.n*</td></tr>
</table>

Figure 6: Coding of the GIT Information Element

NOTE - Octet group 6 can be repeated to form new octet groups numbered sequentially octet group 7, 8, ..., N.

Further information may be provided by future ATM Forum and ITU-T specifications.

For the MPOA VPN identifier, the coding and contents is as follows:

Identifier related standard/application (octet 5)

Bits 8 7 6 5 4 3 2 1	
(...)	
0 0 0 0 0 1 1 1	ATM Forum MPOA (Note)
(...)	

Note: When the identifier related standard/application field is coded "ATM Forum MPOA", the related identifiers are coded as indicated in this specification. Only the MPOA-related codepoint shown above is normative for this specification; other uses of the GIT information element are outside the scope of this specification.

Identifier type (Octet 6, 7, ..., N)

Bits 8 7 6 5 4 3 2 1	
(...)	
0 0 0 0 0 1 1 1	MPOA VPN identifier (Note)
(...)	

Note: When the identifier type field is coded "MPOA VPN identifier", the MPOA VPN ID is coded as outlined below. Only the MPOA-related codepoint shown above is normative for this specification; other uses of the GIT information element are outside the scope of this specification.

Identifier related standard/applications								
0	0	0	0	0	1	1	1	5
VPN identifier								
0	0	0	0	0	1	1	1	6
Identifier length = 7								6.1
OUI								6.2
								6.3
								6.4
OUI-specific VPN Index value								6.5
								6.6
								6.7
								6.8

Figure 7: Coding of the ATM Forum MPOA VPN Identifier

Octets 6.2 to 6.4: Organizationally Unique Identifier (OUI), as specified in IEEE 802-1990.

Octets 6.5 to 6.8: a 4-Octet integer value identifying the VPN; this value is allocated by the organization identified by the OUI.

Annex A: Virtual Private Networks Identifier [Normative]

This Annex contains a copy of the following Internet Draft:

Fox, B., Gleeson, B., "Virtual Private Networks Identifier", INTERNET DRAFT <draft-ietf-ion-vpn-id-02.txt>, expires January 2000.

It is the intent of the ATM Forum to replace this Annex with a reference to the official Request For Comments (RFC) when it becomes available.

Internet Engineering Task Force Barbara A. Fox
INTERNET-DRAFT Lucent Technologies
<draft-ietf-ion-vpn-id-02.txt> Bryan Gleeson
Expires January 2000 Shasta Networks, Inc.

Virtual Private Networks Identifier

Status of this Memo

Abstract

Virtual Private IP networks may span multiple Autonomous Systems or Service Providers. There is a requirement for the use of a globally unique VPN identifier in order to be able to refer to a particular VPN (see section 6.1.1 of [1]). This document proposes a format for a globally unique VPN identifier.

1. Introduction

As the Public Internet expands and extends its infrastructure globally, the determination to exploit this infrastructure has led to widespread interest in IP based Virtual Private Networks. This VPN emulates a private IP network over public or shared infrastructures.

Virtual Private Networks provide advantages to both the Service Provider and its customers. For its customers, a VPN can extend the IP capabilities of a corporate site to remote offices and/or users with intranet, extranet, and dialup services. This connectivity should be achieved at a lower cost to the customer with savings in capital equipment, operations, and services. The Service Provider is able to make better use of its infrastructure and network administration expertise offering IP VPN connectivity and/or services to its customers.

There are many ways in which IP VPN services may be implemented. The IP based VPN framework document [1] identifies four types of VPN to be supported: Virtual Leased Lines, Virtual Private Routed Networks, Virtual Private Dial Networks, and Virtual Private LAN Segments. In addition, numerous drafts and white papers outline methods to be used by Service Providers and/or Service Provider customers to enable this service. Solutions may be customer based or network based. Network based solutions may provide connectivity and services at layer 2 and/or layer 3. The devices involved in enabling the solution may be Customer Premises Equipment (CPE), Service Provider Edge equipment, Service Provider Core equipment, or some combination of these.

While the various methods of VPN service implementation are being discussed and debated, there are two points on which there is agreement:

Because a VPN is private, it may use a private address space which may overlap with the address space of another VPN or the Public Internet.

A VPN may span multiple IP Autonomous Systems (AS) or Service Providers.

The first point indicates that an IP address only has meaning within the VPN in which it exists. For this reason, it is necessary to identify the VPN in which a particular IP address has meaning, the "scope" of the IP address.

The second point indicates that several methods of VPN service implementation may be used to provide connectivity and services to a single VPN. Different service providers may employ different strategies based on their infrastructure and expertise. It is desirable to be able to identify any particular VPN at any layer and at any location in which it exists using the same VPN identifier.

2. Global VPN Identifier

The purpose of a VPN-ID is to identify a VPN. This identifier may be used in various ways depending on the method of VPN service implementation. For example, the VPN-ID may be included:

- In a MIB to configure attributes to a VPN, or to assign a physical or logical access interface to a particular VPN.

- In a control or data packet, to identify the "scope" of a private IP address and the VPN to which the data belongs.

It is necessary to be able to identify the VPN with which a data packet is associated. The VPN-ID may be used to make this association, either explicitly (e.g. through inclusion of the VPN-ID in an encapsulation header [2]) or implicitly (e.g. through inclusion of the VPN-ID in a ATM signalling exchange [3]). The appropriateness of using the VPN-ID in other contexts needs to be carefully evaluated.

There is another very important function that may be served by the VPN identifier. The VPN identifier may be used to define the "VPN authority" who is responsible for coordinating the connectivity and services employed by that VPN. The VPN authority may be the Private Network administrator or the primary Service Provider. The VPN authority will administer and serve as the main point of contact for the VPN. The authority may outsource some functions and connectivity, set up contractual agreements with the different Service Providers involved, and coordinate configuration, performance, and fault management.

These functions require a VPN that is global in scope and usable in various solutions. To be a truly global VPN identifier, the format cannot force assumptions about the shared network(s). Conversely, the format should not be defined in such a way as to prohibit use of features of the shared network. It is necessary to note that the same VPN may be identified at different layers of the same shared network, e.g. ATM and IP layers. The same VPN-ID format and value should apply at both layers.

The methods of VPN-ID usage are beyond the scope of this draft.

3. Global VPN Identifier Format Requirements

The VPN Identifier format should meet the following requirements:

- Provide a globally unique VPN Identifier usable across multiple Service Providers.
- Enable support of a non-IP dependent VPN-ID for use in layer 2 VPNs.
- Identify the VPN Authority within the VPN Identifier.

4. Global VPN Identifier Format

The global VPN Identifier format is:

```
  3 octet VPN authority Organizationally Unique Identifier [4]
followed by
  4 octet VPN index identifying VPN according to OUI
```

```
0 1 2 3 4 5 6 7 8
+-+-+-+-+-+-+-+-+
| VPN OUI (MSB) |
+-+-+-+-+-+-+-+-+
|   VPN OUI     |
+-+-+-+-+-+-+-+-+
| VPN OUI (LSB) |
+-+-+-+-+-+-+-+-+
|VPN Index (MSB)|
+-+-+-+-+-+-+-+-+
|  VPN Index    |
+-+-+-+-+-+-+-+-+
|  VPN Index    |
+-+-+-+-+-+-+-+-+
|VPN Index (LSB)|
+-+-+-+-+-+-+-+-+
```

The VPN OUI (IEEE 802-1990 Organizationally Unique Identifier) [4] identifies the VPN authority. The VPN authority will serve as the primary VPN administrator. The VPN authority may be the company/organization to which the VPN belongs or a Service Provider that provides the underlying infrastructure using its own and/or other providers’ shared networks. The 4 octet VPN Index identifies a particular VPN serviced by the VPN authority.

5. Security Considerations

This document defines the format of the global VPN identifier without specifying usage. However, the association of particular characteristics and capabilities with a VPN identifier necessitates use of standard security procedures with any specified usage. Misconfiguration or deliberate forging of VPN identifier may result different breaches in security including the interconnection of different VPNs.

References

[1] Gleeson, Heinanen, Lin, Armitage, Malis, "A Framework for IP Based Virtual Private Networks", work in progress.

[2] Grossman, Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", work in progress.

[3] "MPOA v1.1 Addendum on VPN Support", ATM Forum, str-mpoa-vpn-01_00, July, 1999, Bernhard Petri, editor, straw ballot document.

[4] http://standards.ieee.org/regauth/oui/index.html

Author Information

Barbara A. Fox
Lucent Technologies
300 Baker Ave, Suite 100
Concord, MA 01742-2168
phone: +1-978-287-2843
email: barbarafox@lucent.com

Bryan Gleeson
Shasta Networks
249 Humboldt Court
Sunnyvale, CA 94089-1300
phone: +1-408-548-3711
email: bgleeson@shastanets.com

Annex B: VPN Encapsulation

This Annex contains a copy of Section 8 of the following Internet Draft:

Grossman, D., Heinanen, J., “Multiprotocol Encapsulation over ATM Adaptation Layer 5”, INTERNET DRAFT <draft-ietf-ion-multiprotocol-atm-03.txt>, expires December 1999.

It is the intent of the ATM Forum to replace this Annex with a reference to the official Request For Comments (RFC) when it becomes available.

8. Virtual Private Network (VPN) identification

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:

```
     VPN Encapsulation Header
+-------------------------------+
|       LLC  0xAA-AA-03         |
+-------------------------------+
|        OUI 0x00-00-5E         |
+-------------------------------+
|        PID 0x00-08            |
+-------------------------------+
|      Reserved (1 octet)       |
+-------------------------------+
|   VPN related OUI (3 octets)  |
+-------------------------------+
|    VPN Index (4 octets)       |
+-------------------------------+
|                               |
|     (remainder of PDU)        |
|                               |
+-------------------------------+
```

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.

--- --- --- --- --- --- ---

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

Appendix 1: Example Frame Formats for VPN Encapsulation [informative]

The format of the VPN encapsulation header is specified in Annex B above. This Appendix provides further information and examples for these formats.

The VPN encapsulation header consists of an 8-byte LLC/SNAP header (the OUI is IANA's OUI), a 1-byte Reserved field, a 7-byte VPN-ID field, and a LLC encapsulated PDU. Both VPN encapsulated packets and non-VPN encapsulated packets are allowed to go through the same VCC.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0xAA     |      0xAA     |      0x03     |      0x00     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00     |      0x5E     |        0x08 (Note)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Reserved   |                     OUI                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           VPN Index                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            LLC encapsulated PDU (up to 2^16 - 16 octets)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Note: Protocol ID allocated by IANA for VPN encapsulation

Figure 8: VPN Encapsulation

The format for the VPN encapsulation of MPOA 1.1 control messages is as shown in Figure 9 below.

```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0xAA     |      0xAA     |      0x03     |      0x00     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00     |      0x5E     |        0x08 (Note)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Reserved   |                     OUI                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           VPN Index                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0xAA     |      0xAA     |      0x03     |      0x00     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00     |      0x5E     |      0x00     |      0x03     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      MPOA control message                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Note: Protocol ID allocated by IANA for VPN encapsulation

Figure 9: VPN Encapsulation of MPOA Control Messages

IP packets are encapsulated by VPN encapsulation as follows.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0xAA     |      0xAA     |      0x03     |      0x00     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00     |      0x5E     |        0x08 (Note)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Reserved   |                     OUI                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           VPN Index                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0xAA     |      0xAA     |      0x03     |      0x00     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00     |      0x00     |             0x08-00           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     IP PDU (up to 2^16 - 24 octets)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Note: Protocol ID allocated by IANA for VPN encapsulation

Figure 10: VPN Encapsulation for IP Packets

MPOA Tagged Encapsulation packets are encapsulated by VPN encapsulation as follows.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0xAA     |      0xAA     |      0x03     |      0x00     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00     |      0x5E     |        0x08 (Note)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Reserved   |                     OUI                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           VPN Index                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0xAA     |      0xAA     |      0x03     |      0x00     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00     |      0x00     |             0x88-4c           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           MPOA Tag                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Internetwork Layer PDU (up to 2^16 - 28 octets)     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Note: Protocol ID allocated by IANA for VPN encapsulation

Figure 11: VPN Encapsulation for MPOA Tagged Encapsulation