IPoRPR Working Group	M. Holness
Internet-Draft	G. Parsons
Expires: January 12, 2006	Nortel
	July 11, 2005

Mapping of IP/MPLS ~~Packets~~ packets into IEEE 802.17 (Resilient ~~Packet~~ packet ~~Ring~~ring) ~~Networks~~networks

draft-ietf-iporpr-basic-00.txt

Status of this Memo

The list of current Internet-Drafts can be accessed at **http://www.ietf.org/ietf/1id-abstracts.txt**.

The list of Internet-Draft ~~Shadow~~ shadow ~~Directories~~ directories can be accessed at **http://www.ietf.org/shadow.html**.

This Internet-Draft will expire on January 12, 2006.

Copyright Notice

Abstract

This document specifies a basic standard method of encapsulating IPv4, IPv6, and MPLS datagrams into IEEE 802.17 Resilient ~~Packet~~ packet ~~Ring~~ ring (RPR) datagrams.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirements Levels,” March 1997.)** [1].

The term "Higher Layer" refers to IPv4, IPv6, and MPLS when they act as clients of the IEEE 802.17 network.

"IP" refers to both IPv4 and IPv6. The terms "IPv4" and "IPv6" are used only when a specific version of IP is meant.

---

1. IEEE 802.17

This section gives a brief introduction to the IEEE 802.17 protocol. The intent is to provide information needed to understand the rest of this document. This section is SHALL NOT be used as a definitive description of **IEEE 802.17 (, "Resilient ~~Packet~~ packet ~~Ring~~ ring ~~Access~~ access ~~Method~~ method and Physical Layer Specifications - medium access control parameters, physical layer interface, and management parameters," July 2004.)**[2].

IEEE 802.17 SHALL be consulted for specific details on the functionality. Section 5 contains a ~30 page overview of the ~700 page specification. Details on the MAC service is contains in section 6.

1.1 Overview of IEEE 802.17

IEEE 802.17 is a dual, counter-rotating, ring network technology with destination stripping. In the event of a fault (such as a fiber cut) the stations on each side of the fault can continue to function by wrapping the ring and/or by steering away from the fault and towards the operational path. When the fault clears, the ring reverts to normal operation.

The ring is composed of two ringlets, called ringlet0 and ringlet1.

A station may transmit a frame in either direction around the ring. IEEE 802.17 includes MAC-level protocols to determine the "best" path to each destination. The determination of "best" may be by any of several algorithms, including shortest path. Normally, the 802.17 MAC layer will automatically send frames via the "best" path. Alternatively, higher layers (such as IP) may explicitly specify the ringlet to use.

All stations on the ring have 48-bit IEEE 802 addresses.

IEEE 802.17 is a media-independent network protocol that is layered over several different physical media. SONET/SDH, Gigabit Ethernet and 10-Gigabit Ethernet are currently specified. The higher layers are shielded from any media dependencies.

There are fairness and bandwidth-management elements. There are three service classes: ~~Class~~ classA provides low delay and low delay variation, class~~-~~B has committed and excess bandwidth components, and class~~-~~C is best-effort.

There are several frame types, one of which is a data frame. The data frame contains a payload (such as an IPv4, IPv6, or MPLS packet). The type of the payload is indicated by a 2-byte type field. The type-field is identical to the type field in IEEE 802.3 Ethernet.

There is a TTL in the IEEE 802.17 frame headers. This TTL is used to prevent frames from infinitely looping.

1.2 IEEE 802.17 MAC ~~Service~~service

The IEEE 802.17 MAC ~~Service~~ service ~~Definition~~ definition defines the MA_DATA.request primitive which a station uses to transmit data (see section 6.4.1 of **[2] (, "Resilient ~~Packet~~ packet ~~Ring~~ ring ~~Access~~ access ~~Method~~ method and ~~Physical~~ physical ~~Layer~~ layer ~~Specifications~~ specifications - medium access control parameters, physical layer interface, and management parameters," July 2004.)**). This primitive takes several ~~Parameters~~ parameters (only three of which are mandatory):

destination_address
source_address optional
mac_service_data_unit
frame_check_sequence optional
service_class
ringlet_id optional
mac_protection optional
mark_fe optional
strict_order optional
destination_address_extended optional
source_address_extended optional
flooding_form optional

1.2.1 IEEE 802.17 ~~Addressing~~addressing

The ~~Destination~~ destination ~~Address~~ address (DA) [destination_address] is the 48-bit MAC address of the destination station. This may be a multicast or broadcast address. This address is an IEEE 802 address. This is a required parameter.

The ~~Source~~ source ~~Address~~ address (SA) [source_address] is the 48-bit MAC address of the source station. This address is an IEEE 802 address. This is an optional parameter. If it is omitted, the MAC uses the source address that is assigned to the station.

1.2.2 IEEE 802.17 ~~Payload~~payload

The MAC SDU [mac_service_data_unit] is the RPR payload. It includes the entire IP/MPLS packet prefaced with the Ethertype field. This is a required parameter. .

1.2.3 IEEE 802.17 ~~S~~service ~~Classes~~classes

One of the key features of RPR that can distinguish it from other network interconnects, is it ability to support multiple service qualities. Per service quality flow control protocols regulate traffic introduced by clients. The list of supported service classes are listed below:

Class~~ a~~A:

Class~~-~~A services provides an allocated, guaranteed data rate, and low end-to-end delay and jitter bound. C~~lass A~~lassA traffic is allocated with a committed information rate (CIR). Traffic above the allocated rate is rejected. C~~lass A~~lassA traffic has precedence over clas~~s~~ B and class~~-~~C traffic at the ingress to the ring. This class is well suited for real time applications.

Class~~ b~~B:

Class~~-~~B services provides an allocated, guaranteed data rate, and bounded end-to-end delay and jitter for the traffic within the allocated rate. Class~~-~~B also provides access to additional best effort data transmission that is not allocated, guaranteed, or bounded. Class\~~-~~B traffic is allocated with a CIR component. Any class~~-~~B traffic amount beyond the allocated CIR is referred to as excess information rate (EIR) class-B traffic. Class-B traffic (including clas~~s~~ B EIR) has precedence over class C traffic at the ingress to the ring.

Class ~~c~~C:

Class-C services provides a best-effort traffic service with non allocated or guaranteed data rate, and no bounds on end-to-end delay or jitter. Class-C traffic has the lowest precedence for ingress to the ring. Both class-B EIR and class-C traffic is governed by the RPR fairness algorithm which ensures proper partitioning of opportunistic traffic over the ring. This class is well suited for best effort applications. The RPR datagram carries the priority (i.e., service class) of the traffic being transported within a sc (service class) field found within the baseControl field of the RPR header.

The RPR sc is a 2-bit field. The values are shown in Table 1 below.

Value	Name
00	CLASS_C
01	CLASS_B
10	CLASS_A1
11	CLASS_A0

Table 1: sc values

1.2.4 IEEE 802.17 ~~Fairness~~fairness

The RPR fairness algorithm ensures proper partitioning of opportunistic traffic over the ring and governs class B EIR and class-C traffic. The RPR datagram conveys the application of the fairness algorithm on the datagram by the value of the fairness eligible (fe) field, found in the baseControl field of the RPR header.

The fe (fairness eligible) bit marks whether the frame is subject to the fairness algorithm. A value of 0 indicates that the frame is not fairness eligible, while a value of 1 indicates that the frame is fairness eligible.

---

2. General Mapping Details

This section covers issues that are common to IPv4, IPv6, and MPLS.

2.1 IEEE 802.17 MAC ~~Service~~ service ~~Parameters~~parameters

When transmitting an IP or MPLS packet, a host or router indicates various parameters to the IEEE 802.17 MAC layer (see section 6.4 of **[2] (, "Resilient ~~Packet~~ packet ~~Ring~~ ring ~~Access~~ access ~~Method~~ method and ~~Physical~~ physical ~~Layer~~ layer ~~Specifications~~ specifications - medium access control parameters, physical layer interface, and management parameters," July 2004.)**). This section specifies how those parameters are to be used:

2.1.1 Destination_address

Is the 48-bit MAC address of the 802.17 station to which the packet is being transmitted.

2.1.2 Source_address

The source_address SHOULD be the address assigned to the station that is transmitting the packet. Per **[2] (,"Resilient packet ring access method and physical layer specifications - ~~"Resilient Packet Ring Access Method and Physical Layer Specifications -~~ medium access control parameters, physical layer interface, and management parameters," July 2004.)** if the client omits this parameter then the MAC inserts the correct address.

2.1.3 mac_service_data_unit

This is the payload, including the Ethernet type field. See **"Protocol Type Field" (Protocol Type Field)**, for more information.

2.1.4 frame_check_sequence

The MAC will calculate the FCS

2.1.5 serviceClass

Specific service class mapping from DSCP and EXP within the client payload SHOULD be used to determine the RPR service class. These mappings are shown in **Section 3.2 (IP Differentiated Service (DSCP) Mapping to RPR)** and **Section 5.1 (MPLS EXP bit Mapping to RPR)**.

2.1.6 ~~Ringlet~~ringlet_id

The client SHOULD NOT specify the ringletID. The MAC will use its default algorithm to select a ringlet.

2.1.7 mac_protection

This is set by the MAC to indicate if RPR protection is used for the frame.

2.1.8 mark_fe

This parameter SHOULD NOT be specified unless the RPR service class is CLASS B as indicated from the mappings in **Section 3.2 (IP Differentiated Service (DSCP) Mapping to RPR)** and **Section 5.1 (MPLS EXP bit Mapping to RPR)**.

2.1.9 strict_order

This parameter SHOULD NOT be specified. The IEEE 802.17 MAC will then use its default treatment.

2.1.10 destination_address_extended

This parameter SHOULD NOT be specified. The IEEE 802.17 MAC will populate if necessary.

2.1.11 source_address_extended

This parameter SHOULD NOT be specified. The IEEE 802.17 MAC will populate if necessary.

2.1.12 flooding_form

This parameter SHOULD NOT be specified. The IEEE 802.17 MAC will populate if necessary.

2.2 Protocol Type Field

The 16-bit protocol type field (or Ethertype) is set to a value to indicate the payloads protocol. The values for IPv4, IPv6, and MPLS are:

0x0800 If the payload contains an IPv4 packet.
0x0806 If the payload contains an ARP packet.
0x86DD If the payload contains an IPv6 packet.
0x8847 If the payload contains a MPLS Unicast packet.
0x8848 if the payload contains a MPLS Multicast packet.
0x8100 if the payload contains an Ethernet VLAN/Priority tagged packet.

2.3 Payload

The payload contains the IPv4, IPv6, or MPLS packet. The first byte of the IPv4 header, IPv6 header, or top MPLS label begins immediately after the 802.17 headers.

Note that in 802.17 there is no minimum size for frames carried over Ethernet physical layers, thus there is no need to pad frames that are shorter than the minimum size. However, the robustness principle dictates that nodes be able to handle frames that are padded.

Like 802.3 Ethernet, 802.17 defines the maximum regular frame payload as 1500 bytes. Note that a maximum jumbo frame payload size that MAY be supported is defined at 9100 bytes.

2.4 Byte Order

As described in "APPENDIX B: Data Transmission Order" of **RFC 791 (Postel, J., "Internet Protocol," September 1981.)**[3], IP and MPLS datagrams are transmitted over the IEEE 802.17 network as a series of 8-bit bytes in "big endian" order. This is the same byte order as used for Ethernet.

2.5 Trailer ~~Format~~format

Trailer encapsulation is NOT specified for IEEE 802.17 networks.

2.6 Ringlet and ~~Direction~~ direction ~~Selection~~selection

IEEE 802.17 allows the ~~Higher~~ higher ~~Layer~~ layer to select the direction around the ring that traffic is to go. If the ~~Higher~~ higher ~~Layer~~ layer does not make the selection then the IEEE 802.17 MAC makes the decision. Ringlet and ~~Direction~~ direction selection are left to the MAC. The advanced version of this specification may change this.

2.7 Higher ~~Layer~~ layer TTL and ~~Ring~~ ring ~~TTL~~ttl

There is no correlation or interaction between the ~~Higher~~ higher ~~Layer~~ layer TTL and the IEEE 802.17 ~~TTL~~ttl.

---

3. IPv4 ~~Specific~~ specific ~~Mapping~~ mapping ~~Details~~details

3.1 Address ~~Resolution~~resolution

ARP (Plummer, D., "An Ethernet Address Resolution Protocol," November 1982.)[4] is used to map IPv4 addresses to the appropriate MAC address. The "Hardware Address Space" parameter (ar$hrd) used for IEEE 802.17 networks is TBD. ARP parameter assignments may be found at IANA.

3.1.1 Editor's ~~Notes~~notes

The hardware type is to be allocated by IANA prior to publication.

We could overload the Ethernet (1) or IEEE 802 (6) hardware type value since 802.17 addresses are the same size and format as Ethernet addresses. However, it is not inconceivable that overloading this value may turn out to have unforeseen undesired consequences. As we are not in any danger of running out of ARP hardware codes, we'll get an 802.17-specific one.

3.2 IP Differentiated Service (DSCP) ~~Mapping~~ mapping to RPR

The ~~Differentiated~~ differentiated ~~Service~~ service (DS) field of the IPv4 and IPv6 frame can be used to convey service priority. The format of the IP DS field is shown in Figure 1 below.

```
       |   0   |   1   |   2   |   3   |   4   |   5   |   6   |
   7   |
       |-----------------------------------------|-----------
   ---|
       |                   DSCP                  |     ECN
   |
       |-----------------------------------------|-----------
   ---|
```

Figure 1: Differentiated ~~Services~~ services ~~Field~~ field

The DSCP field denotes the differentiated services codepoint. The DSCP is used to select the per hop behavior a packet experiences at each network node. As per **[6] (Nichols, K., "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.," December 1998.)**, **[7] (Heinanen, J., "Assured Forwarding PHB Group.," June 1999.)**, **[8] (Jacobson, V., "An Expedited Forwarding PHB Group.," June 1999.)** and **[9] (Babiarz, J., "Configuration Guidelines for Diffserv Service Classes," June 2005.)**, the DSCP field description is illustrated in Table 2.

IP Service Class	DSCP	Per Hop Behaviour
Standard	000000	Default Forwarding
Low Priority Data	001000	Class Selector 1
High Throughput	001010	AF11
Data	001100	AF12
	001100	AF13
OAM	010000	Class Selector 2
	010010	AF21
Low Latency Data	010100	AF22
	010110	AF23
Broadcast Video	011000	Class Selector 3
Multimedia	011010	AF31
Streaming	011100	AF32
	011110	AF33

```
    |---------------------|----------|----------
---------|
    |Real-time Interactive|  100000  | Class
Selector 4  |
    |---------------------|----------|----------
---------|
    |    Multimedia       |  100010  |      AF41
|
    |    Conferencing     |  100100  |      AF42
|
    |                     |  100110  |      AF43
|
    |---------------------|----------|----------
---------|
    |    Signaling        |  101000  | Class
Selector 5  |
    |---------------------|----------|----------
---------|
    |    Telephony        |  101110  |      EF
|
    |---------------------|----------|----------
---------|
    |   Network Control   |  110000  | Class
Selector 6  |
    |---------------------|----------|----------
---------|
    |       Reserved      |  111000  | Class
Selector 7  |
    |    for future use   |          |
|
    |---------------------|----------|----------
---------|
```

Table 2: DSCP ~~Field~~ field ~~Definition~~ definition

The best effort DSCP group denotes a best effort service.

The ~~Assured~~ assured ~~Forwarding~~ forwarding (AF) PHB groups are a means for a provider DS domain to offer different levels of forwarding assurances for IP packets received from a customer DS domain. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. A congested DS node tries to protect packets with a lower drop precedence value from being lost by preferably discarding packets with a higher drop precedence value.

The ~~Expedited~~ expedited ~~Forwarding~~ forwarding (EF) PHB group is used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS domains.

The Class Selector PHBs are to provide limited backwards capability for IP precedence.

The mapping between IP DSCP to RPR header service class relevant fields are shown in Table 3. Note that four treatment aggregates are used as suggested by **[10] (Chan, K., "Aggregation of Diffserv Service Classes.," February 2005.)**.

DSCP	RPR ~~Service~~ service ~~Class~~ class	RPR sc	RPR fe
000000	Class C	00	1
001000			
001010			0-Class B CIR
001100			1-Class B EIR
001110			
010000			0-Class B CIR

```
    |----------|     Class B       |        |---
------------|
    |  010010  |                   |        |
|
    |  010100  |                   |        | 1-
Class B EIR |
    |  010110  |                   |        |
|
    |----------|                   |        |---
------------|
    |  011010  |                   |        | 0-
Class B CIR |
    |          |                   |        |---
------------|
    |  011100  |                   |        | 1-
Class B EIR |
    |  011110  |                   |        |
|
    |----------|-------------------|--------|---
------------|
    |  011000  |                   |        |
|
    |----------|                   |        |
|
    |  100000  |     Class\_A0      |   11   |       |
|
    |----------|                   |        |
|
    |  100010  |                   |        |
|
    |  100100  |        or         |   or   |
0       |
    |  100110  |                   |        |
|
    |----------|                   |        |
|
    |  101000  |     Class_A1      |   10   |       |
|
    |----------|                   |        |
|
    |  101110  |                   |        |
|
    |----------|-------------------|--------|---
------------|
    |          |     Class_A0      |   11   |       |
|
```

```
    |  110000  |         or         |   or   |
0       |
    |          |     Class–A1       |   10   |
|
    |----------|------------------|--------|---
-------------|
```

Table 3: IP DSCP to RPR ~~Header~~ header mMapping

Internal to the RPR MAC, ~~C~~c~~lass A~~lassA traffic is partitioned into two sub classes: ~~C~~class~~ ~~A0 and ~~Class A~~classA1. This partitioning is done in order to increase the ability of the ring to reclaim unused ~~Class A~~classA traffic. The RPR MAC is configured for a total ~~Class A~~classA amount, from which it determines how much is ~~Class A~~classA0 and ~~ClassA1~~classA1. The division of ~~Class A~~classA is based on ring circumference and the size of internal transit queues. The reclaimable bandwidth allocated to ~~Class A~~classA1 can be reclaimed by traffic of ~~Class~~ classB-EIR and Class C when not being used by the station originating the ~~Class~~ classA traffic being reclaimed.

Services marked with a DF and CS1 DSCP do not have a small amount of assured bandwidth component. That is, it only has an EIR component. Services marked with AF1x, AF2x, AF3x, AF4x and CS2 DSCPs have an aggregate CIR and EIR component. Services marked with CS3, CS4, CS5 and EF DSCPs only have a CIR component. Routing traffic marked with CS6 DSCP class also only has a CIR component. As CS7 is for future use, no mapping is provided.

As per **[11] (Ramakrishnan, K., “The Addition of Explicit Congestion Notification (ECN) to IP,” September 2001.)**, bits 6 and 7 of the DS field can be defined to be the ~~Explicit~~ explicit ~~Congestion~~ congestion ~~Notification~~ notification (ECN) field. The coding of the ECN does not influence the mappings to the RPR service class relevant fields (listed in Table 3).

4. IPv6 Specific Details

Transport of IPv6 packets over IEEE 802.17 networks is designed to be as similar to IPv6 over Ethernet as possible. The intent is to minimize time and risk in developing both the standard and the implementations.

4.1 Stateless ~~Autoconfiguration~~autoconfiguration

IPv6 stateless autoconfiguration follows the rules and procedures in section 4 of **RFC 2464 (Crawford, ., “Transmission of IPv6 Packets over Ethernet Networks,” December 1998.)**[5].

4.2 Link ~~Local~~ local ~~Address~~address

IPv6 link-local addresses follow the rules and procedures in section 5 of **RFC 2464 (Crawford, ., “Transmission of IPv6 Packets over Ethernet Networks,” December 1998.)**[5].

4.3 Unicast ~~Address~~ address ~~Mappings~~mappings

IPv6 unicast address mappings follow the rules and procedures in section 6 of **RFC 2464 (Crawford, ., “Transmission of IPv6 Packets over Ethernet Networks,” December 1998.)**[5].

4.4 Multicast ~~Address~~ address ~~Mappings~~mappings

IPv6 multicast address mappings follow the rules and procedures in section 7 of **RFC 2464 (Crawford, ., “Transmission of IPv6 Packets over Ethernet Networks,” December 1998.)**[5].

4.5 Diffserv mapping

The mapping is as specified in **Section 3.2 (IP Differentiated Service (DSCP) Mapping to RPR)**

---

5. MPLS ~~Specific~~ specific ~~Details~~details

Transport of MPLS packets over IEEE 802.17 follows **RFC 3032 (Rosen, E., “MPLS Label Stack Encoding,” January 2001.)**[12]. As with IPv6, the intent is to allow the IEEE 802.17 network to be treated as a simple Ethernet LAN.

5.1 MPLS EXP bit ~~Mapping~~ mapping to RPR

MPLS support for DiffServ is defined in **RFC 3270 (Le Faucheur, F., “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services,” May 2002.)**[13]. The MPLS shim header is illustrated in Figure 2 below.

```
       |              20              |    3    |
1  |       8        |
       |-----------------------------|---------|--
---|----------------|
       |            Label             |   EXP   |
S  |      TTL       |
       |-----------------------------|---------|--
---|----------------|
```

Figure 2: MPLS shim

The EXP bits define the PHB. However **[12] (Rosen, E., “MPLS Label Stack Encoding,” January 2001.)**does not recommend specific EXP values for DiffServ PHB (e.g., EF, AF, DF).

5.1.1 MPLS EXP PHB ~~Mapping~~ mapping to RPR

The mapping between MPLS EXP bits to RPR header service class relevant fields are shown in Table 4. Note that four treatment aggregates are used as suggested by **[10] (Chan, K., “Aggregation of Diffserv Service Classes.,” February 2005.)**.

```
    |-------------|-------------------|--------
|---------------|
    |   MPLS EXP  | RPR Service Class | RPR sc |
RPR fe       |
```

```
|=============|==================|========|====
===========|
    |     000     |     Class C       |   00   |
1       |
    |     001     |                   |        |
|
    |-------------|------------------|--------
|---------------|
    |     010     |     Class B       |   01   |
0-Class B CIR |
    |     011     |                   |        |
1-Class B EIR |
    |-------------|------------------|--------
|---------------|
    |     100     |     ~~C~~class~~ ~~A0       |   11        |
|               |
    |             |        or         |   or   |
0       |
    |101(reserved)|     ~~Class ~~classA1       |            |
10   |               |
    |-------------|------------------|--------
|---------------|
    |     110     |     ~~Class ~~classA0       |            |
11   |               |
    |             |        or         |   or   |
0       |
    |111(reserved)|     ~~Class ~~classA1       |            |
10   |               |
    |-------------|------------------|--------
|---------------|
```

Table 4: MPLS EXP to RPR ~~Header ~~header ~~Mapping~~ mapping

---

6. Ethernet ~~Specific ~~specific ~~Details~~details

Encapsulation of Ethernet packets over IEEE 802.17 is fairly simple since they are both 802 MACs and can be either transparently mapped or bridged.

Details of address translation, priority mappings and learning are fully described in **IEEE 802.17 (,“Resilient packet ring access method and physical layer specifications -~~ “Resilient Packet Ring Access Method and Physical Layer Specifications -~~ medium access control parameters, physical layer interface, and management parameters,” July 2004.)**[2], **IEEE 802.17a (, “Media Access Control (MAC) Bridges - Amendment 1: Bridging of 802.17,” October 2004.)**[14], and **IEEE 802.17b (, “Resilient Packet Ring Access Method and Physical Layer Specifications - Amendment 1: Spatially Aware Sublayer,” .)**[15]

---

7. Security ~~Considerations~~considerations

This specification provides no security measures. In particular:

1. Masquerading and spoofing are possible. There is no strong authentication.
2. Traffic analysis and snooping is possible since no encryption is provided, either by this specification or by IEEE 802.17
3. Limited denial of Service attacks are possible by, eg, flooding the IEEE 802.17 network with ARP broadcasts. These attacks are limited to other class-C (best effort) traffic.
4. Attacks against the IEEE 802.17 ring management protocols are possible by stations that are directly connected to the ring. We note that all of these vulnerabilities exist today for transport of IP and MPLS over Ethernet networks.

---

8. IANA ~~Considerations~~considerations

A new ARP codepoint is to be assigned by IANA per **Section 3.1 (Address Resolution)**

---

9. Acknowledgements

The authors acknowledge and appreciate the work and comments of the IETF IPoRPR working group and the IEEE 802.17 working group.

---

10. References

[1] Bradner, S., "**Key words for use in RFCs to Indicate Requirements Levels**," RFC 2119, BCP 14, March 1997.

[2] "**Resilient Packet Ring Access Method and Physical Layer Specifications - medium access control parameters, physical layer interface, and management parameters**," IEEE 802.17-2004, July 2004.

[3] Postel, J., "**Internet Protocol**," RFC 791, September 1981.

[4] Plummer, D., "**An Ethernet Address Resolution Protocol**," RFC 826, November 1982.

[5] Crawford, ., "**Transmission of IPv6 Packets over Ethernet Networks**," RFC 2464, December 1998.

[6] Nichols, K., "**Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.**," RFC 2474, December 1998.

[7] Heinanen, J., "**Assured Forwarding PHB Group.**," RFC 2597, June 1999.

[8] Jacobson, V., "**An Expedited Forwarding PHB Group.**," RFC 2598, June 1999.

[9] Babiarz, J., "**Configuration Guidelines for Diffserv Service Classes**," draft-ietf-tsvwg-diffserv-service-classes-00 (work in progress), June 2005.

[10] Chan, K., "**Aggregation of Diffserv Service Classes.**," draft-chan-tsvwg-diffserv-class-aggr-01 (work in progress), February 2005.

[11] Ramakrishnan, K., "**The Addition of Explicit Congestion Notification (ECN) to IP**," RFC 3168, September 2001.

[12] Rosen, E., "**MPLS Label Stack Encoding**," RFC 3032, January 2001.

[13] Le Faucheur, F., "**Multi-Protocol Label Switching (MPLS) Support of Differentiated Services**," RFC 3270, May 2002.

[14] "**Media Access Control (MAC) Bridges - Amendment 1: Bridging of 802.17**," IEEE 802.17a-2004, October 2004.

[15] "**Resilient Packet Ring Access Method and Physical Layer**

Specifications - Amendment 1: Spatially Aware Sublayer,"
IEEE P802.17b.

Authors' ~~Addresses~~addresses

Marc Holness
Nortel
3500 Carling Avenue
Ottawa, ON K2H 8E9
CA
Phone: +1 613 765 2840
Email: holness@nortel.com

Glenn Parsons
Nortel
3500 Carling Avenue
Ottawa, ON K2H 8E9
CA
Phone: +1 613 763 7582
Email: gparsons@nortel.com

Intellectual ~~Property~~ property ~~Statement~~statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at **http://www.ietf.org/ipr**.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at **ietf-ipr@ietf.org**.

Disclaimer of ~~Validity~~validity

Copyright ~~Statement~~statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.