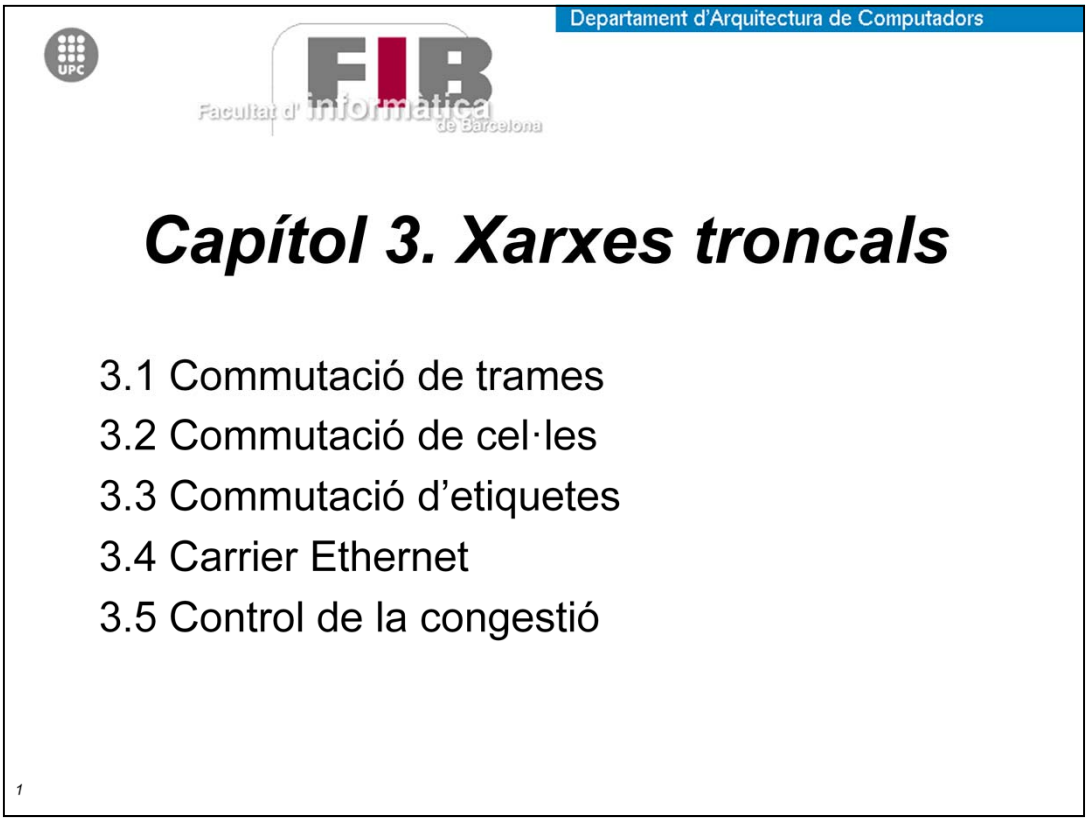
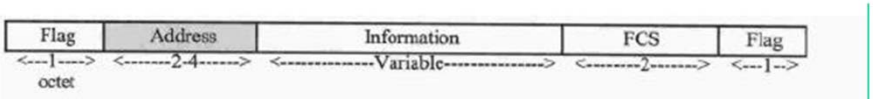

Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
Capítol 3. Xarxes troncals
3.1 Commutació de trames
3.2 Commutació de cel·les
3.3 Commutació d'etiquetes
3.4 Carrier Ethernet
3.5 Control de la congestió
1

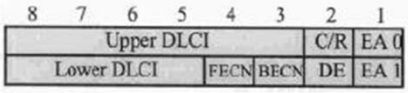

Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
3.1 Commutació de trames
2

Departament d'Arquitectura de Computadors

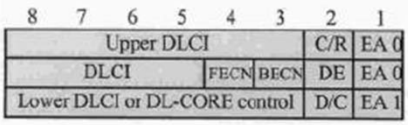
LAPF Core



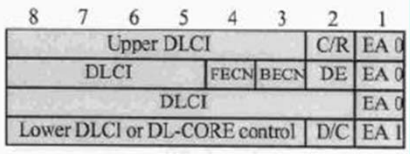
(a) Frame format



(b) Address field - 2 octets (default)



(c) Address field - 3 octets



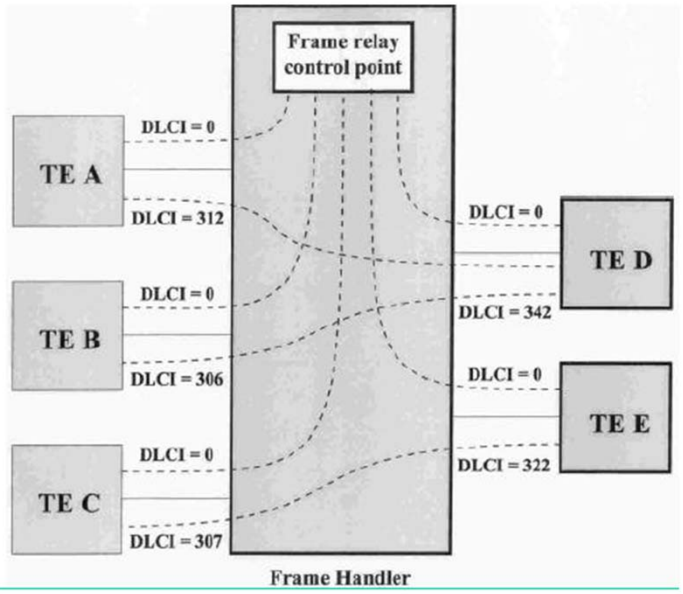
(d) Address field - 4 octets

EA	Address field extension bit
C/R	Command/response bit
FECN	Forward explicit congestion notification
BECN	Backward explicit congestion notification
DLCI	Data link connection identifier
D/C	DLCI or DL-CORE control indicator
DE	Discard eligibility

3

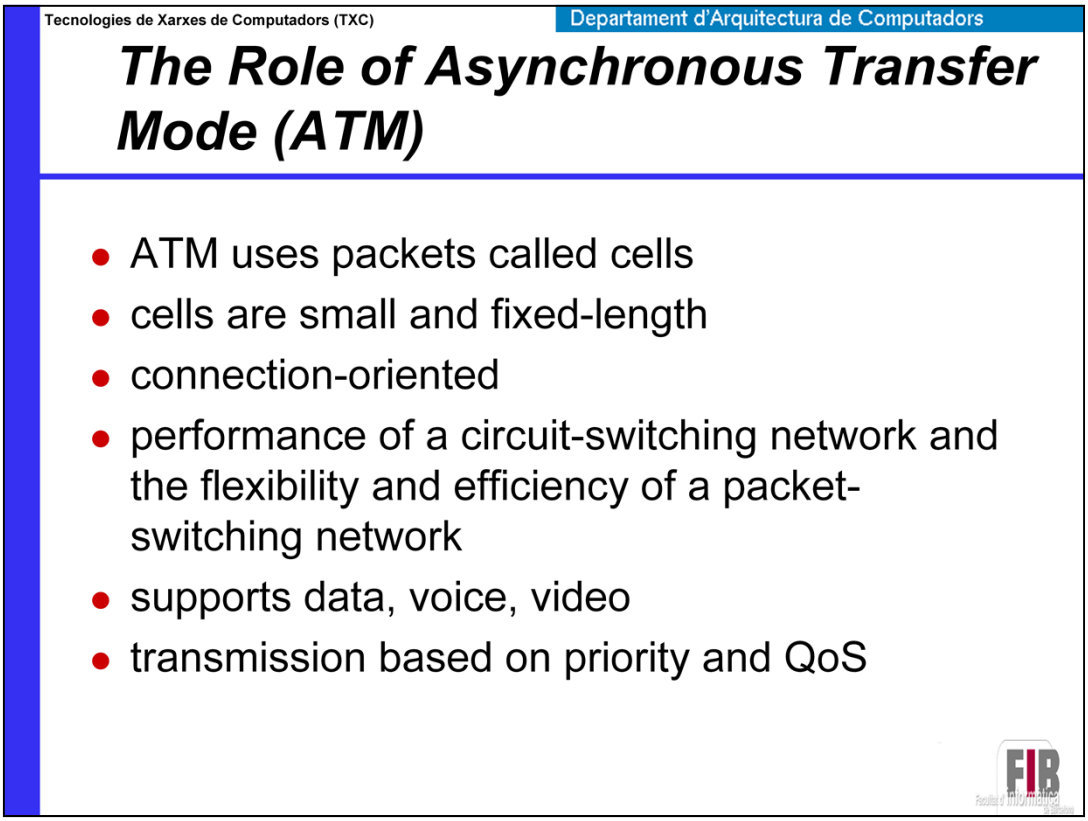
Departament d'Arquitectura de Computadors

Data Link Connection



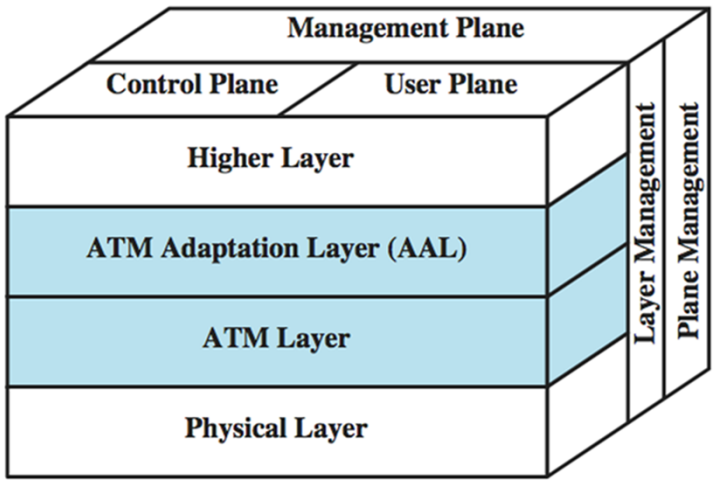
4


Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
3.2 Commutació de cel·les
5



Asynchronous transfer mode (ATM) is a switching and multiplexing technology that employs small, fixed-length packets, call **cells**. A fixed-size packet was chosen to ensure that the switching and multiplexing function could be carried out efficiently, with little delay variation. A small cell size was chosen primarily to support delay-intolerant interactive voice service with a small packetization delay. ATM is a connection-oriented packet-switching technology that was designed to provide the performance of a circuit-switching network and the flexibility and efficiency of a packet-switching network. A major thrust of the ATM standardization effort was to provide a powerful set of tools for supporting a rich QoS capability and a powerful traffic management capability. ATM was intended to provide a unified networking standard for both circuit-switched and packet-switched traffic, and to support data, voice, and video with appropriate QoS mechanisms. With ATM, the user can select the desired level of service, obtain guaranteed service quality. Internally, the ATM network makes reservations and preplans routes so that transmission allocation is based on priority and QoS characteristics.

Protocol Architecture



The standards issued for ATM by ITU-T are based on the protocol architecture shown in Stallings DCC9e Figure 11.1, which illustrates the basic architecture for an interface between user and network. The physical layer involves the specification of a transmission medium and a signal encoding scheme. The data rates specified at the physical layer range from 25.6 Mbps to 622.08 Mbps. Other data rates, both higher and lower, are possible.

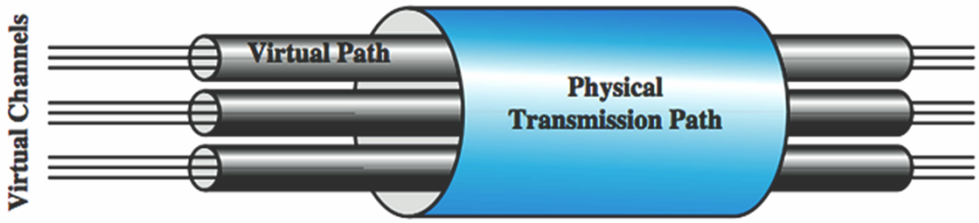
Two layers of the protocol architecture relate to ATM functions. There is an ATM layer common to all services that provides packet transfer capabilities, and an ATM adaptation layer (AAL) that is service dependent. The ATM layer defines the transmission of data in fixed-size cells and defines the use of logical connections. The use of ATM creates the need for an adaptation layer to support information transfer protocols not based on ATM. The AAL maps higher-layer information into ATM cells to be transported over an ATM network, then collects information from ATM cells for delivery to higher layers.

Delay in ATM networks

- End to end delay R = Rp + Rt
- Rp (packet delay) = *48x8* / V_{ts}
- Rt (transfer delay) = Tt + Tp + W
  - *Tt (transmission time)* Σt_t ($t_t = 53x8 / V_{tn}$)
  - *Tp (propagation time)* Σt_p ($t_p = d / V_p$)
  - *W (queue waiting time)* Σw ($w = nxt_t$)

ATM Virtual Path Connection

- virtual path connection (VPC)
  - bundle of VCC with same end points

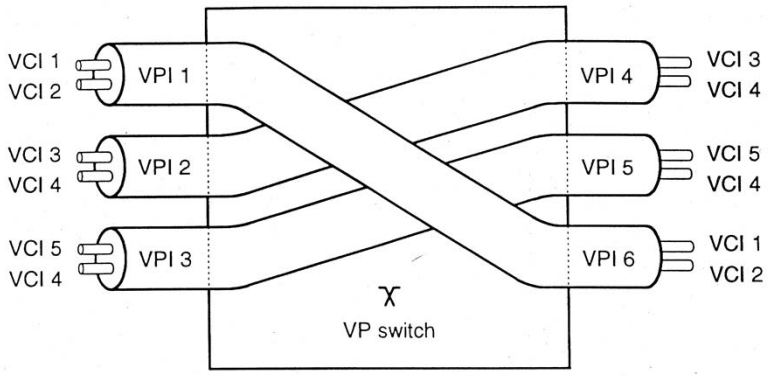


For ATM, a second sublayer of processing has been introduced that deals with the concept of virtual path (Stallings DCC9eFigure 11.4). A **virtual path connection** (VPC) is a bundle of VCCs that have the same endpoints. Thus, all of the cells flowing over all of the VCCs in a single VPC are switched together. The virtual path concept was developed in response to a trend in high-speed networking in which the control cost of the network is becoming an increasingly higher proportion of the overall network cost. The virtual path technique helps contain the control cost by grouping connections sharing common paths through the network into a single unit. Network management actions can then be applied to a small number of groups of connections instead of a large number of individual connections.

Departament d'Arquitectura de Computadors

Virtual Channel and Virtual Path

- Virtual Path switch



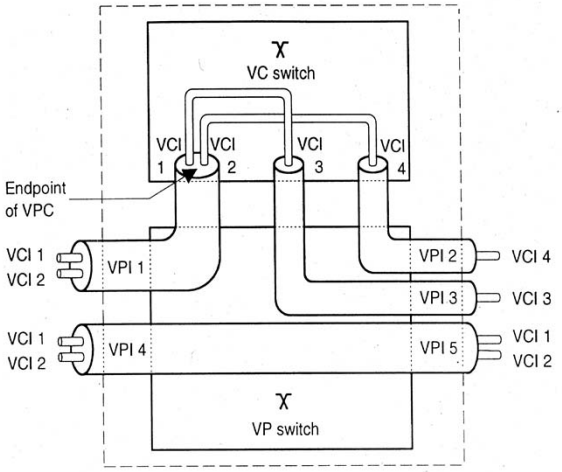
VCI Virtual channel identifier
VP Virtual path
VPI Virtual path identifier

10

Departament d'Arquitectura de Computadors

Virtual Channel and Virtual Path

- Virtual Channel switch



VC Virtual channel
VCI Virtual channel identifier

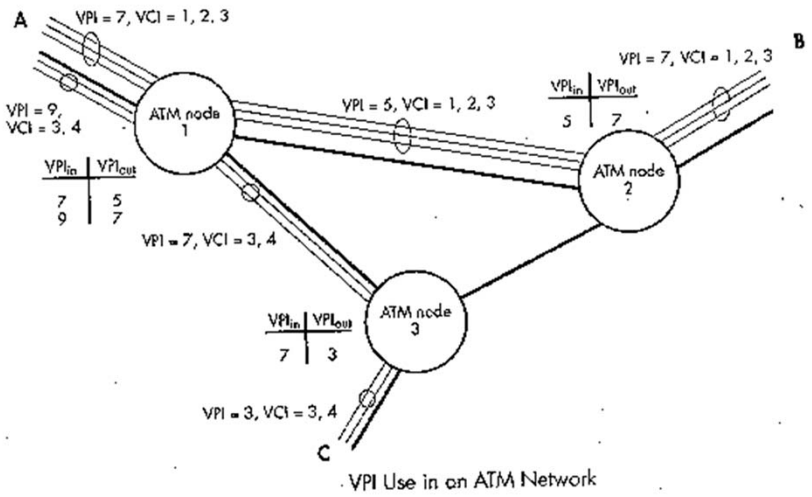
VP Virtual path
VPC Virtual path connection
VPI Virtual path identifier

11

Departament d'Arquitectura de Computadors

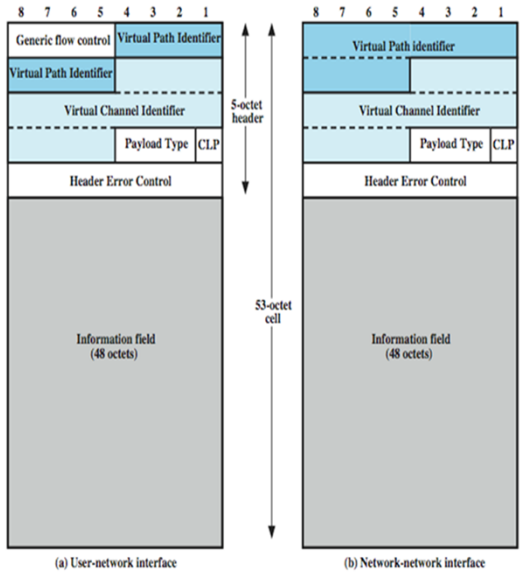
Virtual Channel and Virtual Path

- VPI and VCI relation



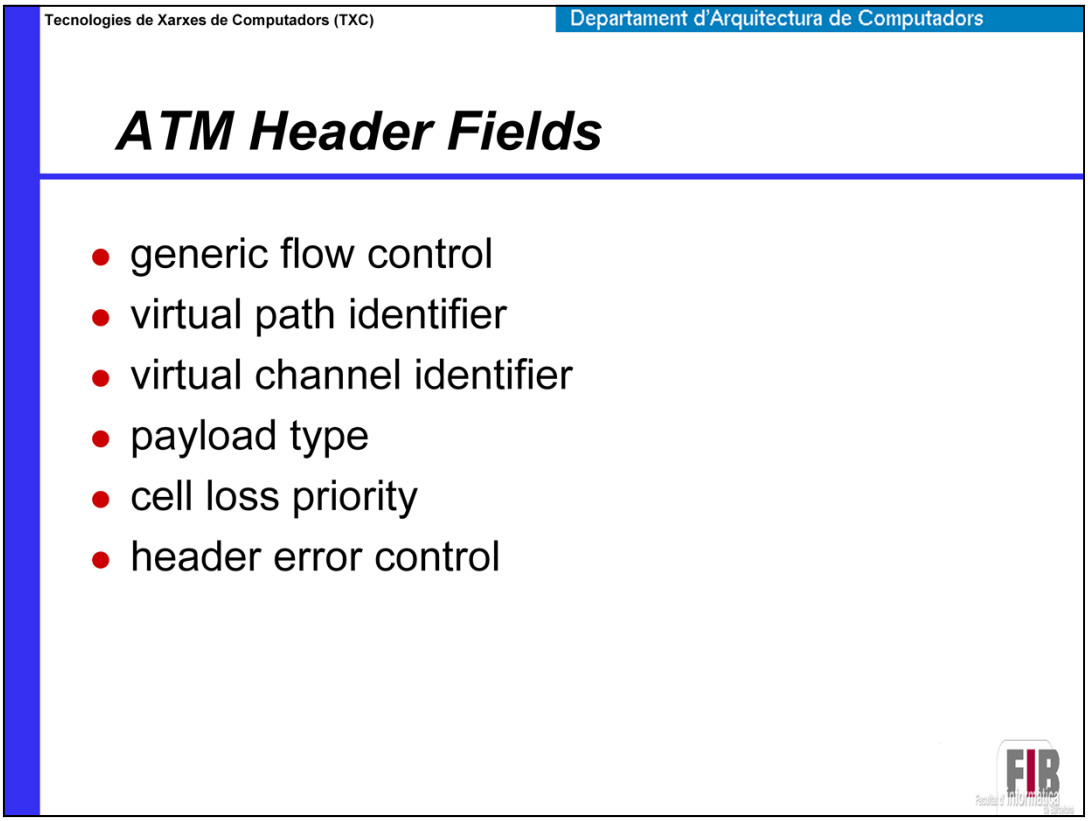
VPI Use in an ATM Network

ATM Cells



The asynchronous transfer mode makes use of fixed-size cells, consisting of a 5-octet header and a 48-octet information field. There are several advantages to the use of small, fixed-size cells. First, the use of small cells may reduce queuing delay for a high-priority cell, because it waits less if it arrives slightly behind a lower-priority cell that has gained access to a resource (e.g., the transmitter). Second, it appears that fixed-size cells can be switched more efficiently, which is important for the very high data rates of ATM [PARE88]. With fixed-size cells, it is easier to implement the switching mechanism in hardware.

Stallings DCC9e Figure 11.6a shows the cell header format at the user-network interface, & Stallings DCC9e Figure 11.6b shows the cell header format internal to the network.



The **Generic Flow Control** (GFC) field does not appear in the cell header internal to the network, but only at the user-network interface. Hence, it can be used for control of cell flow only at the local user-network interface. The field could be used to assist the customer in controlling the flow of traffic for different qualities of service. In any case, the GFC mechanism is used to alleviate short-term overload conditions in the network.

I.150 lists as a requirement for the GFC mechanism that all terminals be able to get access to their assured capacities. This includes all constant-bit-rate (CBR) terminals as well as the variable-bit-rate (VBR) terminals that have an element of guaranteed capacity (CBR and VBR are explained in Section 11.5). The current GFC mechanism is described in a subsequent subsection.

The **Virtual Path Identifier** (VPI) constitutes a routing field for the network. It is 8 bits at the user-network interface and 12 bits at the network-network interface. The latter allows support for an expanded number of VPCs internal to the network, to include those supporting subscribers and those required for network management. The **Virtual Channel Identifier** (VCI) is used for routing to and from the end user.

The **Payload Type** (PT) field indicates the type of information in the information field. Stallings DCC9e Table 11.2 shows the interpretation of the PT bits. A value of 0 in the first bit indicates user information (that is, information from the next higher layer). In this case, the second bit indicates whether congestion has been experienced; the third bit, known as the Service Data Unit

(SDU) type bit, is a one-bit field that can be used to discriminate two types of ATM SDUs associated with a connection. The term *SDU* refers to the 48-octet payload of the cell. A value of 1 in the first bit of the Payload Type field indicates that this cell carries network management or maintenance information. This indication allows the insertion of network-management cells onto a user's VCC without impacting the user's data. Thus, the PT field can provide inband control information.

The **cell loss priority** (CLP) bit is used to provide guidance to the network in the event of congestion. A value of 0 indicates a cell of relatively higher priority, which should not be discarded unless no other alternative is available. A value of 1 indicates that this cell is subject to discard within the network. The user might employ this field so that extra cells (beyond the negotiated rate) may be inserted into the network, with a CLP of 1, and delivered to the destination if the network is not congested. The network may set this field to 1 for any data cell that is in violation of an agreement concerning traffic parameters between the user and the network. In this case, the switch that does the setting realizes that the cell exceeds the agreed traffic parameters but that the switch is capable of handling the cell. At a later point in the network, if congestion is encountered, this cell has been marked for discard in preference to cells that fall within agreed traffic limits.

The **Header Error Control (HEC)** field is used for both error control and synchronization, as explained subsequently.

This is the term used in ATM Forum documents. In ITU-T documents, this bit is referred to as the ATM-user-to-ATM-user (AAU) indication bit. The meaning is the same.

Departament d'Arquitectura de Computadors

ATM Cells Format

- Pre-assigned values of the Cell Header at the physical layer

Cell type	Octet 1	Octet 2	Octet 3	Octet 4
IDLE cells	00000000	00000000	00000000	00000001
Physical Layer OAM	00000000	00000000	00000000	00001001
Reserved for use by Physical Layer	PPP0000	00000000	00000000	0000PPP1

P : Bit is available for use by the PHY layer

15

Departament d'Arquitectura de Computadors

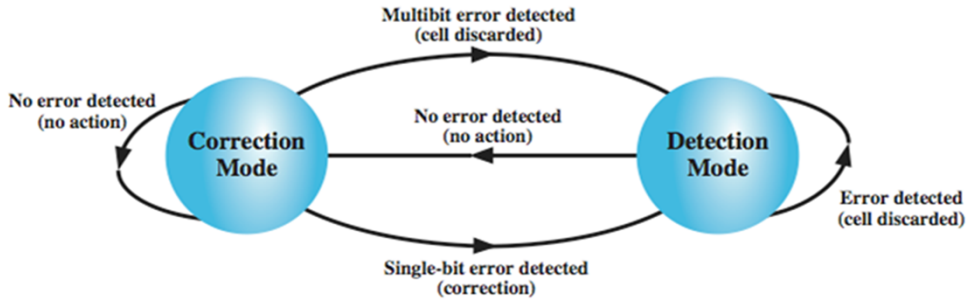
ATM Cells Format

- Payload Type indicator

Payload type	Meaning
000	User data cell, no congestion, cell type 0
001	User data cell, no congestion, cell type 1
010	User data cell, congestion experienced, cell type 0
011	User data cell, congestion experienced, cell type 1
100	Maintenance information between adjacent switches
101	Maintenance information between source and destination switches
110	Resource Management cell (used for ABR congestion control)
111	Reserved for future function

16

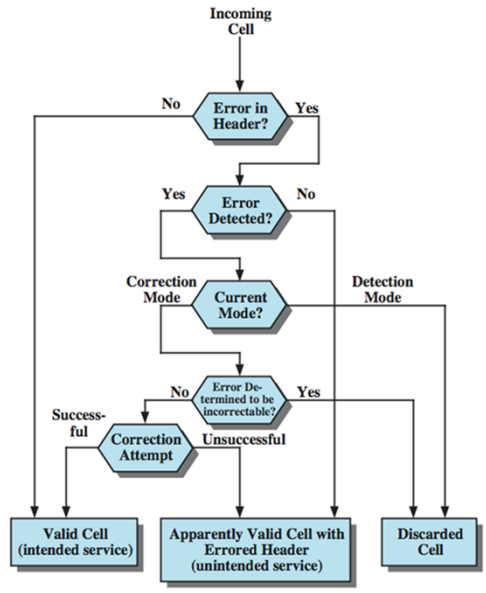
Header Error Control



Each ATM cell includes an 8-bit HEC field that is calculated based on the remaining 32 bits of the header. The polynomial used to generate the code is $X8 + X2 + X + 1$. In most existing protocols that include an error control field, such as HDLC, the data that serve as input to the error code calculation are in general much longer than the size of the resulting error code. This allows for error detection. In the case of ATM, the input to the calculation is only 32 bits, compared to 8 bits for the code. The fact that the input is relatively short allows the code to be used not only for error detection but also, in some cases, for actual error correction. This is because there is sufficient redundancy in the code to recover from certain error patterns.

Stallings DCC9e Figure 11.7 depicts the operation of the HEC algorithm at the receiver. At initialization, the receiver's error correction algorithm is in the default mode for single-bit error correction. As each cell is received, the HEC calculation and comparison is performed. As long as no errors are detected, the receiver remains in error correction mode. When an error is detected, the receiver will correct the error if it is a single-bit error or will detect that a multibit error has occurred. In either case, the receiver now moves to detection mode. In this mode, no attempt is made to correct errors. The reason for this change is a recognition that a noise burst or other event might cause a sequence of errors, a condition for which the HEC is insufficient for error correction. The receiver remains in detection mode as long as errored cells are received. When a header is examined and found not to be in error, the receiver switches back to correction mode.

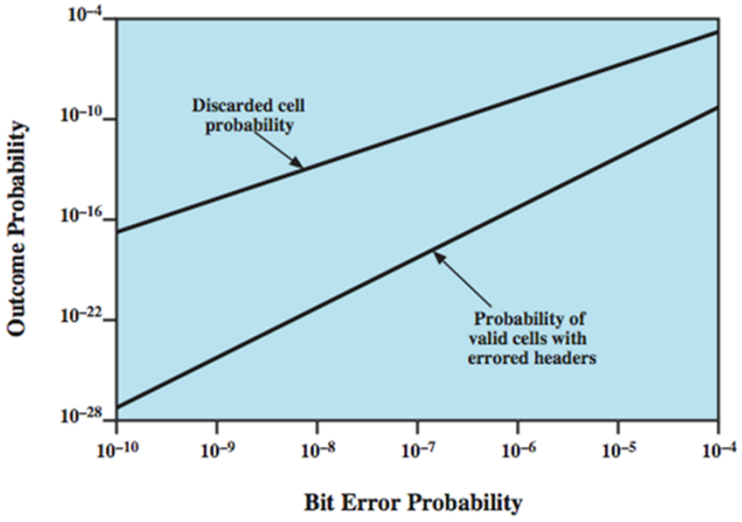
Effect of Error Cell Header



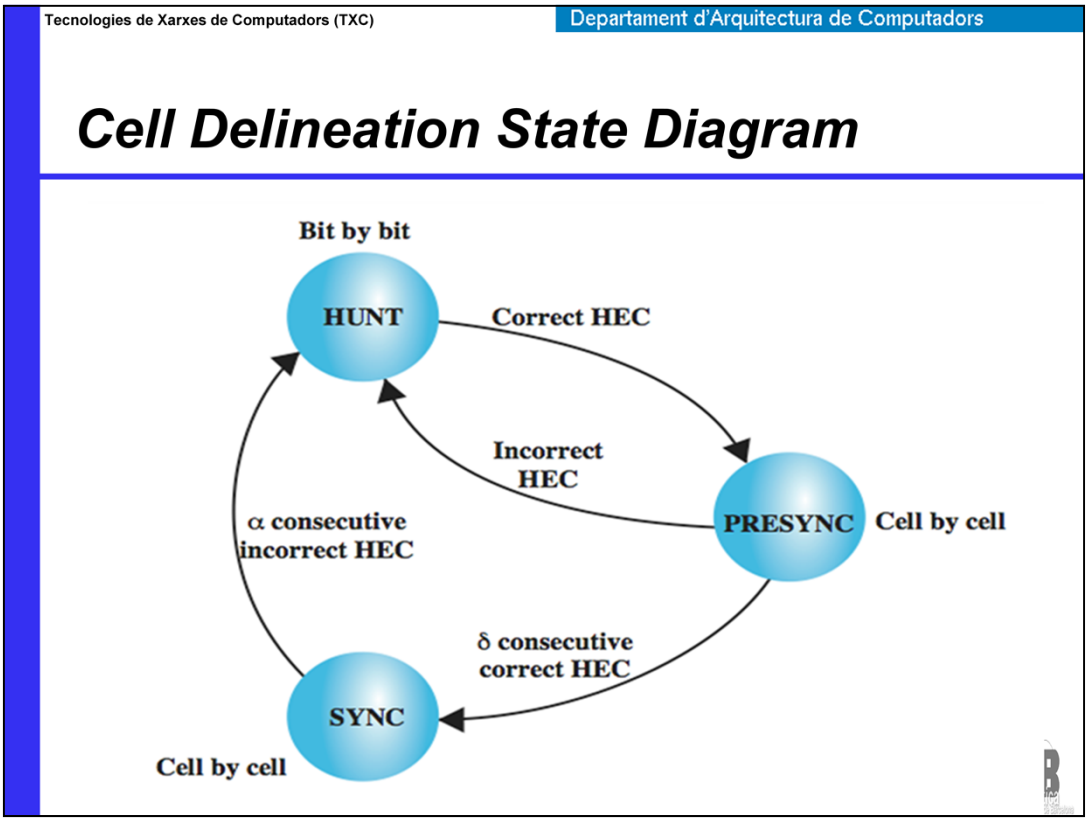
The flowchart of Stallings DCC9e Figure 11.8 shows the consequence of errors in the cell header.

The error-protection function provides both recovery from single-bit header errors and a low probability of the delivery of cells with errored headers under bursty error conditions. The error characteristics of fiber-based transmission systems appear to be a mix of single-bit errors and relatively large burst errors. For some transmission systems, the error correction capability, which is more time-consuming, might not be invoked.

Impact of Random Bit Errors on HEC Performance



Stallings DCC9e Figure 11.9, based on one in ITU-T I.432, indicates how random bit errors impact the probability of occurrence of discarded cells and valid cells with errored headers when HEC is employed.



Stallings DCC9e Figure 11.10 shows the procedure used as follows:

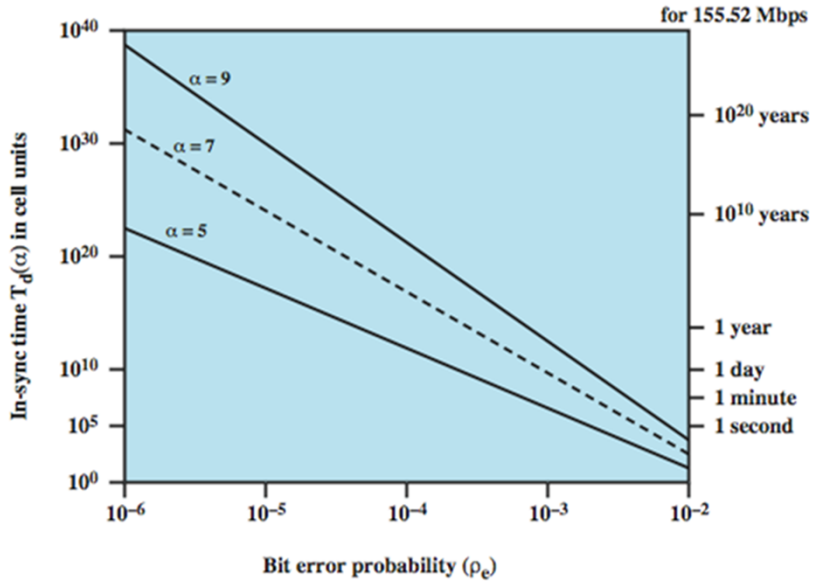
1. In the HUNT state, a cell delineation algorithm is performed bit by bit to determine if the HEC coding law is observed (i.e., match between received HEC and calculated HEC). Once a match is achieved, it is assumed that one header has been found, and the method enters the PRESYNC state.

2. In the PRESYNC state, a cell structure is now assumed. The cell delineation algorithm is performed cell by cell until the encoding law has been confirmed consecutively d times.

3. In the SYNC state, the HEC is used for error detection and correction (see Figure 11.7). Cell delineation is assumed to be lost if the HEC coding law is recognized consecutively as incorrect *a* times.

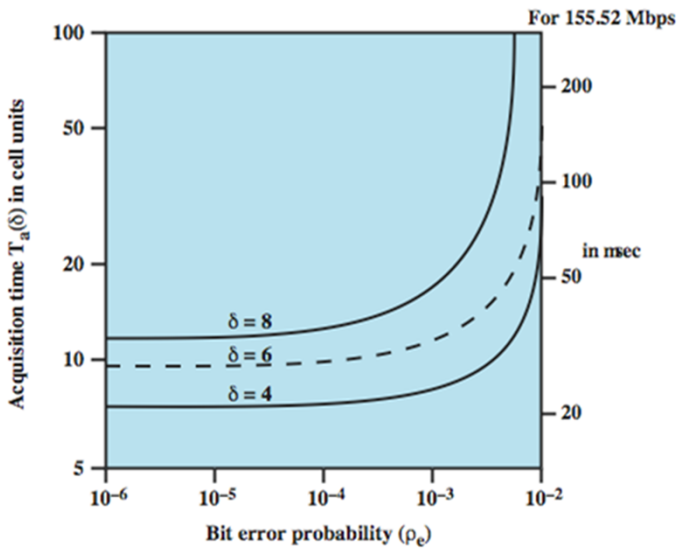
The values of a and d are design parameters. Greater values of d result in longer delays in establishing synchronization but in greater robustness against false delineation. Greater values of a result in longer delays in recognizing a misalignment but in greater robustness against false misalignment.

Impact of Random Bit Errors on Cell Delineation Performance



Stallings DCC9e Figures 11.11, based on I.432, show the impact of random bit errors on cell delineation performance for various values of a and d. The first figure shows the average amount of time that the receiver will maintain synchronization in the face of errors, with a as a parameter.

Acquisition Time vs. Bit Error Rate



Stallings DCC9e Figure 11.12, based on I.432, show the impact of random bit errors on cell delineation performance for various values of α and δ.

The second figure shows the average amount of time to acquire synchronization as a function of error rate, with d as a parameter.

The advantage of using a cell-based transmission scheme is the simplified interface that results when both transmission and transfer mode functions are based on a common structure.

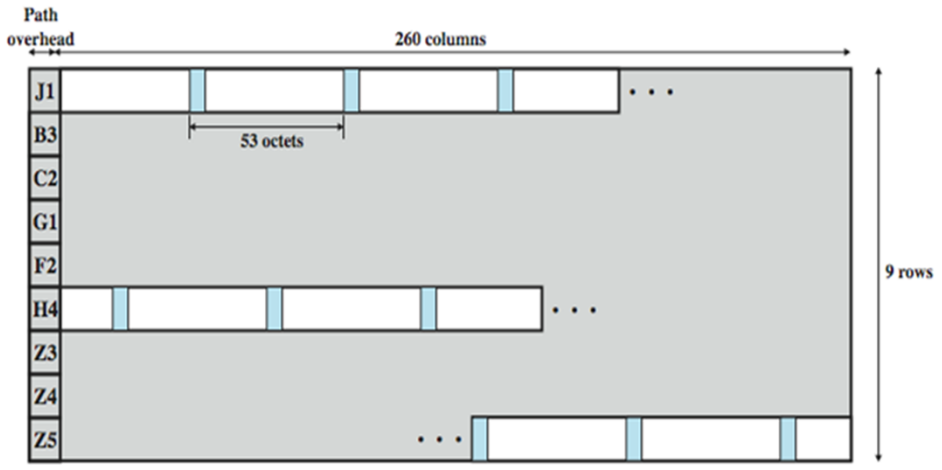
SDH Based Physical Layer

- imposes structure on ATM stream
  - eg. for 155.52Mbps
  - use STM-1 (STS-3) frame
- can carry ATM and STM payloads
- specific connections can be circuit switched using SDH channel
- SDH multiplexing techniques can combine several ATM streams

The SDH-based physical layer imposes a structure on the ATM cell stream.

For the SDH-based physical layer, framing is imposed using the STM-1 (STS-3) frame. Stallings DCC9e Figure 11.13 shows the payload portion of an STM-1 frame (see Stallings DCC 9eFigure 8.11). This payload may be offset from the beginning of the frame, as indicated by the pointer in the section overhead of the frame. As can be seen, the payload consists of a 9-octet path overhead portion and the remainder, which contains ATM cells. Because the payload capacity (2340 octets) is not an integer multiple of the cell length (53 octets), a cell may cross a payload boundary.

STM-1 Payload for SDH-Based ATM Cell Transmission



For the SDH-based physical layer, framing is imposed using the STM-1 (STS-3) frame. Stallings DCC9e Figure 11.13 shows the payload portion of an STM-1 frame (for comparison, see Stallings DCC9e Figure 8.11).

The H4 octet in the path overhead is set at the sending side to indicate the next occurrence of a cell boundary. That is, the value in the H4 field indicates the number of octets to the first cell boundary following the H4 octet. The permissible range of values is 0 to 52.

The advantages of the SDH-based approach include:

It can be used to carry either ATM-based or STM-based (synchronous transfer mode) payloads, making it possible to initially deploy a high-capacity fiber-based transmission infrastructure for a variety of circuit-switched and dedicated applications and then readily migrate to the support of ATM.

Some specific connections can be circuit switched using an SDH channel. For example, a connection carrying constant-bit-rate video traffic can be mapped into its own exclusive payload envelope of the STM-1 signal, which can be circuit switched. This may be more efficient than ATM switching.

Using SDH synchronous multiplexing techniques, several ATM streams can be combined to build interfaces with higher bit rates than those supported by the ATM layer at a particular site. For example, four separate ATM streams, each with a bit rate of 155 Mbps (STM-1), can be combined to build a 622-Mbps (STM-4) interface. This arrangement may be more cost effective than one using a

single 622-Mbps ATM stream.

Departament d'Arquitectura de Computadors

ATM Adaptation Layer

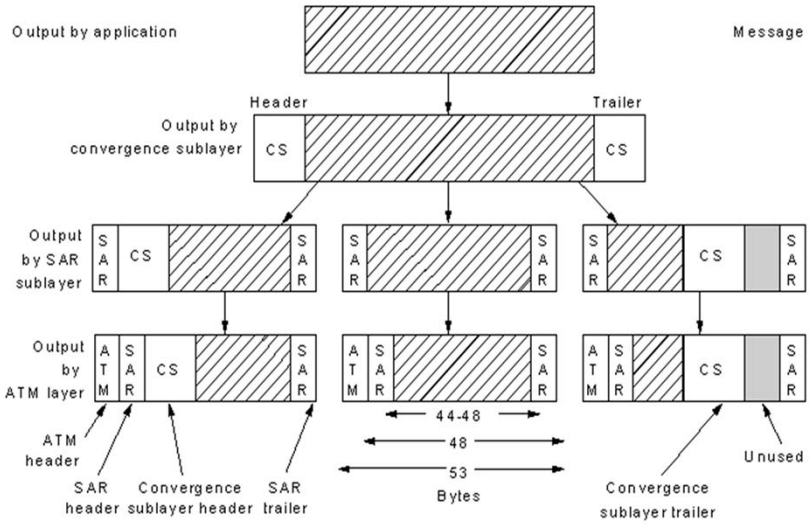
- Service Classification for AAL

	Class A	Class B	Class C	Class D
Timing relation between source and destination	Required		Not required	
Bit rate	Constant	Variable		
Connection mode	Connection-oriented			Connectionless
AAL Protocol	Type 1	Type 2	Type 3/4	Type 5

25

Departament d'Arquitectura de Computadors

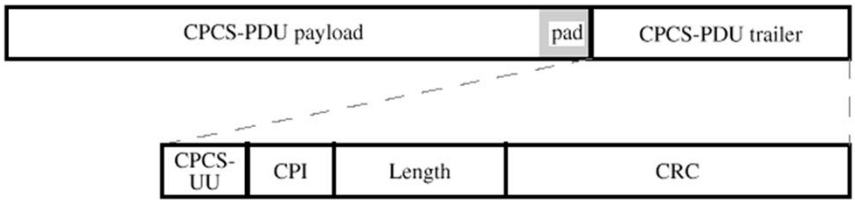
Segmentation and Reassembly



26

Departament d'Arquitectura de Computadors

AAL5 CPCS-PDU

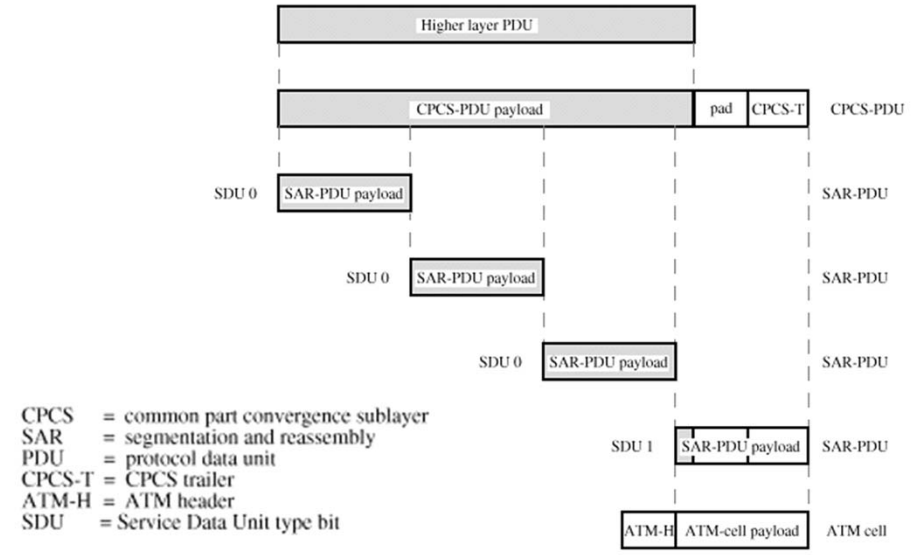


CPCS-UU = CPCS user-to-user indication (1 octet)
CPI = common part indicator (1 octet)
Length = length of CPCS-PDU payload (2 octets)
CRC = cyclic redundancy check (4 octets)

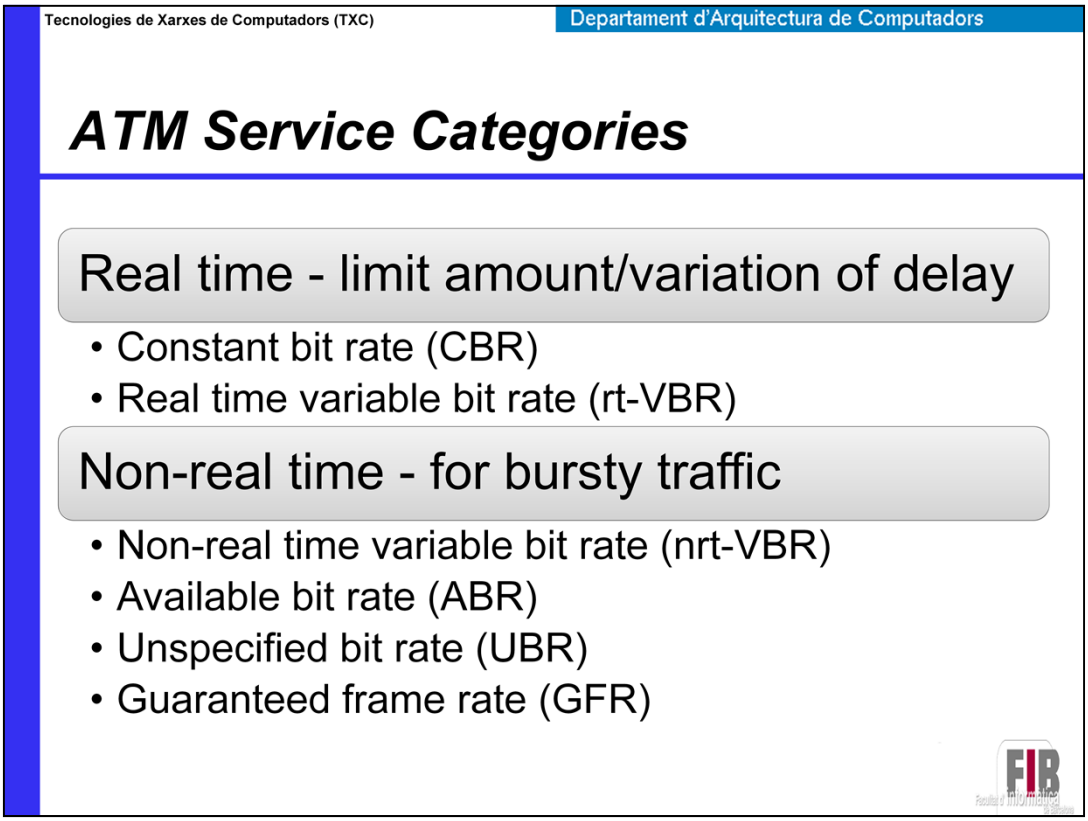
27

Departament d'Arquitectura de Computadors

AAL5 transmission



CPCS = common part convergence sublayer
SAR = segmentation and reassembly
PDU = protocol data unit
CPCS-T = CPCS trailer
ATM-H = ATM header
SDU = Service Data Unit type bit



An ATM network is designed to be able to transfer many different types of traffic simultaneously, including real-time flows such as voice, video, and bursty TCP flows. Although each such traffic flow is handled as a stream of 53-octet cells traveling through a virtual channel, the way in which each data flow is handled within the network depends on the characteristics of the traffic flow and the requirements of the application. For example, real-time video traffic must be delivered within minimum variation in delay.

We examine the way in which an ATM network handles different types of traffic flows in Chapter 13. In this section, we summarize ATM service categories, which are used by an end system to identify the type of service required. The following service categories have been defined by the ATM Forum:

•**Real-Time Service**

—Constant bit rate (CBR)

—Real-time variable bit rate (rt-VBR)

•**Non-Real-Time Service**

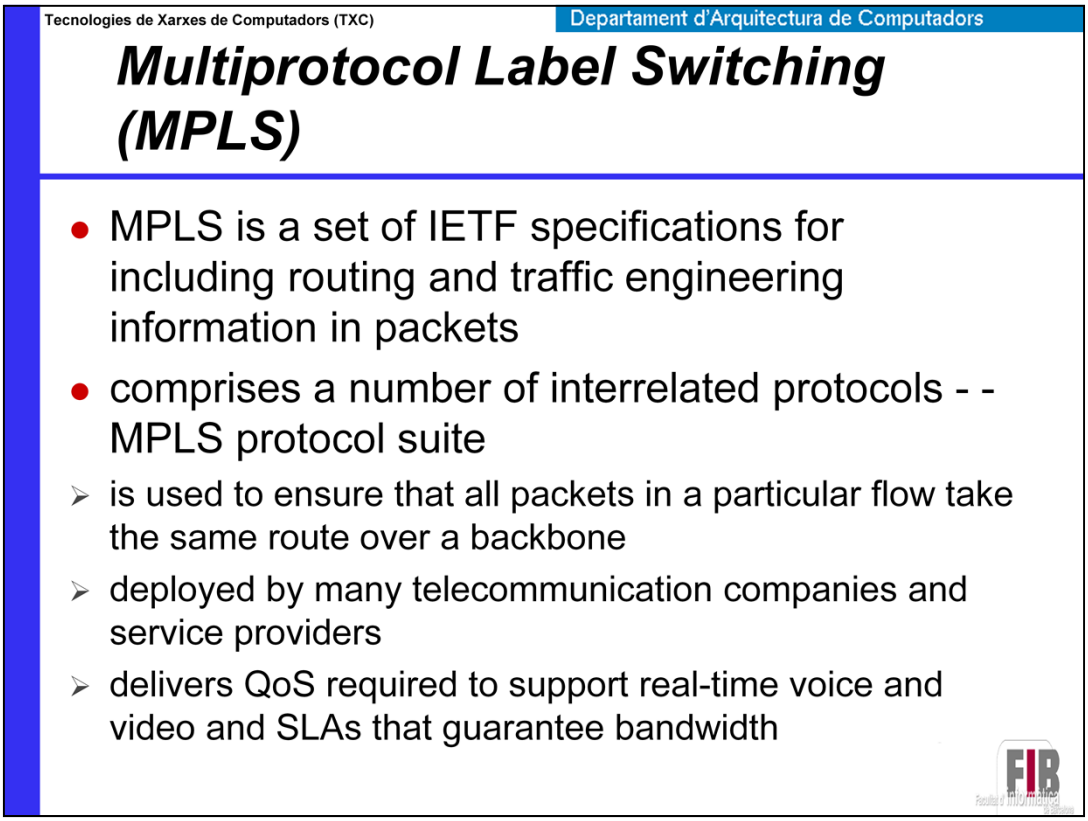
—Non-real-time variable bit rate (nrt-VBR)

—Available bit rate (ABR)

—Unspecified bit rate (UBR)

—Guaranteed frame rate (GFR)


Departament d'Arquitectura de Computadors
Facultat d' Informàtica de Barcelona
3.3 Commutació d'etiquetes
30



In Chapter 19, we examined a number of IP-based mechanisms designed to improve the performance of IP-based networks and to provide different levels of quality of service (QoS) to different service users. Although the routing protocols discussed in Chapter 19 have as their fundamental purpose dynamically finding a route through an internet between any source and any destination, they also provide support for performance goals in two ways:

1. Because these protocols are distributed and dynamic, they can react to congestion by altering routes to avoid pockets of heavy traffic. This tends to smooth out and balance the load on the internet, improving overall performance.

2. Routes can be based on various metrics, such as hop count and delay. Thus a routing algorithm develops information that can be used in determining how to handle packets with different service needs.

More directly, some of the mechanisms Chapter 19 (IS, DS) provide enhancements to an IP-based internet that explicitly provide support for QoS. However, none of the mechanisms or protocols so far discussed in Chapter 19 directly addresses the performance issue: how to improve the overall throughput and delay characteristics of an internet. MPLS is intended to provide connection-oriented QoS with features similar to those found in Differentiated Services; support traffic management to improve network throughput: and retain the flexibility of an IP-based networking approach.

Multiprotocol label switching (MPLS) is a set of Internet Engineering Task Force (IETF) specifications for including routing and traffic engineering information in packets. Thus, MPLS comprises a number of interrelated protocols, which can be referred to as the MPLS protocol suite. It can be used in IP networks but also in other types of packet-switching networks. MPLS is used to ensure that all packets in a particular flow take the same route over a backbone. Deployed by many telecommunication companies and service providers, MPLS delivers the quality of service (QoS) required to support real-time voice and video as well as service level agreements (SLAs) that guarantee bandwidth.

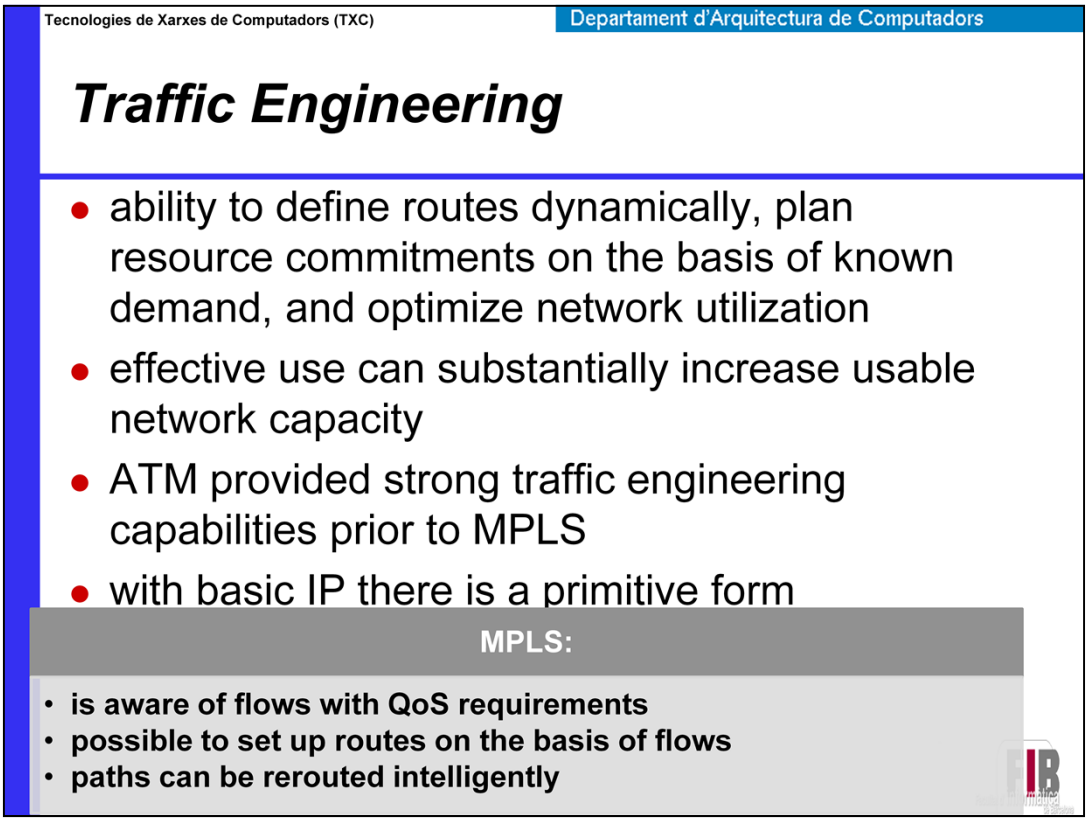
We begin this chapter with an overview of the current status of MPLS as a networking technology.

Although the basic principles of MPLS are straightforward, the set of protocols and procedures that have been built up around MPLS is formidable. As of this writing, the IETF MPLS working group has issued 70 RFCs and has 29 active Internet Drafts. In addition, there four other IETF working groups developing RFCs on topics related to MPLS. Thus, even a book-length treatment fails to capture the full extent of MPLS. Accordingly, the goal is this chapter is to present the fundamental concepts and an overview of the breadth of MPLS.

Role of MPLS

- efficient technique for forwarding and routing packets
- designed with IP networks in mind
  - can be used with any link-level protocol
- fixed-length label encapsulates an IP packet or a data link frame
- MPLS label contains all information needed to perform routing, delivery, Qos, and traffic management functions
- is connection oriented

In essence, MPLS is an efficient technique for forwarding and routing packets. MPLS was designed with IP networks in mind, but the technology can be used without IP to construct a network with any link-level protocol, including ATM and frame relay. In an ordinary packet-switching network packet switches must examine various fields within the packet heard to determine destination, route, quality of service (QoS), and any traffic management functions (such as discard or delay) that may be supported. Similarly, in an IP-based network, routers examine a number of fields in the IP header to determine these functions. In an MPLS network, a fixed-length label encapsulates an IP packet or a data link frame. The MPLS label contains all the information needed by an MPLS-enabled router to perform routing, delivery, QoS, and traffic management functions. Unlike IP, MPLS is connection oriented.



Traffic Engineering

MPLS makes it easy to commit network resources in such a way as to balance the load in the face of a given demand and to commit to differential levels of support to meet various user traffic requirements. The ability to define routes dynamically, plan resource commitments on the basis of known demand, and optimize network utilization is referred to as **traffic engineering**. Prior to the advent of MPLS, the one networking technology that provided strong traffic engineering capabilities was ATM.

With the basic IP mechanism, there is a primitive form of automated traffic engineering. Specifically, routing protocols such as OSPF enable routers to dynamically change the route to a given destination on a packet-by-packet basis to try to balance load. But such dynamic routing reacts in a very simple manner to congestion and does not provide a way to support QoS. All traffic between two endpoints follows the same route, which may be changed when congestion occurs. MPLS, on the other hand, is aware of not just individual packets but flows of packets in which each flow has certain QoS requirements and a predictable traffic demand. With MPLS, it is possible to set up routes on the basis of these individual flows, with two different flows between the same endpoints perhaps following different routers. Further, when congestion threatens, MPLS paths can be rerouted intelligently. That is, instead of simply changing the route on a packet-by-packet basis, with MPLS, the routes are changed on a flow-by-flow basis, taking advantage of the known traffic demands of each flow. Effective use of traffic engineering can substantially increase usable

network capacity.

MPLS Operation

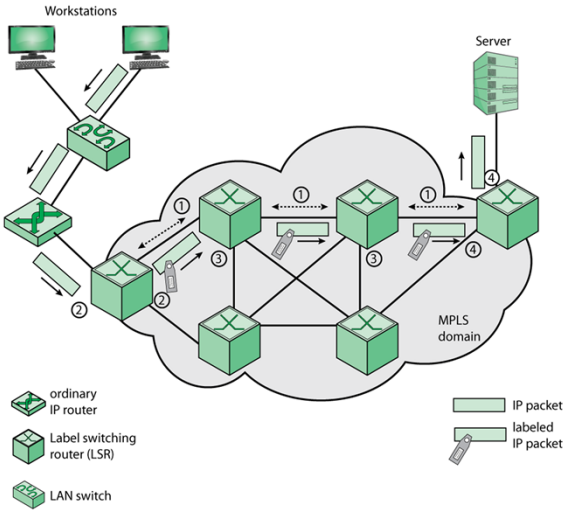


Figure 21.1 MPLS Operation

Stallings DCC9e Figure 21.1 depicts the operation of MPLS within a domain of MPLS-enabled routers. The following are key elements of the operation:

1. Prior to the routing and delivery of packets in a given FEC, a path through the network, known as a **label switched path** (LSP), must be defined and the QoS parameters along that path must be established. The QoS parameters determine (1) how much resources to commit to the path, and (2) what queuing and discarding policy to establish at each LSR for packets in this FEC. To accomplish these tasks, two protocols are used to exchange the necessary information among routers:

(a) An interior routing protocol, such as OSPF, is used to exchange reachability and routing information.

(b) Labels must be assigned to the packets for a particular FEC. Because the use of globally unique labels would impose a management burden and limit the number of usable labels, labels have local significance only, as discussed subsequently. A network operator can specify explicit routes manually and assign the appropriate label values. Alternatively, a protocol is used to determine the route and establish label values between adjacent LSRs. Either of two protocols can be used for this purpose: the Label Distribution Protocol (LDP) or an enhanced version of RSVP. LDP is now considered the standard technique, with the RSVP approach deprecated.

2. A packet enters an MPLS domain through an ingress edge LSR, where it is processed to determine which network-layer services it requires, defining its QoS. The LSR assigns this packet to a particular FEC, and therefore a particular LSP; appends the appropriate label to the packet; and forwards the packet. If no LSP yet exists for this FEC, the edge LSR must cooperate with the other LSRs in defining a new LSP.

3. Within the MPLS domain, as each LSR receives a labeled packet, it

(a) Removes the incoming label and attaches the appropriate outgoing label to the packet

(b) Forwards the packet to the next LSR along the LSP

4. The egress edge LSR strips the label, reads the IP packet header, and forwards the packet to its final destination.

Several key features of MLSP operation can be noted at this point:

1. An MPLS domain consists of a contiguous, or connected, set of MPLS-enabled routers. Traffic can enter or exit the domain from an endpoint on a directly connected network, as shown in the upper-right corner of Figure 21.1. Traffic may also arrive from an ordinary router that connects to a portion of the internet not using MPLS, as shown in the upper-left corner of Figure 21.1.

2. The FEC for a packet can be determined by one or more of a number of parameters, as specified by the network manager. Among the possible parameters:

—Source and/or destination IP addresses or IP network addresses

—Source and/or destination port numbers

—IP protocol ID

—Differentiated services codepoint

—IPv6 flow label

3. Forwarding is achieved by doing a simple lookup in a predefined table that maps label values to next hop addresses. There is no need to examine or process the IP header or to make a routing decision based on destination IP address. This not only makes it possible to separate types of traffic, such as best effort traffic from mission-critical traffic, it also renders an MPLS solution highly scalable. MPLS decouples packet forwarding from IP header information because it uses different mechanisms to assign labels. Labels have local significance only; therefore, it's nearly impossible to run out of labels. This characteristic is essential to implementing advanced IP services such as QoS, VPNs, and traffic engineering

4. A particular per-hop behavior (PHB) can be defined at an LSR for a given FEC. The PHB defines the queuing priority of the packets for this FEC and the discard policy.

5. Packets sent between the same endpoints may belong to different FECs. Thus, they will be labeled differently, will experience different PHB at each LSR, and may follow different paths through the network.

MPLS Packet Forwarding

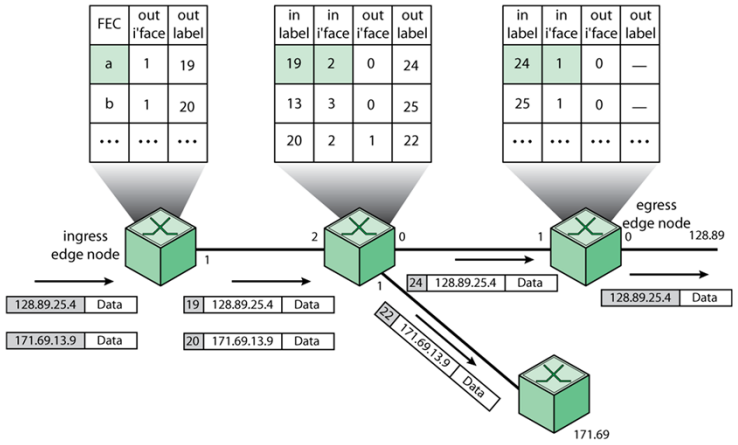


Figure 21.2 MPLS Packet Forwarding

Stallings DCC9e Figure 21.2 shows the label-handling and forwarding operation in more detail. Each LSR maintains a forwarding table for each LSP passing through the LSR. When a labeled packet arrives, the LSR indexes the forwarding table to determine the next hop. For scalability, as was mentioned, labels have local significance only. Thus, the LSR removes the incoming label from the packet and attaches the matching outgoing label before forwarding the packet. The ingress edge LSR determines the FEC for each incoming unlabeled packet and, on the basis of the FEC, assigns the packet to a particular LSP, attaches the corresponding label, and forwards the packet. In this example, the first packet arrives at the edge LSR, which reads the IP header for the destination address prefix, 128.89. The LSR then looks up the destination address in the switching table, inserts a label with a 20-bit label value of 19, and forwards the labeled packet out interface 1. This interface is attached via a link to a core LSR, which receives the packet on its interface 2. The LSR in the core reads the label and looks up its match in its switching table, then replaces label 19 with label 24, and forwards it out interface 0. The egress LSR reads and looks up label 4 in its table, which says to strip the label and forward the packet out interface 0.

LSP Creation and Packet Forwarding

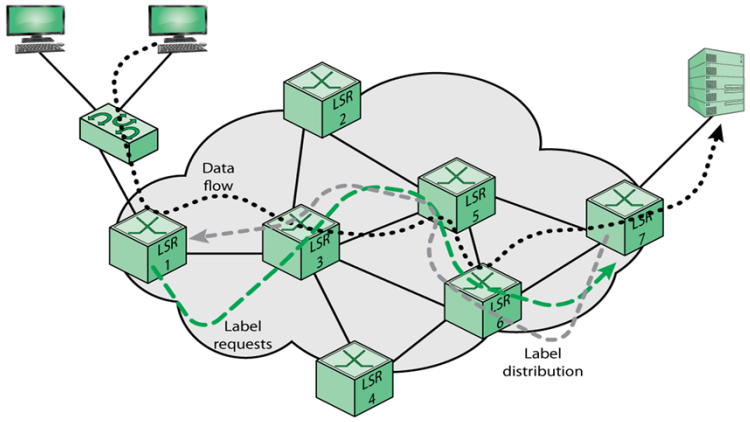
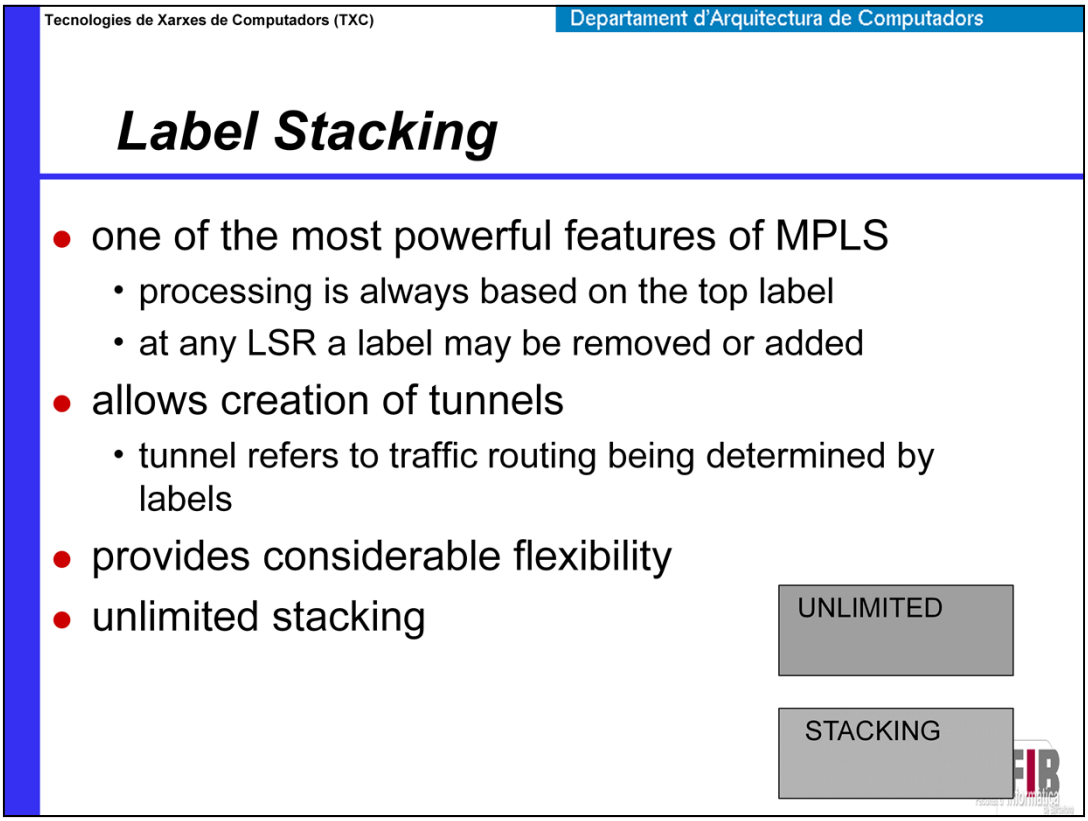


Figure 21.3 LSP Creation and Packet Forwarding through an MPLS Domain

Let us now look at an example that illustrates the various stages of operation of MPLS, using Stallings DCC9e Figure 21.3. We examine the path of a packet as it a source workstation to a destination server. Across the MPLS network, the packet enters at egress node LSR 1. Assume that this is the first occurrence of a packet on a new flow of packets, so that LSR 1 does not have a label for the packet. LSR 1 consults the IP header to find the destination address and then determine the next hop. Assume in this case that the next hop is LSR 3. Then, LSR 1 initiates a label request toward LSR 3. This request propagates through the network as indicated by the dashed green line.

Each intermediate router receives a label from its downstream router starting from LSR 7 and going upstream until LSR 1, setting up an LSP. The LSP setup is indicated by the dashed grey line. The setup can be performed using LDP and may or may not involve traffic engineering considerations.

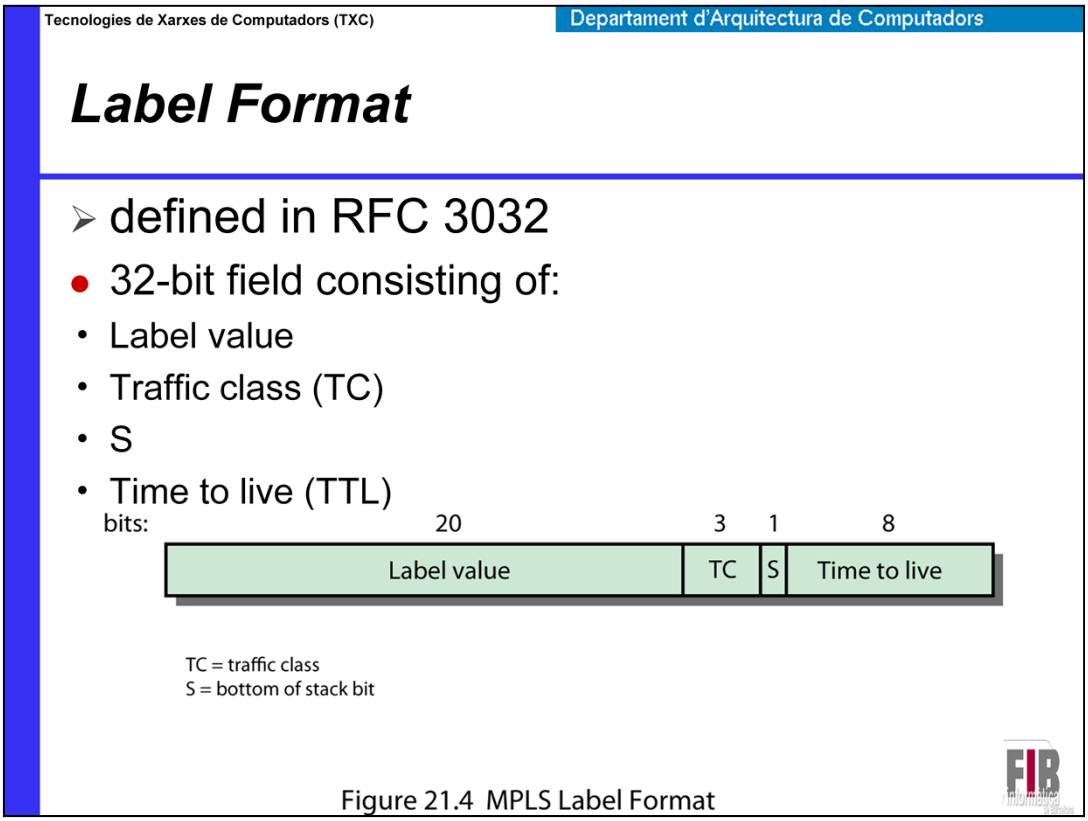
LSR 1 is now able to insert the appropriate label and forward the packet to LSR 3. Each subsequent LSR (LSR 5, LSR 6, LSR 7) examines the label in the received packet, replaces it with the outgoing label, and forwards it. When the packet reaches LSR 7, the LSR removes the label because the packet is departing the MPLS domain and delivers the packet to the destination.



Label Stacking

One of the most powerful features of MPLS is label stacking. A labeled packet may carry a number of labels, organized as a last-in-first-out stack. Processing is always based on the top label. At any LSR, a label may be added to the stack (push operation) or removed from the stack (pop operation). Label stacking allows the aggregation of LSPs into a single LSP for a portion of the route through a network, creating a tunnel. The term *tunnel* refers to the fact that traffic routing is determined by labels, and is exercised below normal IP routing and filtering mechanisms. At the beginning of the tunnel, an LSR assigns the same label to packets from a number of LSPs by pushing the label onto each packet's stack. At the end of the tunnel, another LSR pops the top element from the label stack, revealing the inner label. This is similar to ATM, which has one level of stacking (virtual channels inside virtual paths) but MPLS supports unlimited stacking.

Label stacking provides considerable flexibility. An enterprise could establish MPLS-enabled networks at various sites and establish a number of LSPs at each site. The enterprise could then use label stacking to aggregate multiple flows of its own traffic before handing it to an access provider. The access provider could aggregate traffic from multiple enterprises before handing it to a larger service provider. Service providers could aggregate many LSPs into a relatively small number of tunnels between points of presence. Fewer tunnels means smaller tables, making it easier for a provider to scale the network core.



Label Format

An MPLS label is a 32-bit field consisting of the following elements (Stallings DCC9e Figure 21.4), defined in RFC 3032:

Label value: Locally significant 20-bit label. Values 0 through 15 are reserved.

Traffic class (TC): 3 bits used to carry traffic class information.

S: Set to one for the oldest entry in the stack, and zero for all other entries. Thus, this bit marks the bottom of the stack.

Time to live (TTL): 8 bits used to encode a hop count, or time to live, value.

Label Placement

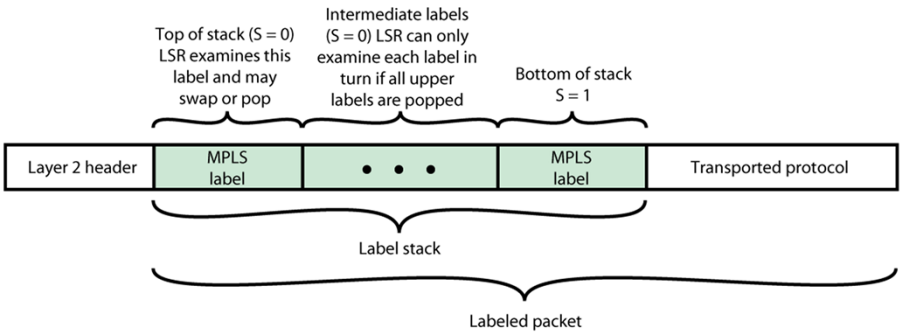


Figure 21.5 Encapsulation for Labeled Packet

Label Placement

The label stack entries appear after the data link layer headers, but before any network layer headers. The top of the label stack appears earliest in the packet (closest to the data link header), and the bottom appears latest (closest to the network layer header), as shown in Stallings DCC9e Figure 21.5. The network layer packet immediately follows the label stack entry that has the S bit set.

Label Stack

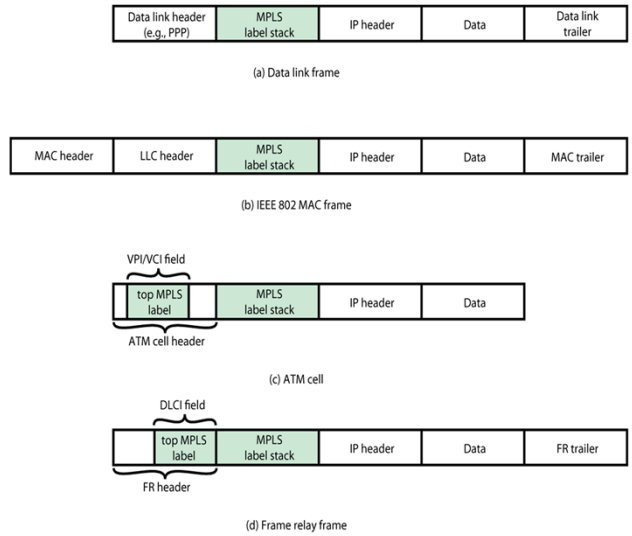
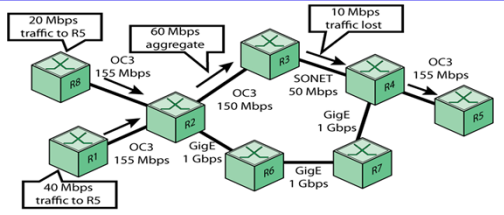


Figure 21.6 Position of MPLS Label Stack

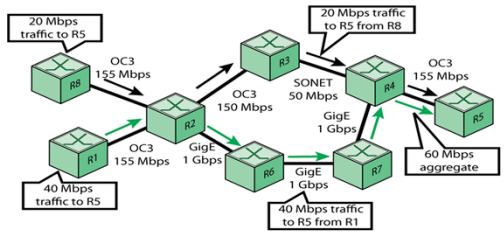
In data link frame, such as for PPP (point-to-point protocol), the label stack appears between the IP header and the data link header (Stallings DCC9e Figure 21.6a). For an IEEE 802 frame, the label stack appears between the IP header and the LLC (logical link control) header (Figure 21.6b).

If MPLS is used over a connection-oriented network service, a slightly different approach may be taken, as shown in Figures 21.6c and d. For ATM cells, the label value in the topmost label is placed in the VPI/VCI field in the ATM cell header. The entire top label remains at the top of the label stack, which is inserted between the cell header and the IP header. Placing the label value in the ATM cell header facilitates switching by an ATM switch, which would, as usual, only need to look at the cell header. Similarly, the topmost label value can be placed in the DLCI (data link connection identifier) field of a frame relay header. Note that in both these cases, the Time to Live field is not visible to the switch and so is not decremented. The reader should consult the MPLS specifications for the details of the way this situation is handled.

Example of Traffic Engineering



(a) A shortest-path solution



(b) A traffic-engineered solution

Figure 21.9 Traffic Engineering Example

Stallings DCC9e Figure 21.9 provides a simple example of traffic engineering. Both R1 and R8 have a flow of packets to send to R5. Using OSPF or some other routing protocol, the shortest path is calculated as R2-R3-R4. However, if we assume that R8 has a steady-state traffic flow of 20 Mbps and R1 has a flow of 40 Mbps, then the aggregate flow over this route will be 60 Mbps, which will exceed the capacity of the R3-R4 link. As an alternative, a traffic engineering approach is to determine a route from source to destination ahead of time and reserve the required resources along the way by setting up a LSP and associating resource requirements with that LSP. In this case, the traffic from R8 to R5 follows the shortest route, but the traffic from R1 to R5 follows a longer route that avoids overloading the network.

RSVP – TE Operation

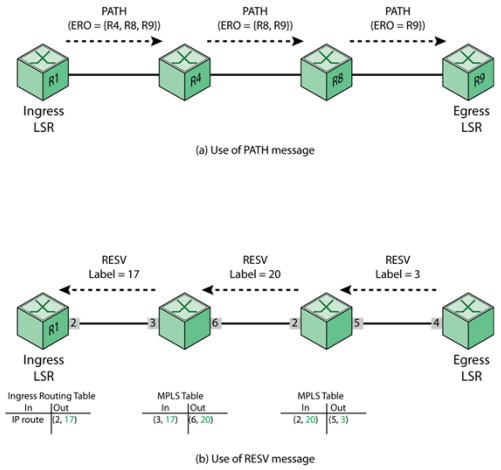


Figure 21.11 RSVP-TE Operation

RSVP-TE

Early in the MPLS standardization process, it became clear that a protocol was needed that would enable providers to set up LSPs that took into account QoS and traffic engineering parameters. Development of this type of signaling protocol proceeded on two different tracks:

Extensions to RSVP for setting up MPLS tunnels, known as RSVP-TE [RFC3209]

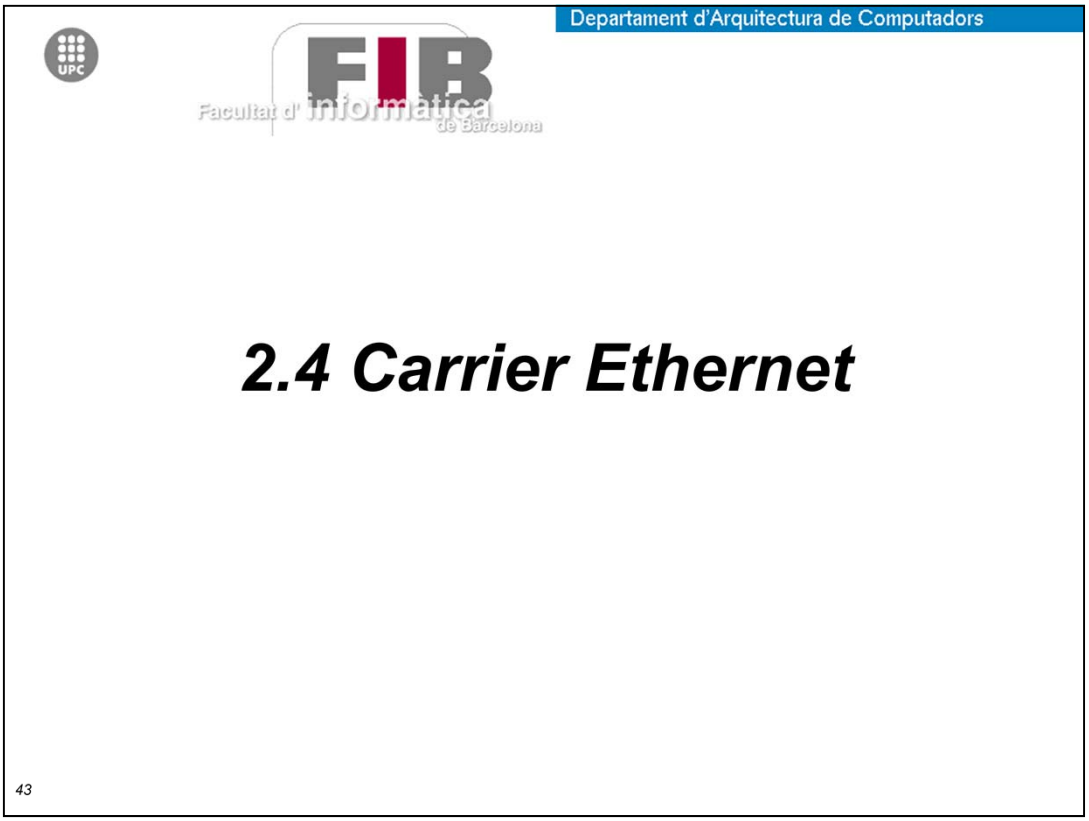
Extensions to LDP for setting constraint based LSPs [RFC3212]

The motivation for the choice of protocol in both cases was straightforward. Extending RSVP-TE to do in an MPLS environment what it already was doing (handling QoS information and reserving resources) in an IP environment is comprehensible; you only have to add the label distribution capability. Extending a native MPLS protocol like LDP, which was designed to do label distribution, to handle some extra TLVs with QoS information is also not revolutionary. Ultimately, the MPLS working group announced, in RFC 3468, that RSVP-TE is the preferred solution.

In general terms, RSVP-TE operates by associating an MPLS label with an RSVP flow. RSVP is used to reserve resources and to define an explicit router for an LSP tunnel. Stallings DCC9e Figure 21.11 illustrates the basic operation of RSVP-TE. An ingress node uses the RSVP PATH message to request an LSP to be defined along an explicit route. The PATH message includes a label request object and an explicit route object (ERO). The ERO defines the explicit route to be followed by the LSP.

The destination node of a label-switched path responds to a LABEL_REQUEST by including a LABEL object in its response RSVP Resv message. The LABEL object is inserted in the filter spec list immediately following the filter spec to which it pertains. The Resv message is sent back upstream towards the sender,

following the path state created by the Path message, in reverse order.



Fins aquí el primer control 2014 tardor

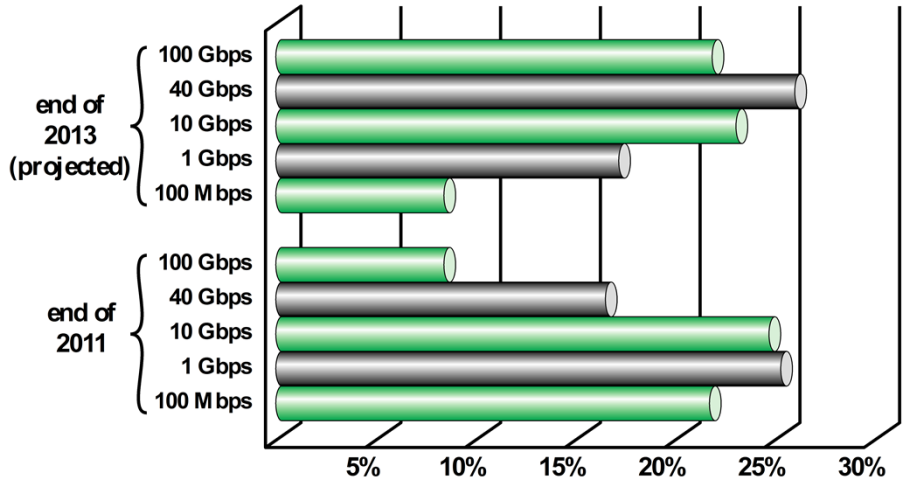


Figure 12.1 Data Center Study—Percentage of Ethernet Links by Speed

Figure 12.1, based on data from [IEEE12], shows that systems running at 1 Gbps and above dominate in data centers, and that demand is rapidly evolving toward 100-Gbps systems.

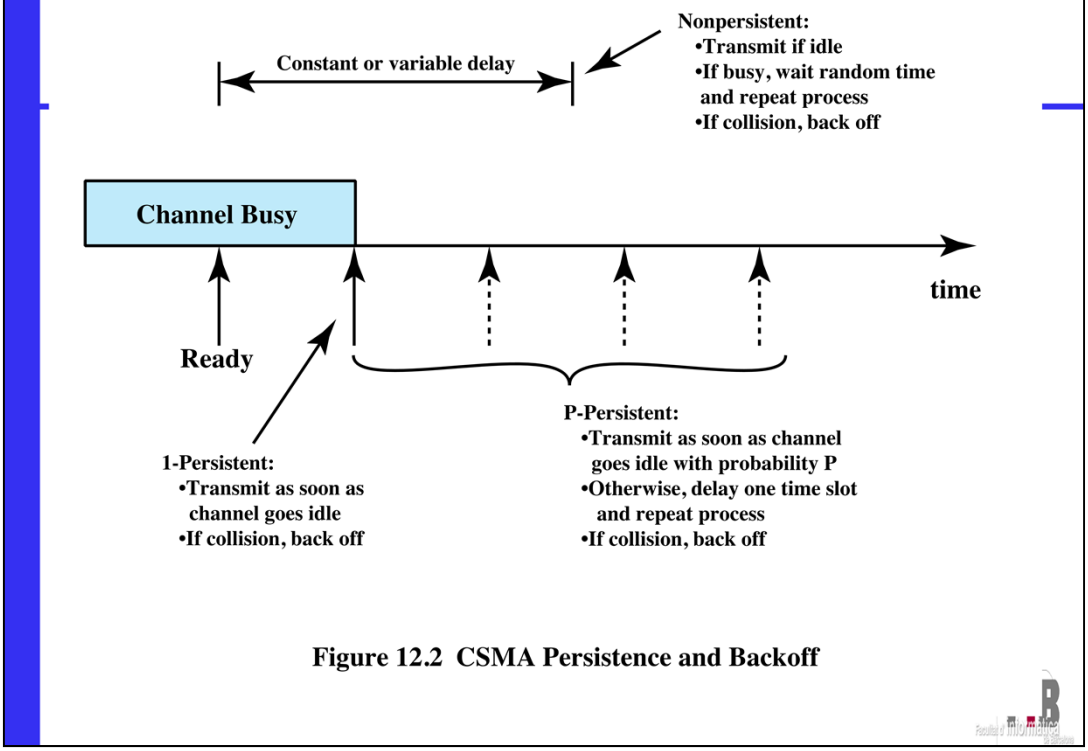


Figure 12.2 CSMA Persistence and Backoff

With CSMA, an algorithm is needed to specify what a station should do if the

medium is found busy. Three approaches are depicted in Figure 12.2.

P-Persistent CSMA

- A compromise to try and reduce collisions and idle time
- P-persistent CSMA rules:
  1. *If medium is idle, transmit with probability p, and delay one time unit with probability (1–p)*
  2. *If medium is busy, listen until idle and repeat step 1*
  3. *If transmission is delayed one time unit, repeat step 1*
- Issue of choosing effective value of *p* to avoid instability under heavy load

A compromise that attempts to reduce collisions, like nonpersistent, and reduce idle time, like 1-persistent, is ***p*-persistent**. The rules are:

1. If the medium is idle, transmit with probability *p*, and delay one time unit with probability (1 – *p*). The time unit is typically equal to the maximum propagation delay.

2. If the medium is busy, continue to listen until the channel is idle and repeat step 1.

3. If transmission is delayed one time unit, repeat step 1.

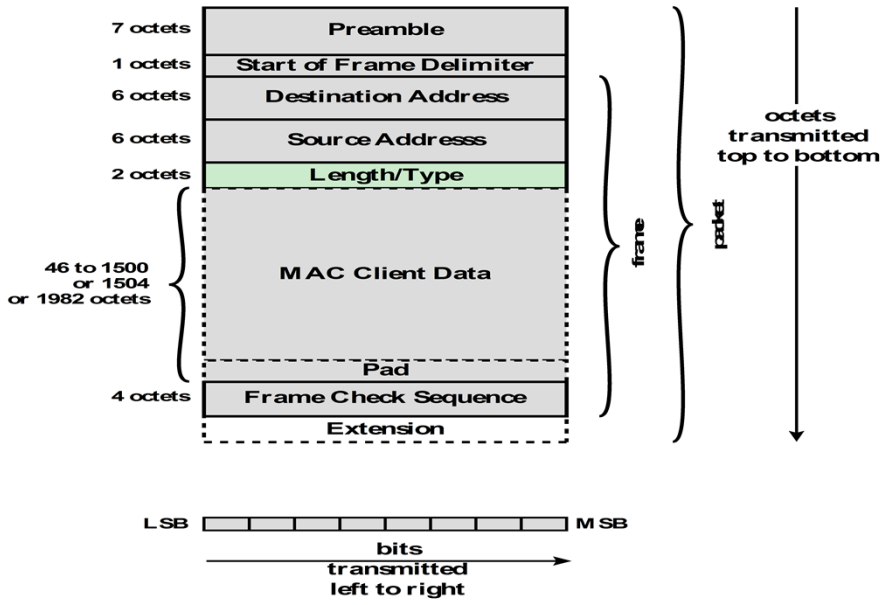


Figure 12.4 IEEE 802.3 MAC Frame Format

IEEE 802.3 defines three types of MAC frames. The basic frame is the original frame format. In addition, to support data link layer protocol encapsulation within the data portion of the frame, two additional frame types have been added. A Q-tagged frame supports 802.1Q VLAN capability, as described in Section 12.3. An envelope frame is intended to allow inclusion of additional prefixes and suffixes to the data field required by higher-layer encapsulation protocols such as those defined by the IEEE 802.1 working group (such as Provider Bridges and MAC Security), ITU-T, or IETF (such as MPLS).

Figure 12.4 depicts the frame format for all three types of frames; the differences are contained in the MAC Client Data field. Several additional fields encapsulate the frame to form an 802.3 packet. The fields are as follows:

• Preamble: A 7-octet pattern of alternating 0s and 1s used by the receiver to establish bit synchronization.

• Start Frame Delimiter (SFD): The sequence 10101011, which that delimits the actual start of the frame and enables the receiver to locate the first bit of the frame.

• Destination Address (DA): Specifies the station(s) for which the frame is intended. It may be a unique physical address, a multicast address, or a broadcast address.

• Source Address (SA): Specifies the station that sent the frame.

• Length/Type: Takes on one of two meanings, depending on its numeric value. If the value of this field is less than or equal to 1500 decimal, then the Length/ Type field indicates the number of MAC Client Data octets contained in the subsequent MAC Client Data field of the basic frame (length interpretation).

If the value of this field is greater than or equal to 1536 decimal then the Length/Type field indicates the nature of the MAC client protocol (Type interpretation). The Length and Type interpretations of this field are mutually exclusive.

• MAC Client Data: Data unit supplied by LLC. The maximum size of this field is 1500 octets for a basic frame, 1504 octets for a Q-tagged frame, and 1982 octets for an envelope frame.

• Pad: Octets added to ensure that the frame is long enough for proper CD operation.

• Frame Check Sequence (FCS): A 32-bit cyclic redundancy check, based on all fields except preamble, SFD, and FCS.

• Extension: This field is added, if required for 1-Gbps half-duplex operation. The extension field is necessary to enforce the minimum carrier event duration on the medium in half-duplex mode at an operating speed of 1 Gbps.

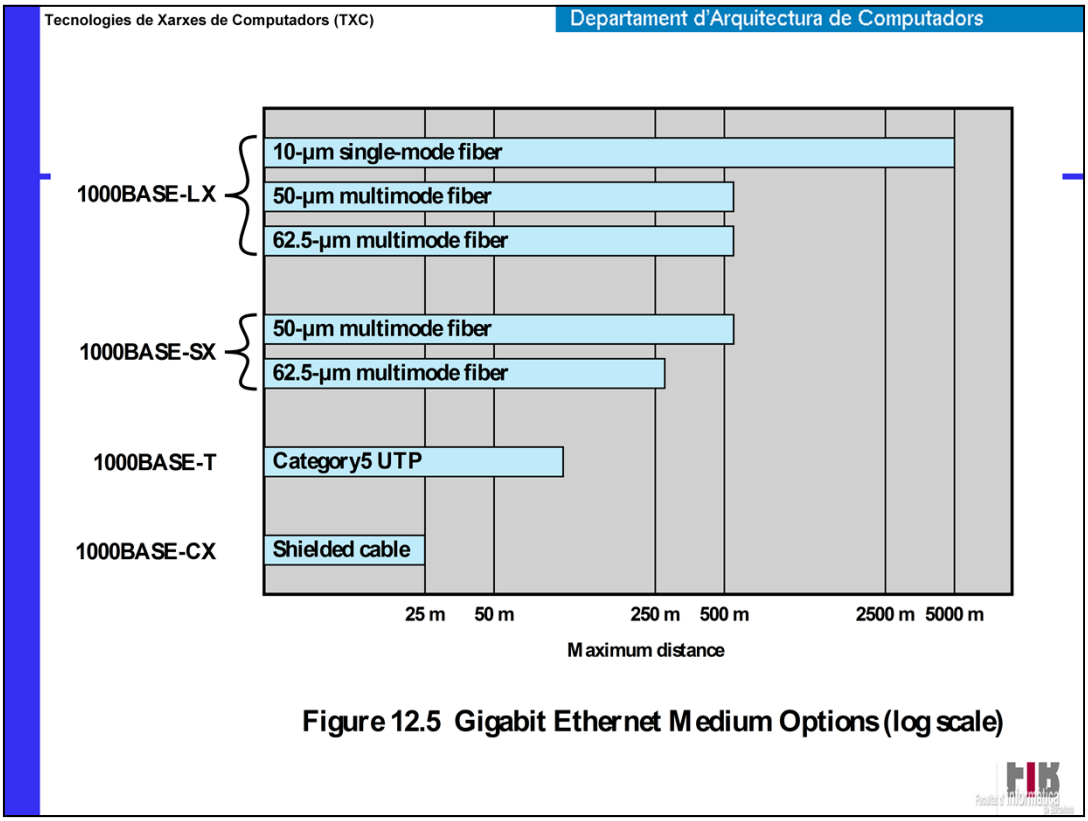


Figure 12.5 Gigabit Ethernet Medium Options (log scale)

The current 1-Gbps specification for IEEE 802.3 includes the following physical layer alternatives (Figure 12.5):

1000BASE-SX: This short-wavelength option supports duplex links of up to 275 m using 62.5-µm multimode or up to 550 m using 50-µm multimode fiber. Wavelengths are in the range of 770 to 860 nm.

1000BASE-LX: This long-wavelength option supports duplex links of up to 550 m of 62.5-µm or 50-µm multimode fiber or 5 km of 10-µm single-mode fiber. Wavelengths are in the range of 1270 to 1355 nm.

1000BASE-CX: This option supports 1-Gbps links among devices located within a single room or equipment rack, using copper jumpers (specialized shielded twisted-pair cable that spans no more than 25 m). Each link is composed of a separate shielded twisted pair running in each direction.

1000BASE-T: This option makes use of four pairs of Category 5 unshielded twisted pair to support devices over a range of up to 100 m, transmitting and receiving on all four pairs at the same time, with echo cancelation circuitry.

The signal encoding scheme used for the first three Gigabit Ethernet options just

listed is 8B/10B, which is described in Appendix 12A. The signal-encoding scheme used for 1000BASE-T is 4D-PAM5, a complex scheme whose description is beyond our scope.

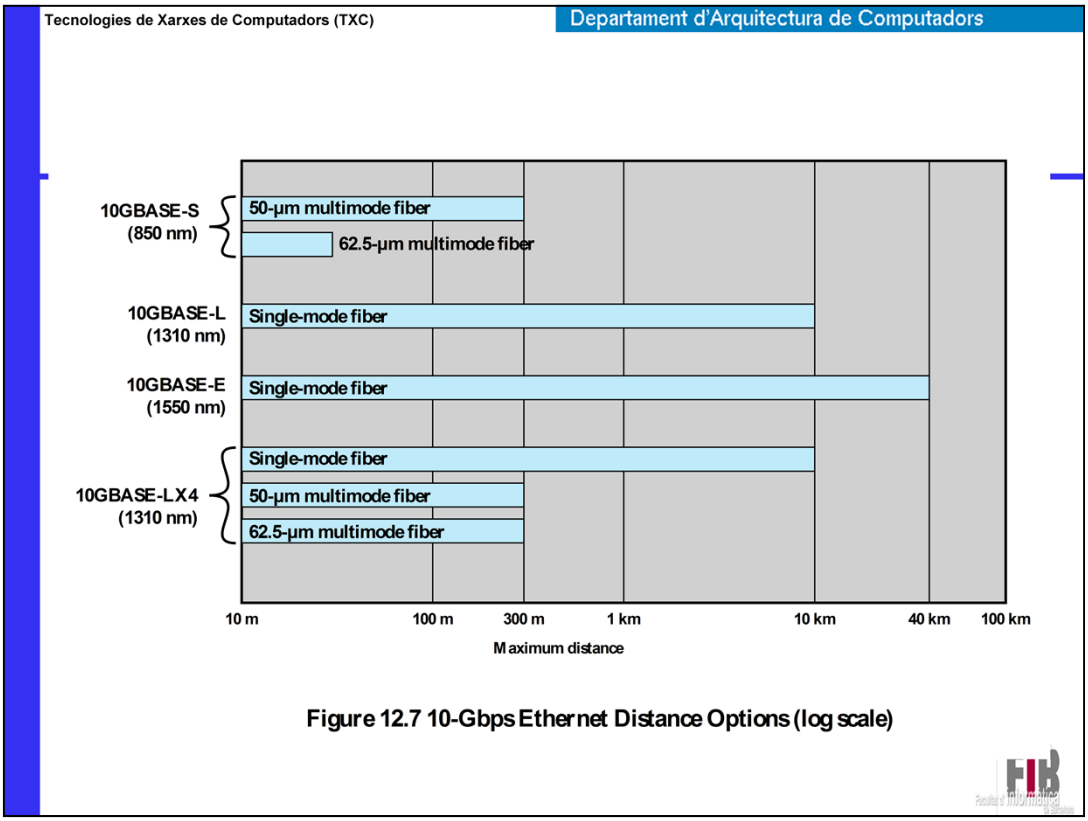


Figure 12.7 10-Gbps Ethernet Distance Options (log scale)

Four physical layer options are defined for 10-Gbps Ethernet (Figure 12.7). The first three of these have two suboptions: an "R" suboption and a "W" suboption. The R designation refers to a family of physical layer implementations that use a signal encoding technique known as 64B/66B, described in Appendix 12A. The R implementations are designed for use over *dark fiber*, meaning a fiber optic cable that is not in use and that is not connected to any other equipment. The W designation refers to a family of physical layer implementations that also use 64B/66B signaling but that are then encapsulated to connect to SONET equipment.

The four physical layer options are

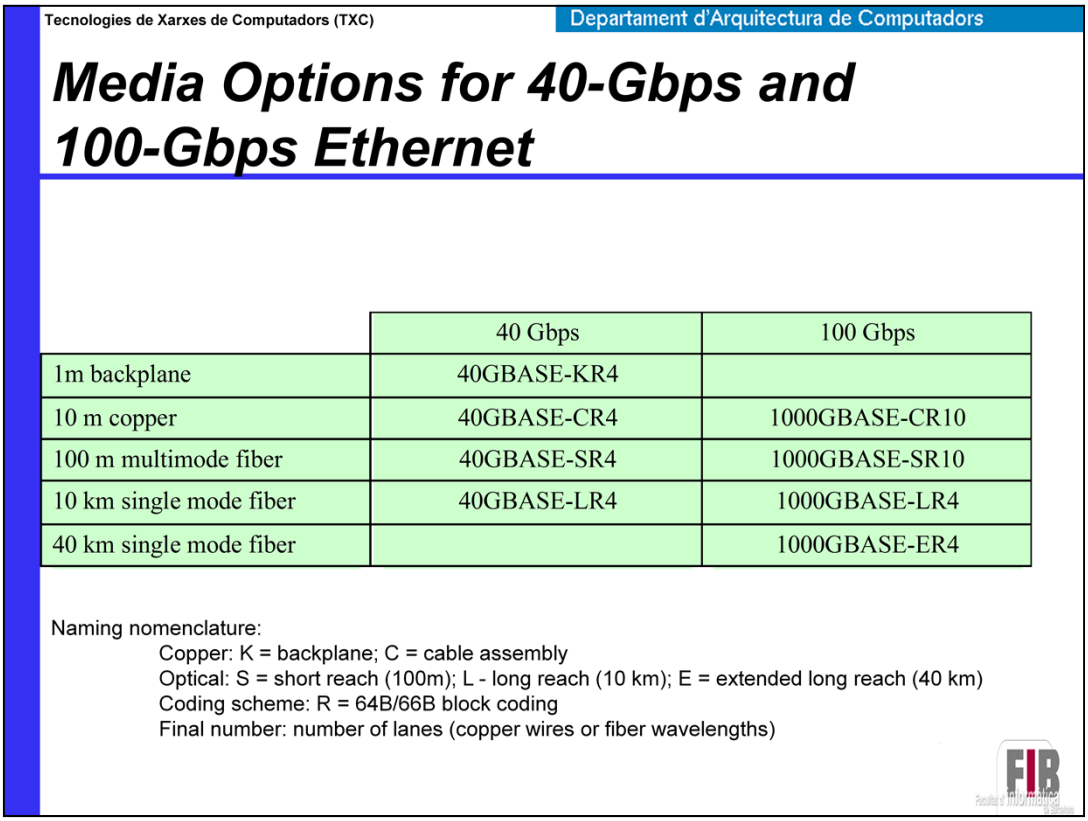
10GBASE-S (short): Designed for 850-nm transmission on multimode fiber. This medium can achieve distances up to 300 m. There are 10GBASE-SR and 10GBASE-SW versions.

10GBASE-L (long): Designed for 1310-nm transmission on single-mode fiber. This medium can achieve distances up to 10 km. There are 10GBASE-LR and 10GBASE-LW versions.

10GBASE-E (extended): Designed for 1550-nm transmission on single-mode fiber. This medium can achieve distances up to 40 km. There are 10GBASE-ER

and 10GBASE-EW versions.

10GBASE-LX4: Designed for 1310-nm transmission on single-mode or multimode fiber. This medium can achieve distances up to 10 km. This medium uses wavelength-division multiplexing (WDM) to multiplex the bit stream across four light waves.



IEEE 802.3ba specifies three types of transmission media (Table 12.3): copper backplane, twisted pair, and optical fiber. For copper media, four separate physical lanes are specified. For optical fiber, either 4 or 10 wavelength lanes are specified, depending on data rate and distance.

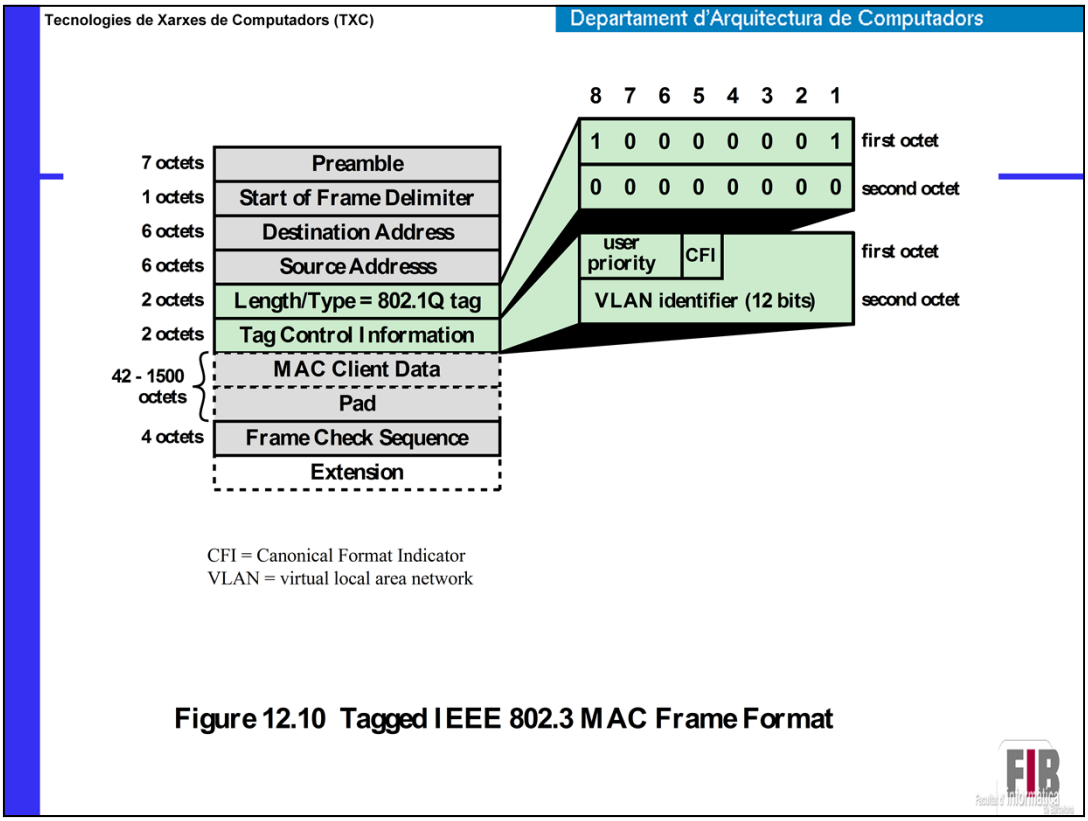


Figure 12.10 Tagged IEEE 802.3 MAC Frame Format

The IEEE 802.1Q standard, last updated in 2005, defines the operation of VLAN bridges and switches that permits the definition, operation and administration of VLAN topologies within a bridged/switched LAN infrastructure. In this section, we will concentrate on the application of this standard to 802.3 LANs.

Recall from Chapter 11 that a VLAN is an administratively configured broadcast domain, consisting of a subset of end stations attached to a LAN. A VLAN is not limited to one switch but can span multiple interconnected switches. In that case traffic between switches must indicate VLAN membership. This is accomplished in 802.1Q by inserting a tag with a VLAN identifier (VID) with a value in the range from 1 to 4094. Each VLAN in a LAN configuration is assigned a globally unique VID. By assigning the same VID to end systems on many switches, one or more VLAN broadcast domains can be extended across a large network.

Figure 12.10 shows the position and content of the 802.1 tag, referred to as Tag Control Information (TCI). The presence of the 2-octet TCI field is indicated by set the Length/Type field in the 802.3 MAC from to a value of 8100 hex. The TCI consists of three subfields:

User priority (3 bits): The priority level for this frame.

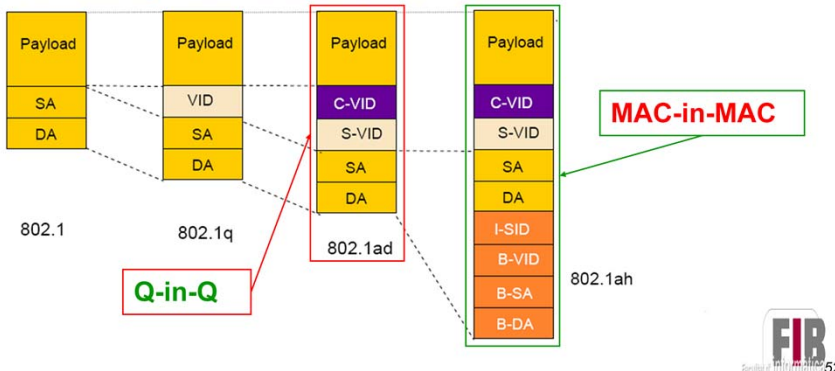
Canonical format indicator (1 bit): s always set to zero for Ethernet switches. CFI is used for compatibility reason between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.

VLAN identifier (12 bits): the identification of the VLAN. Of the 4096 possible VIDs, a VID of 0 is used to identify that the TCI contains only a priority value, and 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4094.

Departament d'Arquitectura de Computadors

The way to PBB-TE/PBT

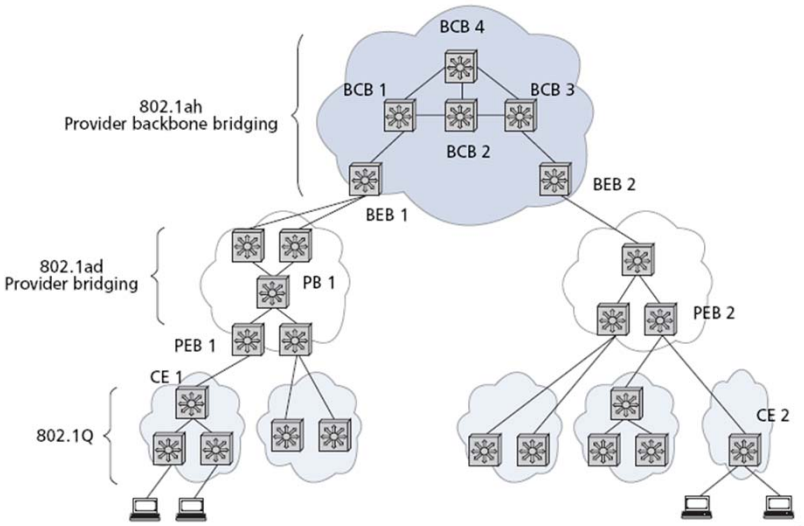
- **IEEE has developed a number of standards providing enhancements to the original Ethernet standards**
  - **802.1Q**: Virtual LAN
  - **802.1ad**: Provider Bridging
  - **802.1ah**: Provider Backbone Bridging
  - **802.1ag**: Connectivity Fault Management (OAM)



52

Departament d'Arquitectura de Computadors

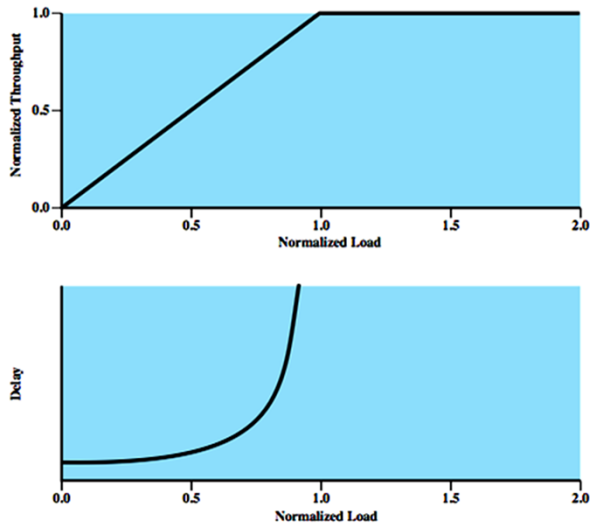
The way to PBB-TE/PBT



53


Departament d'Arquitectura de Computadors
Facultat d' Informàtica de Barcelona
2.5 Control de la congestió
54

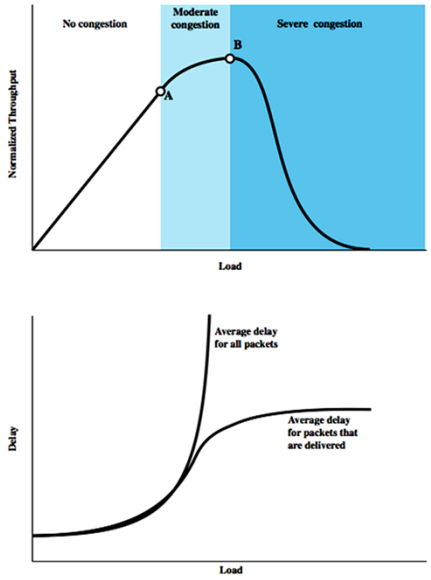
Ideal Network Utilization



Stallings DCC9e Figure 13.3 suggests the ideal goal for network utilization. The top graph plots the steady-state total throughput (number of packets delivered to destination end systems) through the network as a function of the offered load (number of packets transmitted by source end systems), both normalized to the maximum theoretical throughput of the network. For example, if a network consists of a single node with two full-duplex 1-Mbps links, then the theoretical capacity of the network is 2 Mbps, consisting of a 1-Mbps flow in each direction. In the ideal case, the throughput of the network increases to accommodate load up to an offered load equal to the full capacity of the network; then normalized throughput remains at 1.0 at higher input loads. Note, however, what happens to the end-to-end delay experienced by the average packet even with this assumption of ideal performance. At negligible load, there is some small constant amount of delay that consists of the propagation delay through the network from source to destination plus processing delay at each node. As the load on the network increases, queuing delays at each node are added to this fixed amount of delay. When the load exceeds the network capacity, delays increase without bound.

It is important to grasp the meaning of Stallings DCC9e Figure 13.3 before looking at real-world conditions. This figure represents the ideal, but unattainable, goal of all traffic and congestion control schemes. No scheme can exceed the performance depicted in Stallings DCC9e Figure 13.3.

Effects of Congestion - No Control



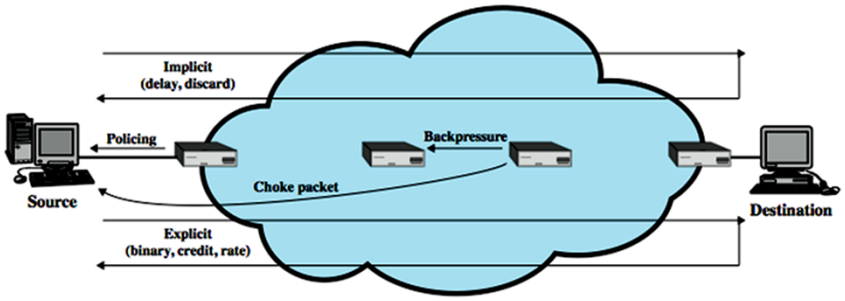
The ideal case reflected in Stallings DCC9e Figure 13.3 assumes infinite buffers and no overhead related to congestion control. In practice, buffers are finite, leading to buffer overflow, and attempts to control congestion consume network capacity in the exchange of control signals.

Let us consider what happens in a network with finite buffers if no attempt is made to control congestion or to restrain input from end systems. The details will, of course, differ depending on network configuration and on the statistics of the presented traffic. However, the graphs in Stallings DCC9e Figure 13.4 depict the devastating outcome in general terms.

At light loads, throughput and hence network utilization increases as the offered load increases. As the load continues to increase, a point is reached (point A in the plot) beyond which the throughput of the network increases at a rate slower than the rate at which offered load is increased. This is due to network entry into a moderate congestion state. In this region, the network continues to cope with the load, although with increased delays. The departure of throughput from the ideal is accounted for by a number of factors. For one thing, the load is unlikely to be spread uniformly throughout the network. Therefore, while some nodes may experience moderate congestion, others may be experiencing severe congestion and may need to discard traffic. In addition, as the load increases, the network will attempt to balance the load by routing packets through areas of lower congestion. For the routing function to work, an increased number of routing messages must be exchanged between nodes to alert each other to areas of congestion; this overhead reduces the capacity available for data packets.

As the load on the network continues to increase, the queue lengths of the various nodes continue to grow. Eventually, a point is reached (point B in the plot) beyond which throughput actually drops with increased offered load. The reason for this is that the buffers at each node are of finite size. When the buffers at a node become full, the node must discard packets. Thus, the sources must retransmit the discarded packets in addition to new packets. This only exacerbates the situation: As more and more packets are retransmitted, the load on the system grows, and more buffers become saturated. While the system is trying desperately to clear the backlog, users are pumping old and new packets into the system. Even successfully delivered packets may be retransmitted because it takes too long, at a higher layer (e.g., transport layer), to acknowledge them: The sender assumes the packet did not get through and retransmits. Under these circumstances, the effective capacity of the system declines to zero.

Mechanisms for Congestion Control



In this book, we discuss various techniques for controlling congestion in packet-switching, frame relay, and ATM networks, and in IP-based internets. To give context to this discussion, Stallings DCC9e Figure 13.5 provides a general depiction of important congestion control techniques, which include:

•backpressure

•choke packets

•implicit congestion signaling

•explicit congestion signaling

Token bucket

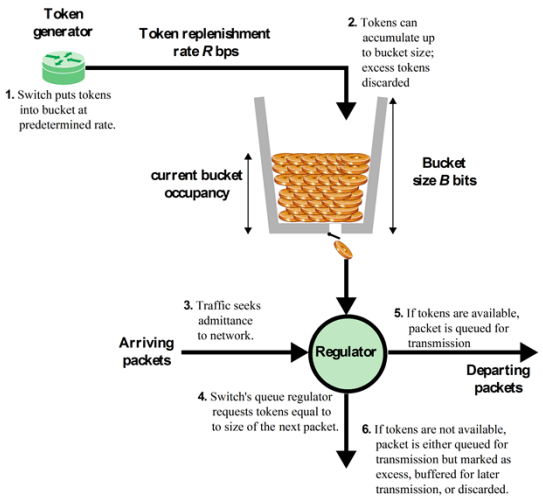


Figure 20.6 Token Bucket Scheme

A token bucket traffic specification consists of two parameters: a token replenishment rate R and a bucket size B. The token rate R specifies the continually sustainable data rate; that is, over a relatively long period of time, the average data rate to be supported for this flow is R. The bucket size B specifies the amount by which the data rate can exceed R for short periods of time. The exact condition is as follows: during any time period T, the amount of data sent cannot exceed $RT + B$.

Figure 20.6 illustrates this scheme and explains the use of the term *bucket*. The bucket represents a counter that indicates the allowable number of bytes of data that can be sent at any time. The bucket fills with byte tokens at the rate of R (i.e., the counter is incremented R times per second), up to the bucket capacity (up

to the maximum counter value). Data arrive from the user and are assembled into packets, which are queued for transmission. A packet may be transmitted if there are sufficient tokens to match the packet size. If so, the packet is transmitted and the bucket is drained of the corresponding number of tokens. If there are insufficient
tokens available, then the packet exceeds the specification for this flow. The treatment for such packets is a design or implementation decision. Possible actions including:

• Queue the packet for transmission until sufficient tokens are available and then transmit.

• Queue the packet for transmission until sufficient tokens are available but label the packet as exceeding a threshold.

• Discard the packet.

The last option is generally not used with token bucket. Token bucket is typically used for traffic shaping but not traffic policing.

The result of this scheme is that if there is a backlog of packets and an empty bucket, then packets are emitted at a smooth flow of packets per second with no packet delay variation until the backlog is cleared. Thus, the token bucket smooths out bursts of cells. Over the long run, the rate of data allowed by the token bucket is R . However, if there is an idle or relatively slow period, the bucket capacity builds up, so that at most an additional B bytes above the stated rate can be accepted. Thus, B is a measure of the degree of burstiness of the data flow that is allowed.

Leacky bucket

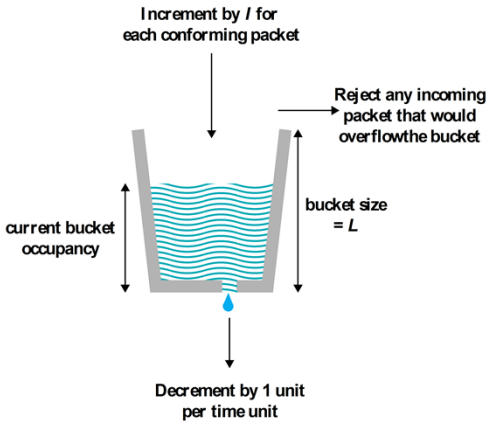


Figure 20.7 Leaky Bucket Algorithm

Another scheme, similar to token bucket, is leaky bucket. Leaky bucket is used in the asynchronous transfer mode (ATM) specification and in the ITU-T H.261 standard for digital video coding and transmission. The basic principle of leaky bucket is depicted in Figure 20.7. The algorithm maintains a running count of the cumulative amount of data sent in a counter X . The counter is decremented at a constant rate of one unit per time unit to a minimum value of zero; this is equivalent to a bucket that leaks at a rate of 1. The counter is incremented by I for each arriving packet, where I is the size of the packet, subject to the restriction that the maximum counter value is L . Any arriving cell that would cause the counter to exceed its maximum is defined as nonconforming; this is equivalent to a bucket with a capacity of L .

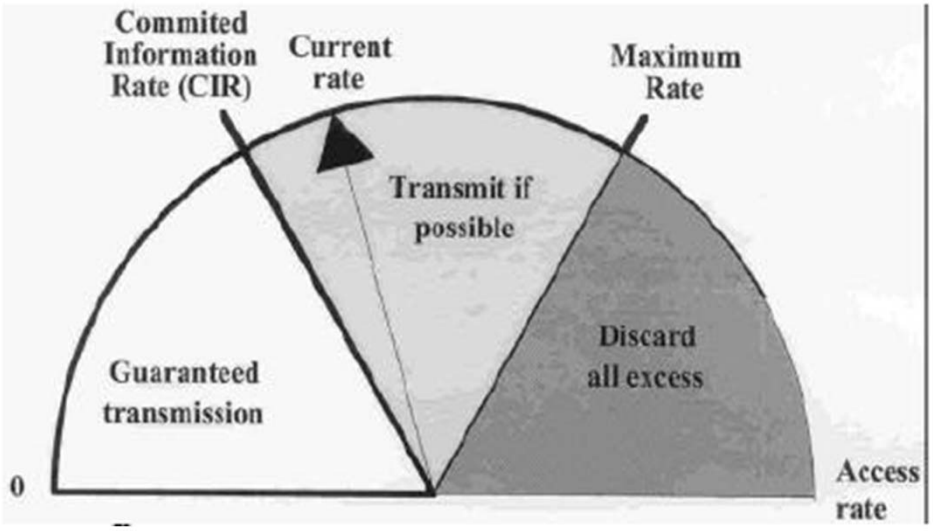
The token bucket and leaky bucket schemes operate in a similar fashion, but there are some differences. A token bucket fills at a constant rate up to the capacity of the bucket and empties at a rate dictated by the input data stream while the bucket is not empty. A leaky bucket empties at a constant rate while the bucket is not empty and fills at a rate dictated by the input stream up to the capacity of the bucket. Thus, for token bucket, as the rate of incoming packets rise, the output of the system speeds up. In effect, token bucket gives credit to a flow or connection that is underused, up to a point.

Example: FR congestion control

Technique	Type	Function	Key Elements
Discard control	Discard strategy	Provides guidance to network concerning which frames to discard	DE bit
Backward explicit Congestion Notification	Congestion avoidance	Provides guidance to end systems about congestion in network	BECN bit or CLLM message
Forward explicit Congestion Notification	Congestion avoidance	Provides guidance to end systems about congestion in network	FECN bit
Implicit congestion notification	Congestion recovery	End system infers congestion from frame loss	Sequence numbers in higher-layer PDU

Departament d'Arquitectura de Computadors

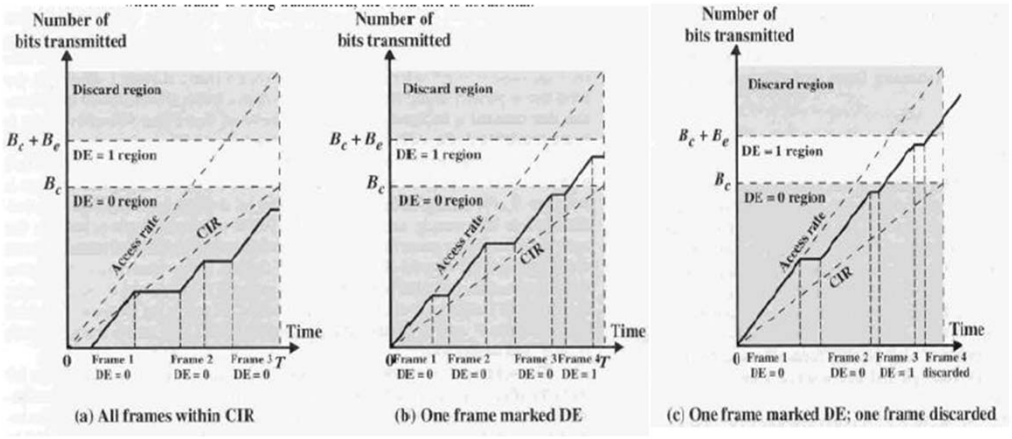
Discard Control



61

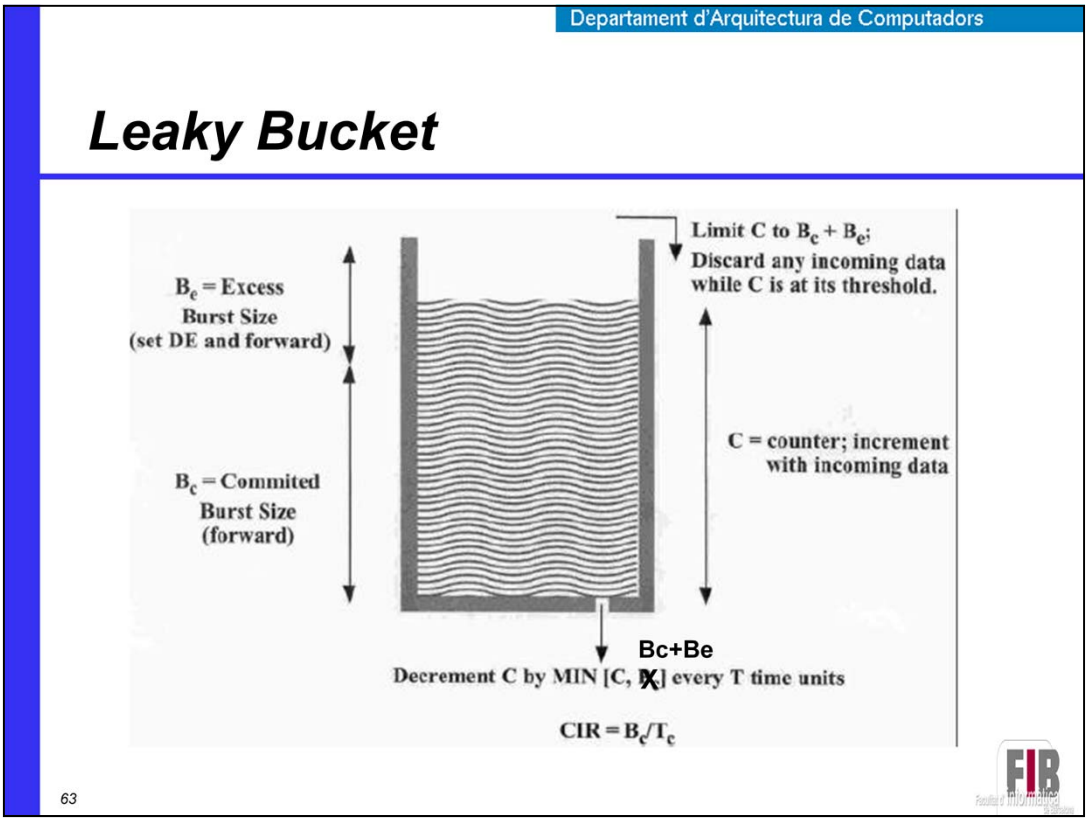
Departament d'Arquitectura de Computadors

Congestion control



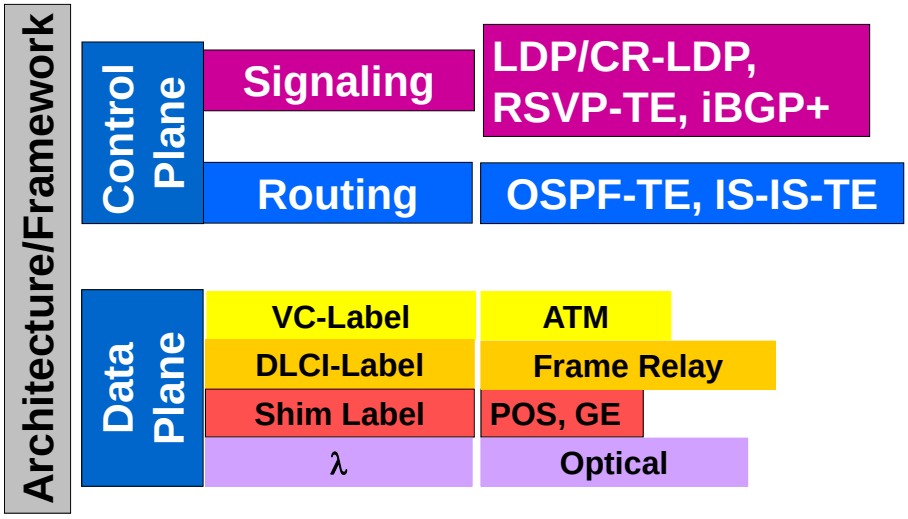
(a) All frames within CIR (b) One frame marked DE (c) One frame marked DE; one frame discarded

62

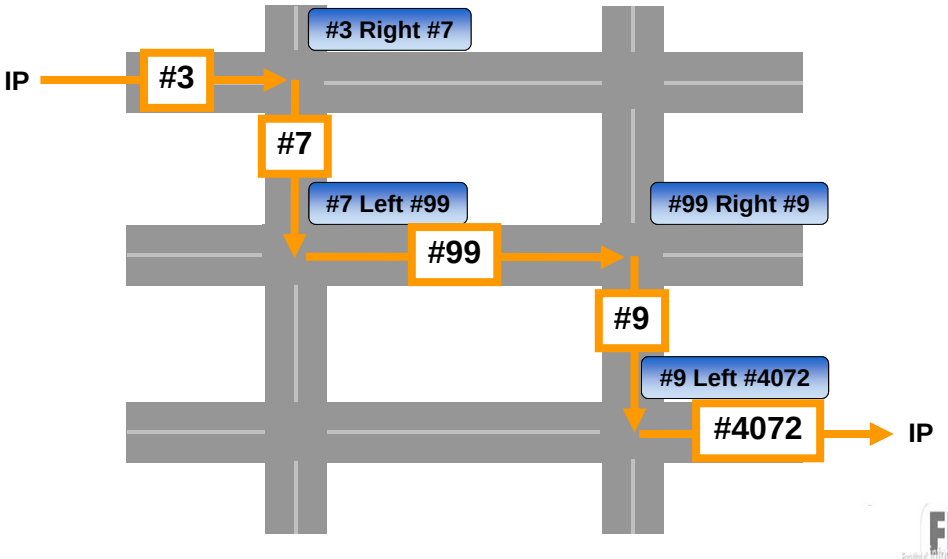


Decrement C by MIN[C,**Bc+Be**]

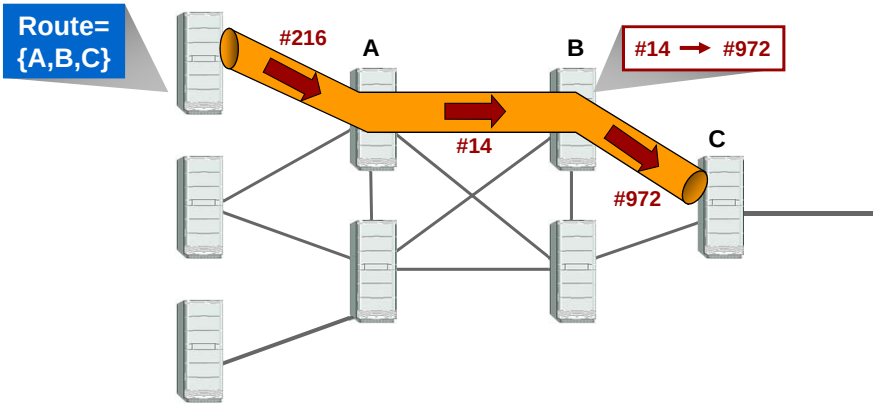
What is Standard MPLS?



Label Switched Path

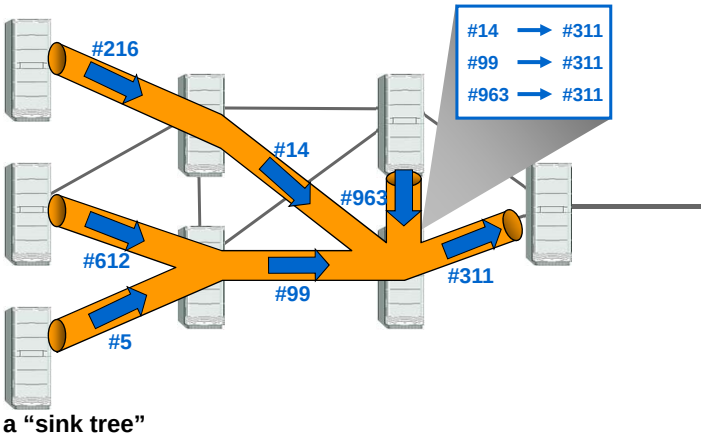


Point-to-point LSP



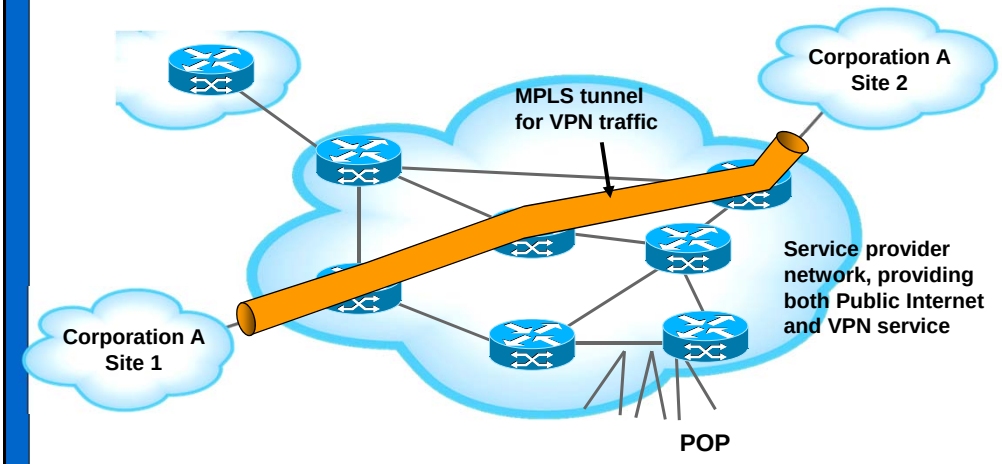
- LSP follows route that source chooses. In other words, the control message to establish the LSP (label request) is *source routed*.

Merging LSP

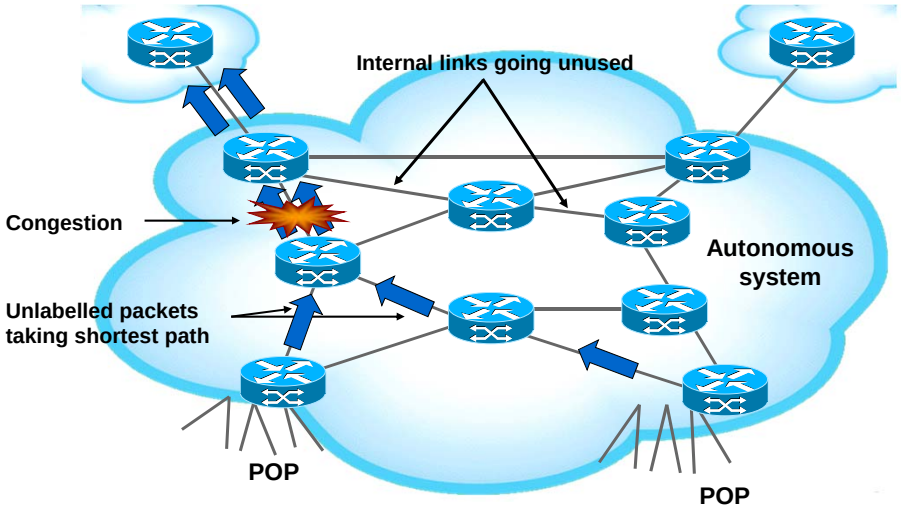


- LSP forms a "sink tree"
- The branches of the LSP always follows the same route as normal IP forwarding; that is, the *shortest path*

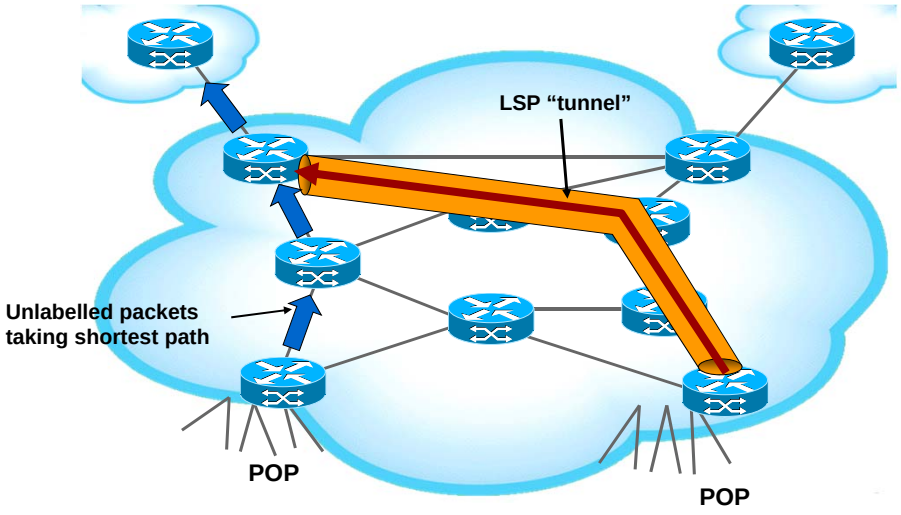
Network-Based Virtual Private Networks using MPLS



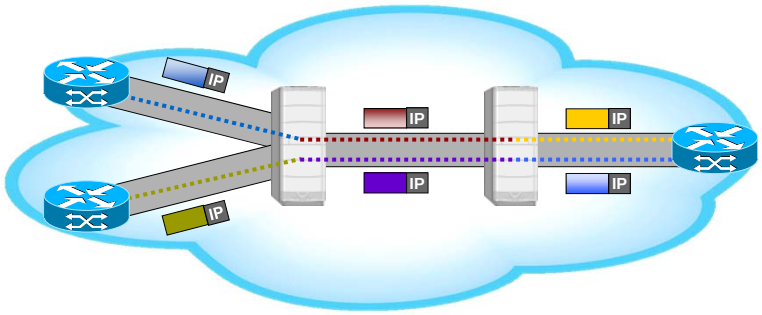
IP Traffic Engineering. Problem Definition



Traffic Engineering using MPLS

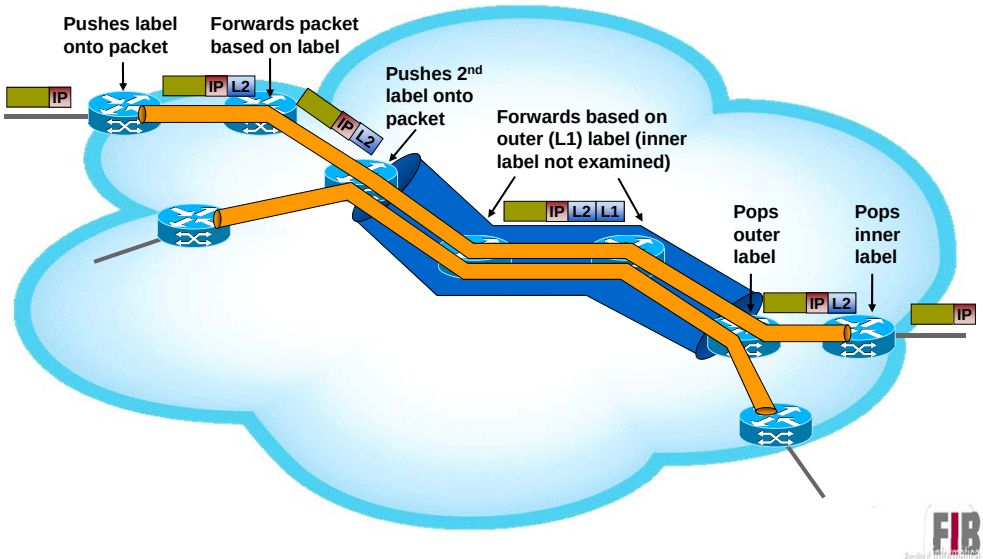


Optical

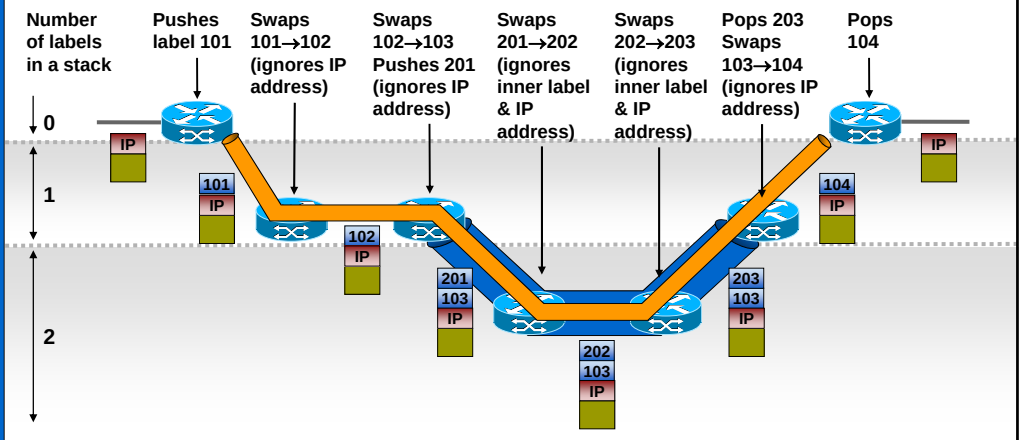


- Label not prepended to packet
- Instead is represented by a fiber number or a wavelength

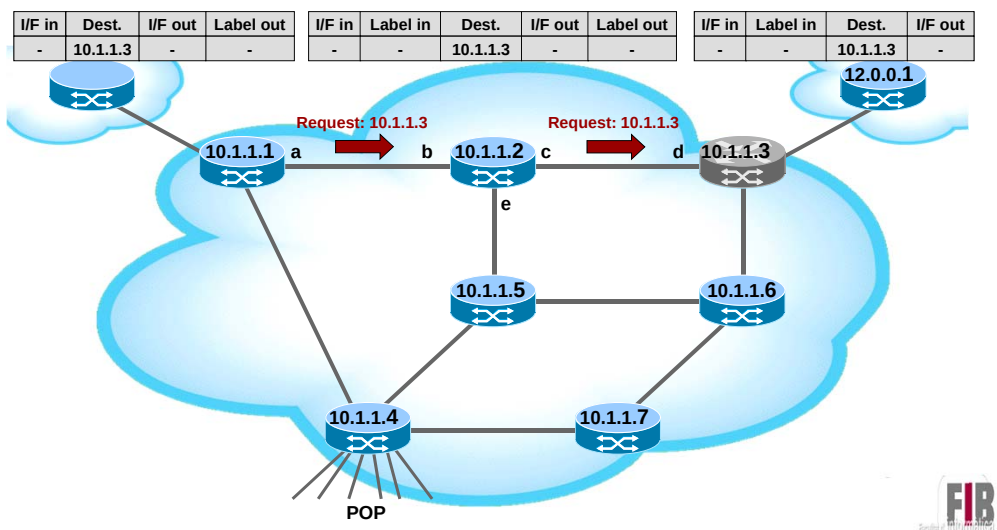
Label Stacking Example



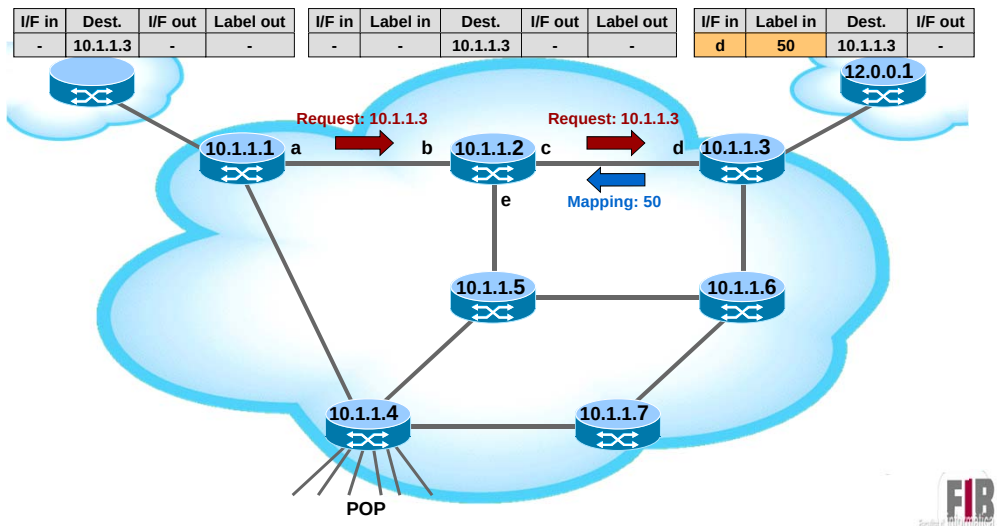
Label Stacking Details



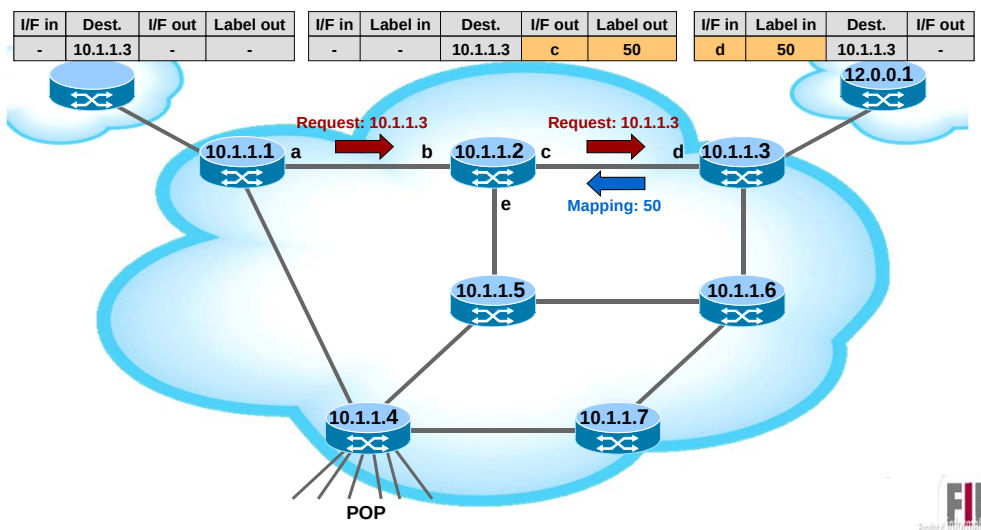
Example establishment LSP with LDP



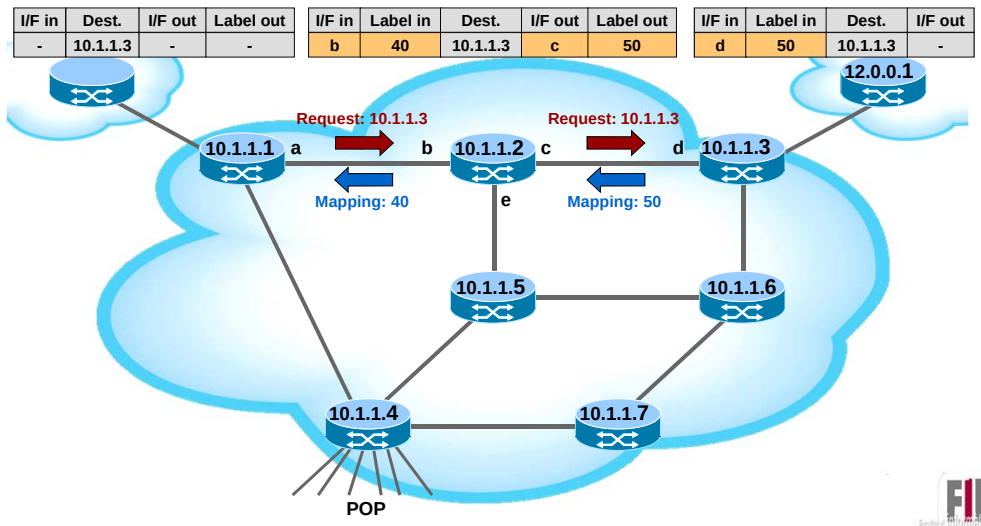
Example establishment LSP with LDP



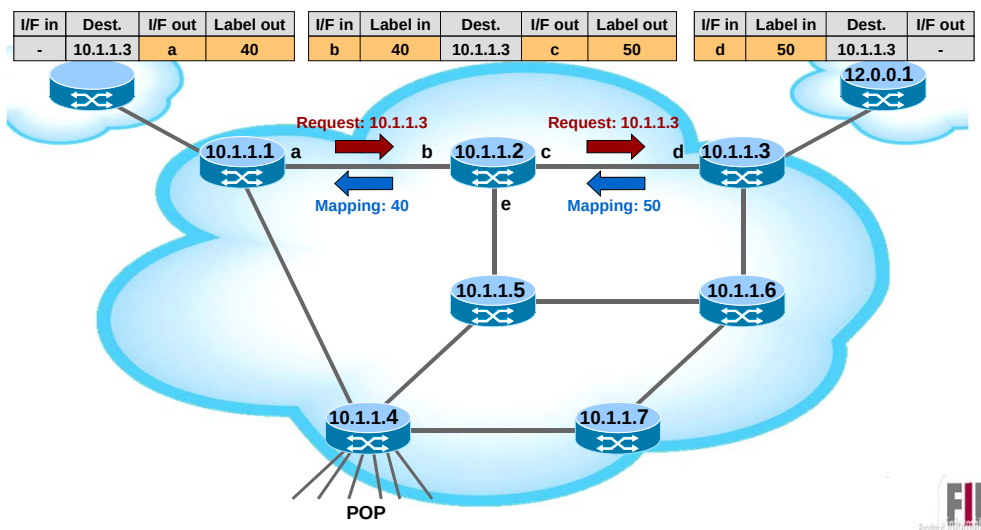
Example establishment LSP with LDP



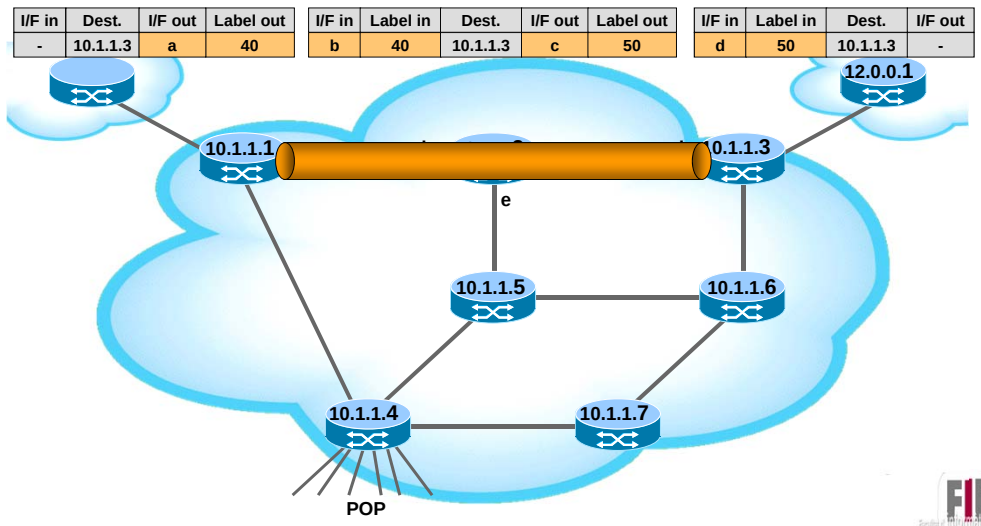
Example establishment LSP with LDP



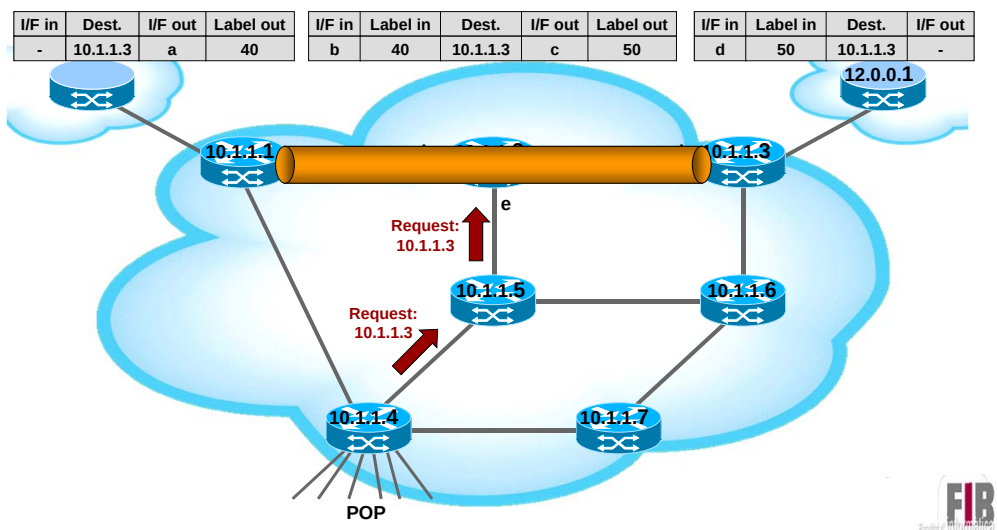
Example establishment LSP with LDP



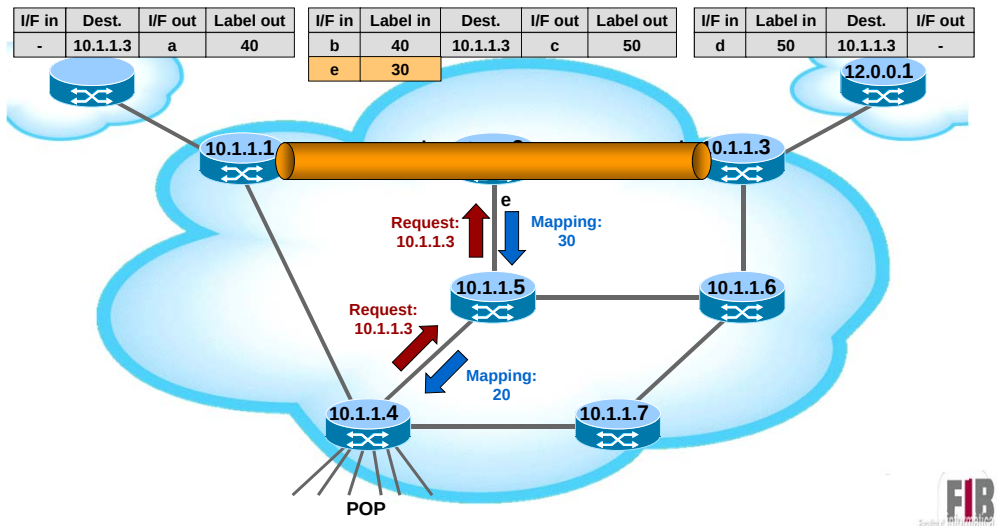
Example establishment LSP with LDP



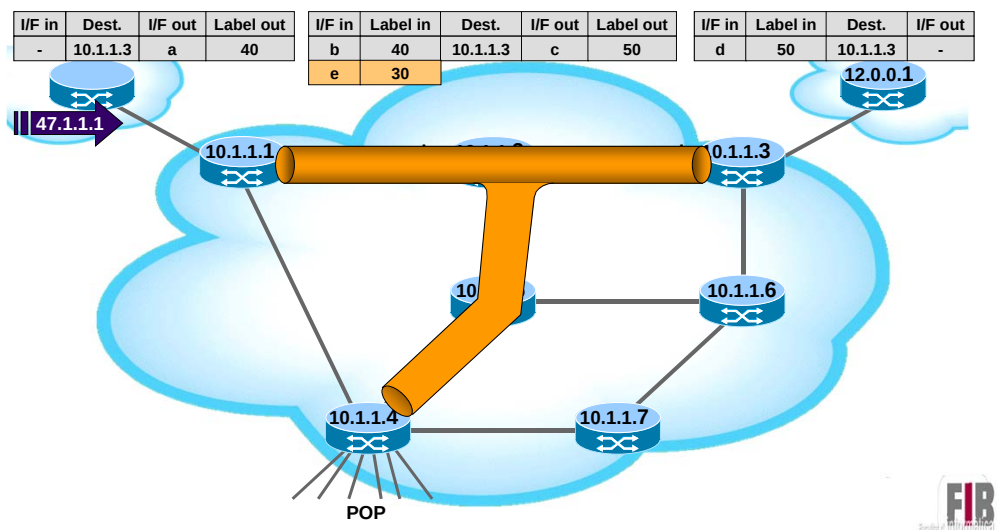
Example establishment LSP with LDP



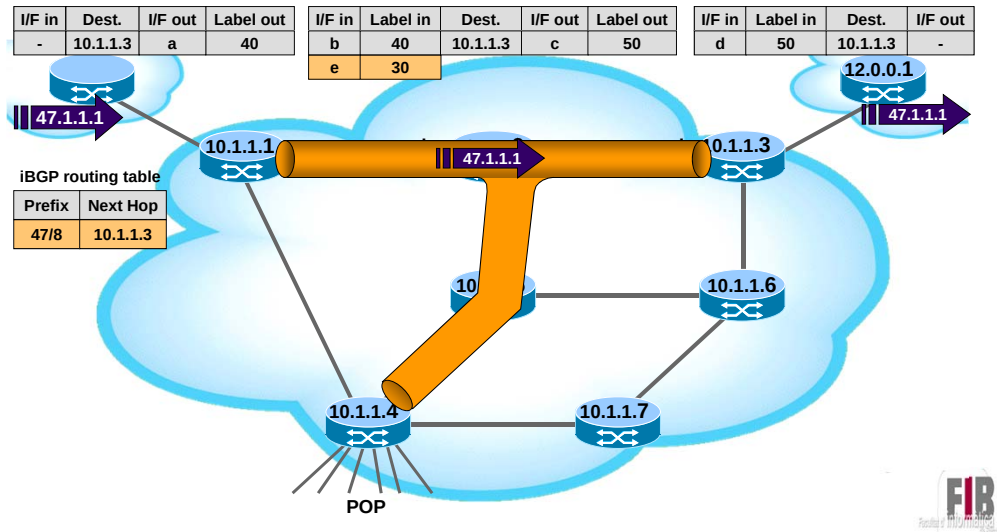
Example establishment LSP with LDP



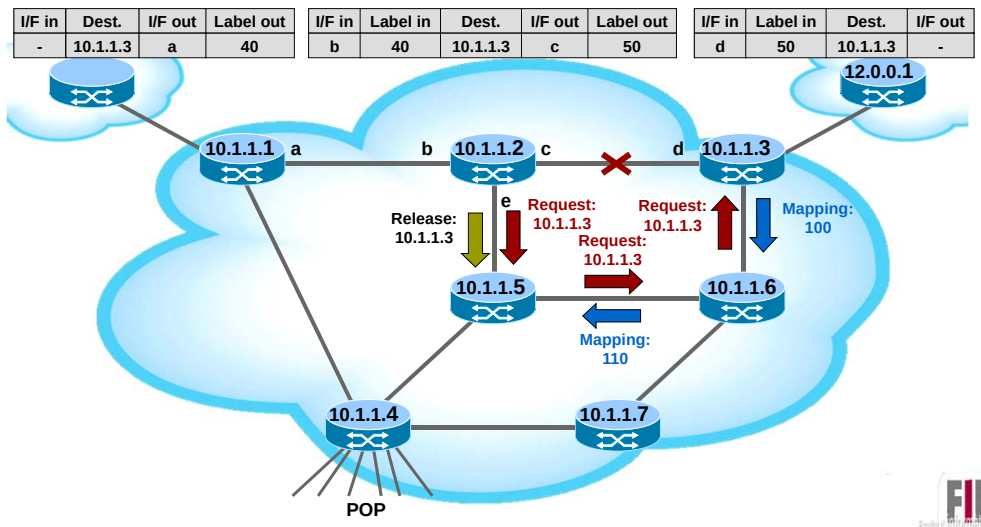
Example establishment LSP with LDP



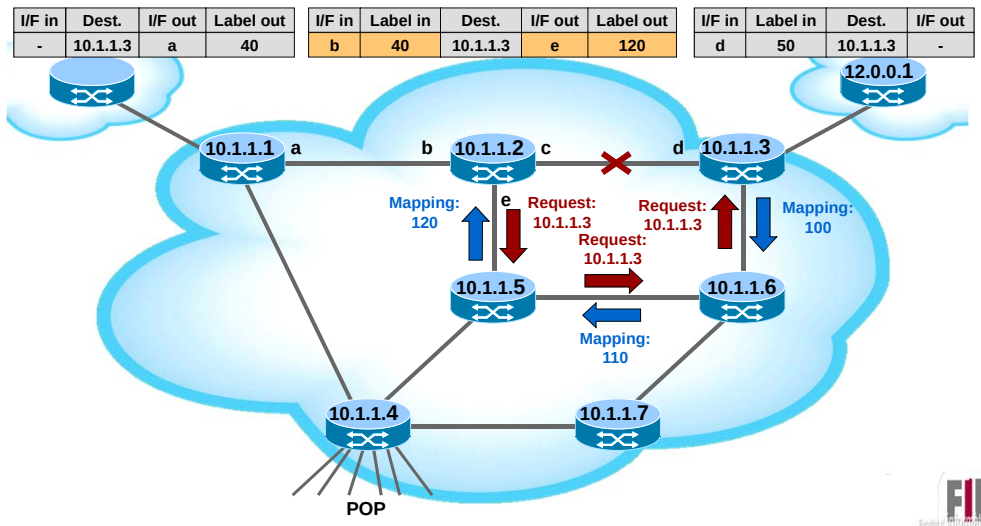
IP travel over LSP



LSP recovery in case of failure



LSP recovery in case of failure

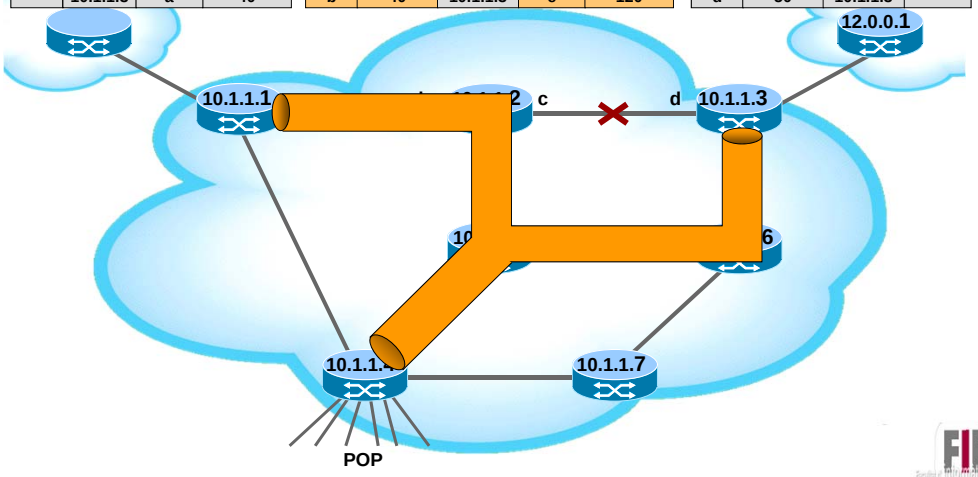


LSP recovery in case of failure

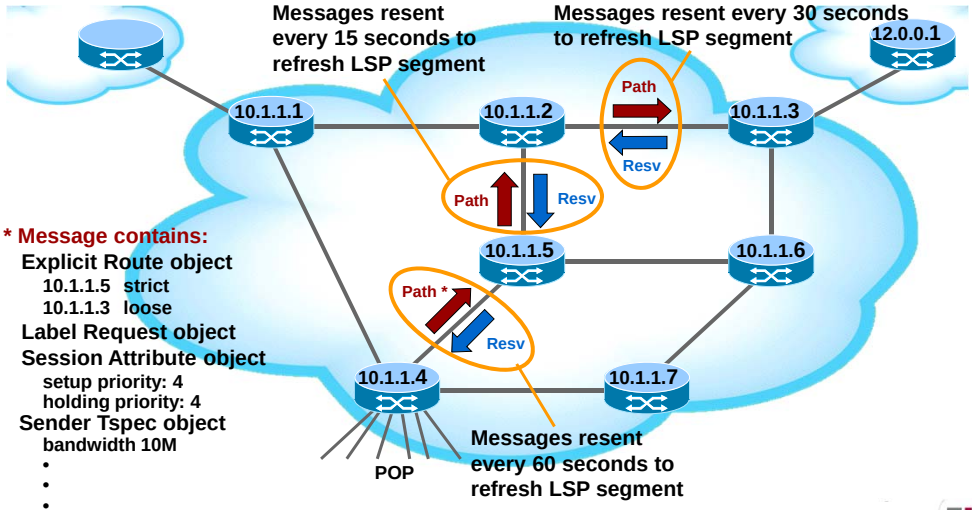
I/F in	Dest.	I/F out	Label out
-	10.1.1.3	a	40

I/F in	Label in	Dest.	I/F out	Label out
b	40	10.1.1.3	e	120

I/F in	Label in	Dest.	I/F out
d	50	10.1.1.3	-

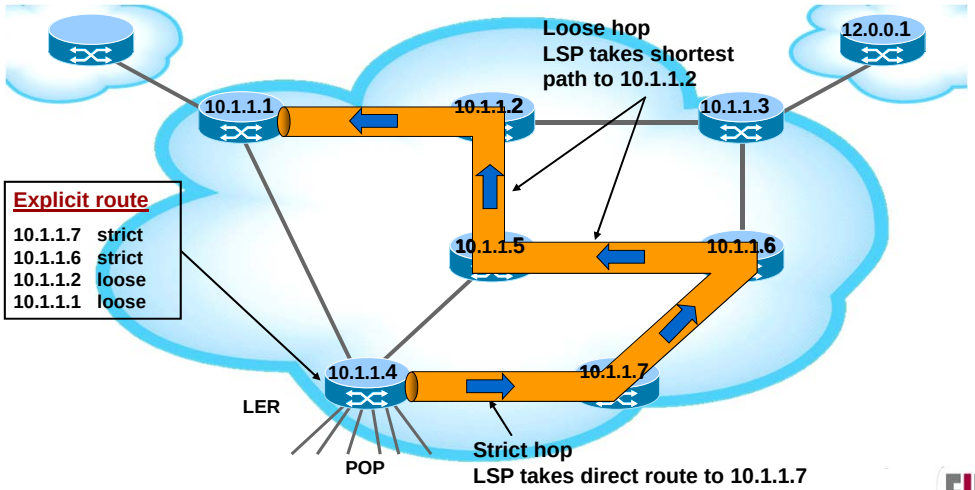


RSVP-TE details: Example

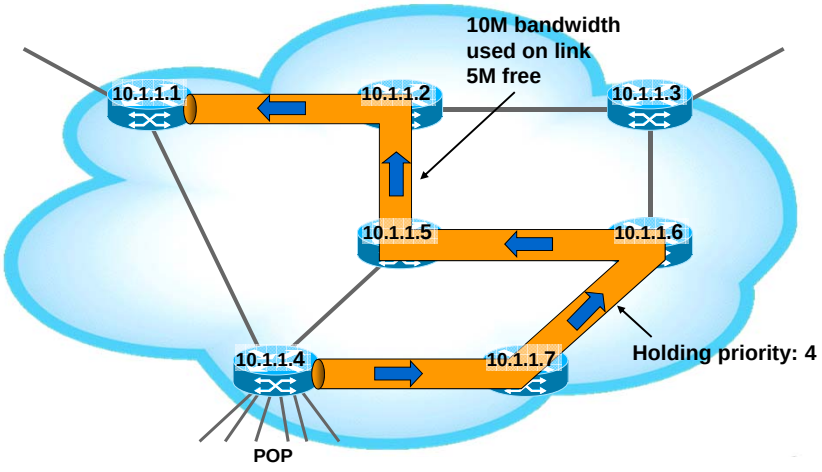


* Message contains:
- Explicit Route object
  - 10.1.1.5 strict
  - 10.1.1.3 loose
- Label Request object
- Session Attribute object
  - setup priority: 4
  - holding priority: 4
- Sender Tspec object
  - bandwidth 10M
- •
- •
- •

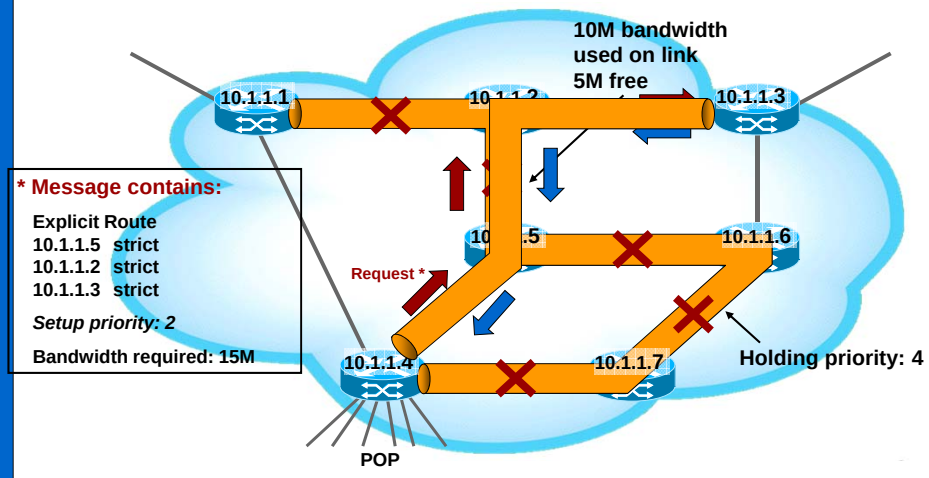
MPLS-TE Explicit Routing.



MPLS-TE: LSP preemption



MPLS-TE: LSP preemption



*** Message contains:**

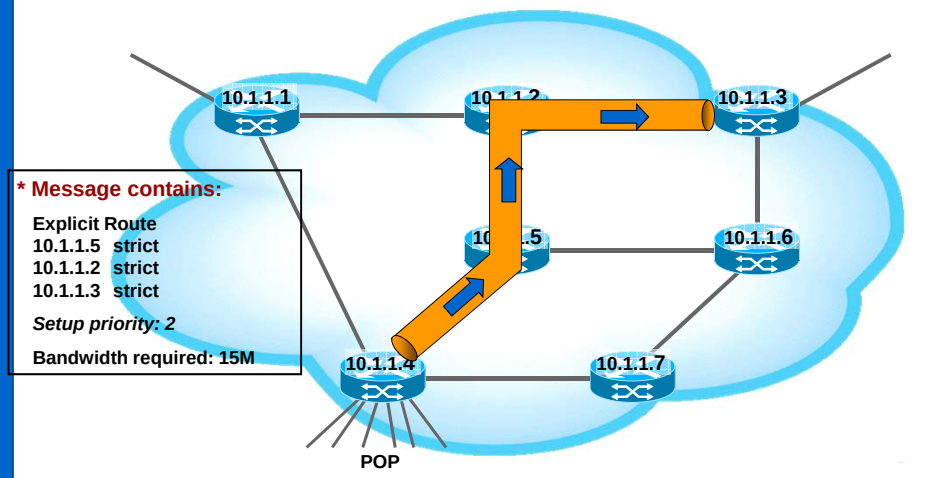
Explicit Route
10.1.1.5 strict
10.1.1.2 strict
10.1.1.3 strict

Setup priority: 2

Bandwidth required: 15M

Departament d'Arquitectura de Computadors

MPLS-TE: LSP preemption



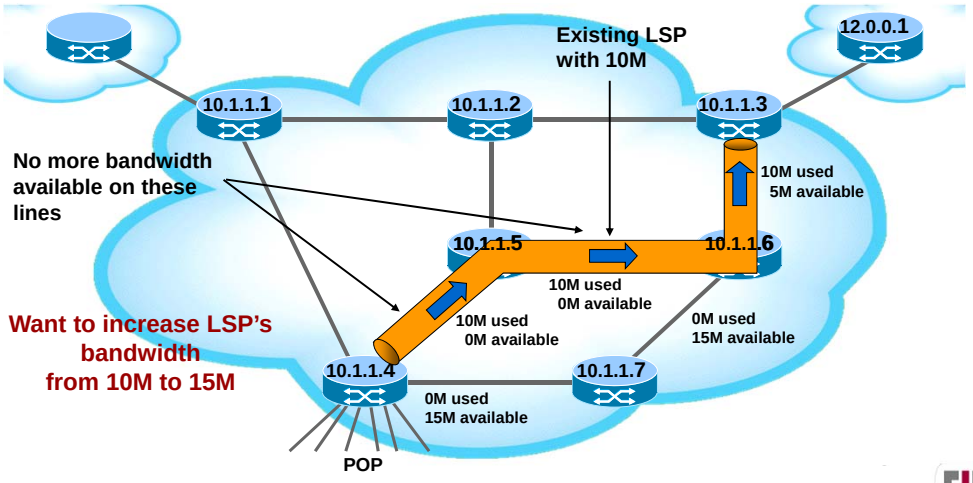
*** Message contains:**

Explicit Route
10.1.1.5 strict
10.1.1.2 strict
10.1.1.3 strict

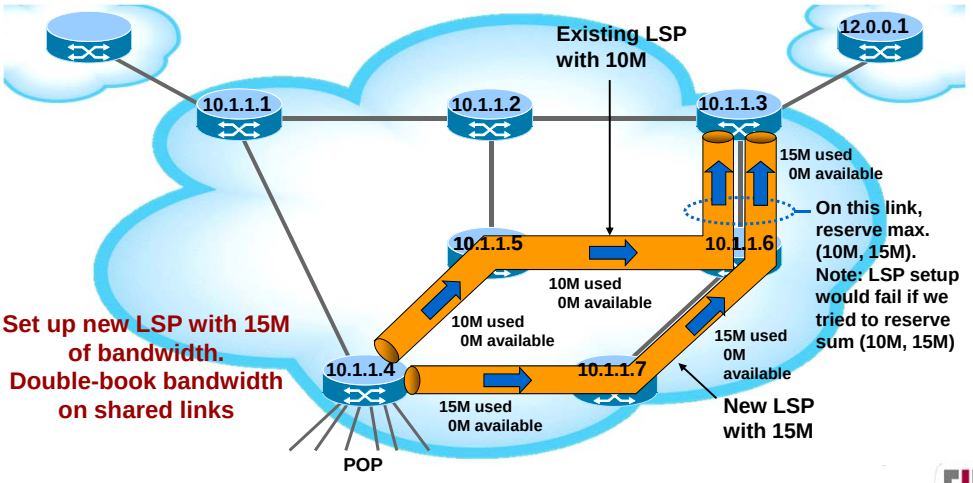
Setup priority: 2

Bandwidth required: 15M

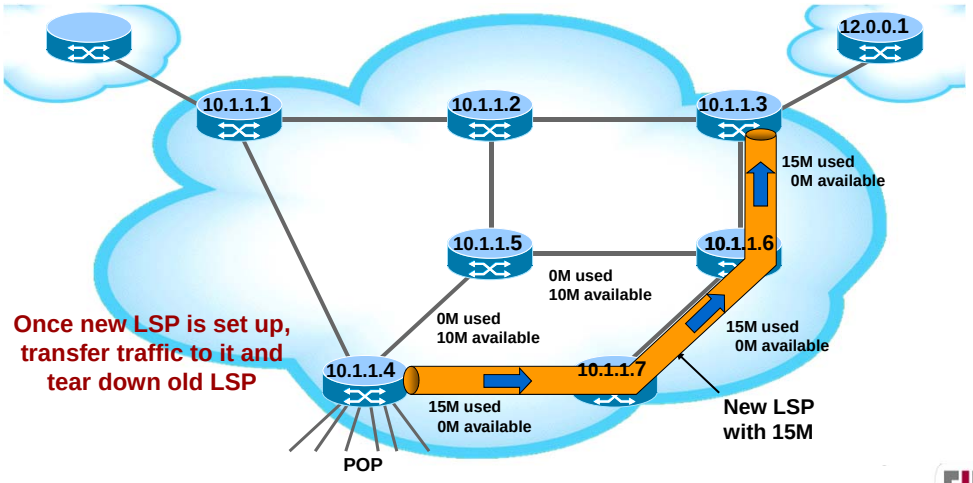
MPLS-TE: LSP modification "make-before-break"

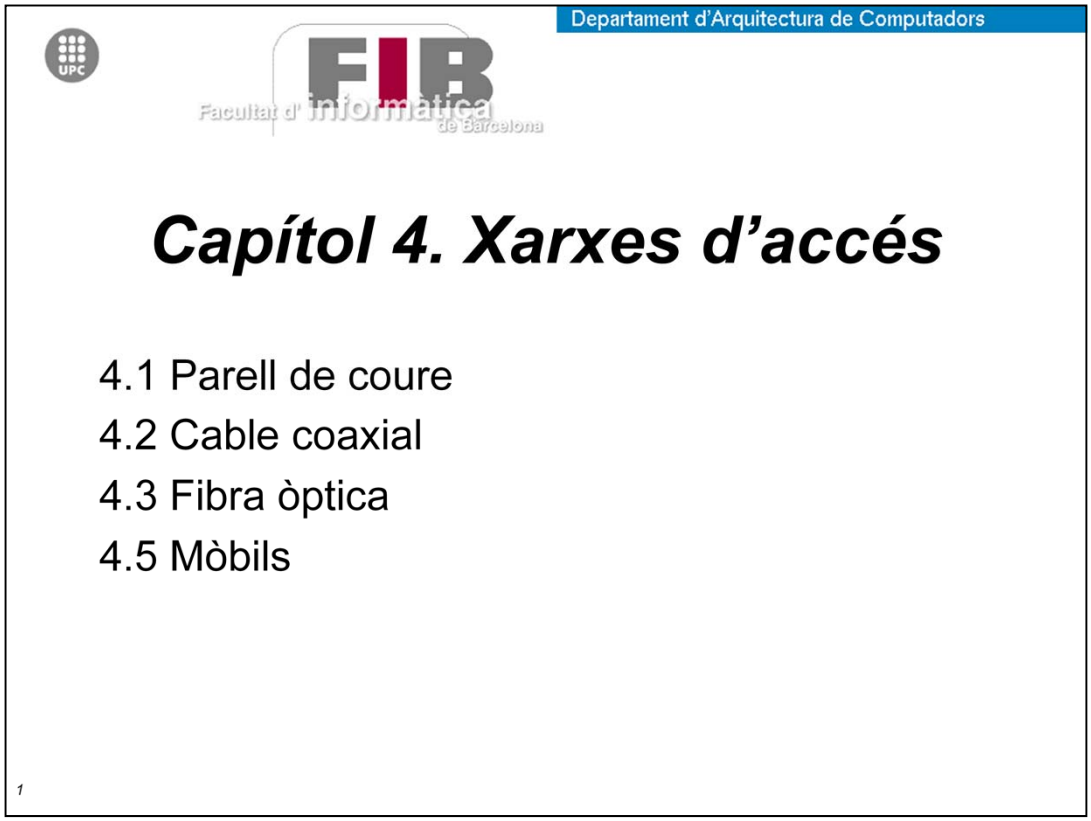


MPLS-TE: LSP modification "make-before-break"



MPLS-TE: LSP modification "make-before-break"




Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
Capítol 4. Xarxes d'accés
4.1 Parell de coure
4.2 Cable coaxial
4.3 Fibra òptica
4.5 Mòbils
1

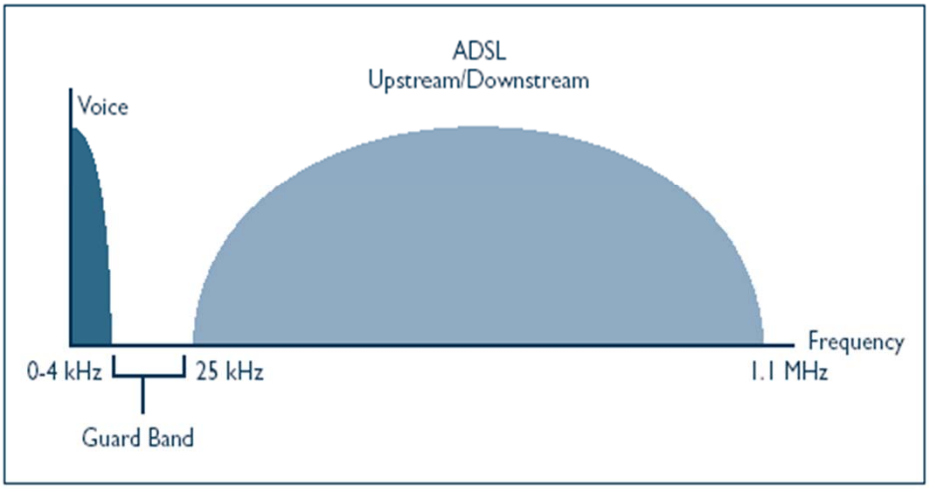

Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
4.1 Parell de coure
2

Departament d'Arquitectura de Computadors

xDSL technologies

A whole family of technologies for data transmission over the copper pair is referred to as xDSL, where "x" is replaced starting in each case by the letters that distinguish each mode. In general xDSL is a set of technologies that provide high bandwidth over local loop copper wire without signal amplifiers or repeaters along the route of the wiring connection between the client and the telephone exchange to which is connected.

Splitting the frequencies



The telephone analogue frequency uses only a small proportion of the bandwidth on a line

(under 4kHz).The maximum amount of data that conventional dial-up modems can transmit

through a POTS system is about 56Kbps. Using this method to send data, the transmission

through the telephone company is a bandwidth bottleneck.

Typical telephone cabling is capable of supporting a greater range of frequencies (around

1MHz). With DSL modems, the digital signal is not limited to 4kHz of voice frequencies, as it

does not need to travel through the telephone switching system. DSL modems enable up to

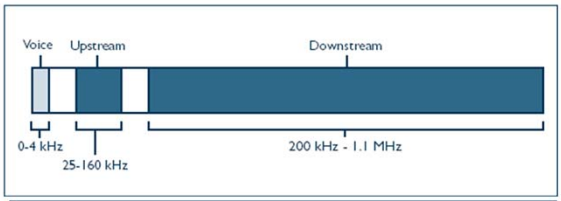
1MHz of bandwidth to be used for transmitting digital (data) alongside analogue (voice) signals

on the same wire by separating the signals, thereby preventing the signals from interfering with

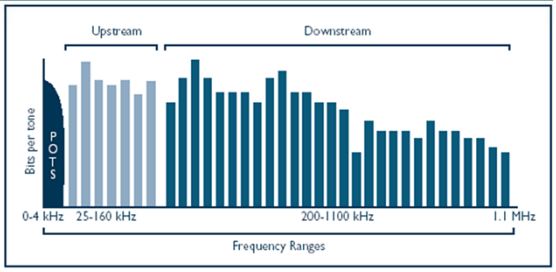
each other. Figure 2 shows how the analogue and digital frequencies are split.

Modulation.

CAP



DMT



The basic idea of DMT is to split the available bandwidth into a large number of subchannels. DMT is able to allocate data so that the throughput of every single subchannel is maximized. If some subchannel can not carry any data, it can be turned off and the use of available bandwidth is optimized.

Carrierless Amplitude Phase (CAP) is an encoding method that divides the signals into two distinct bands:

• The upstream data channel (to the service provider), which is carried in the band between 25 and 160kHz.

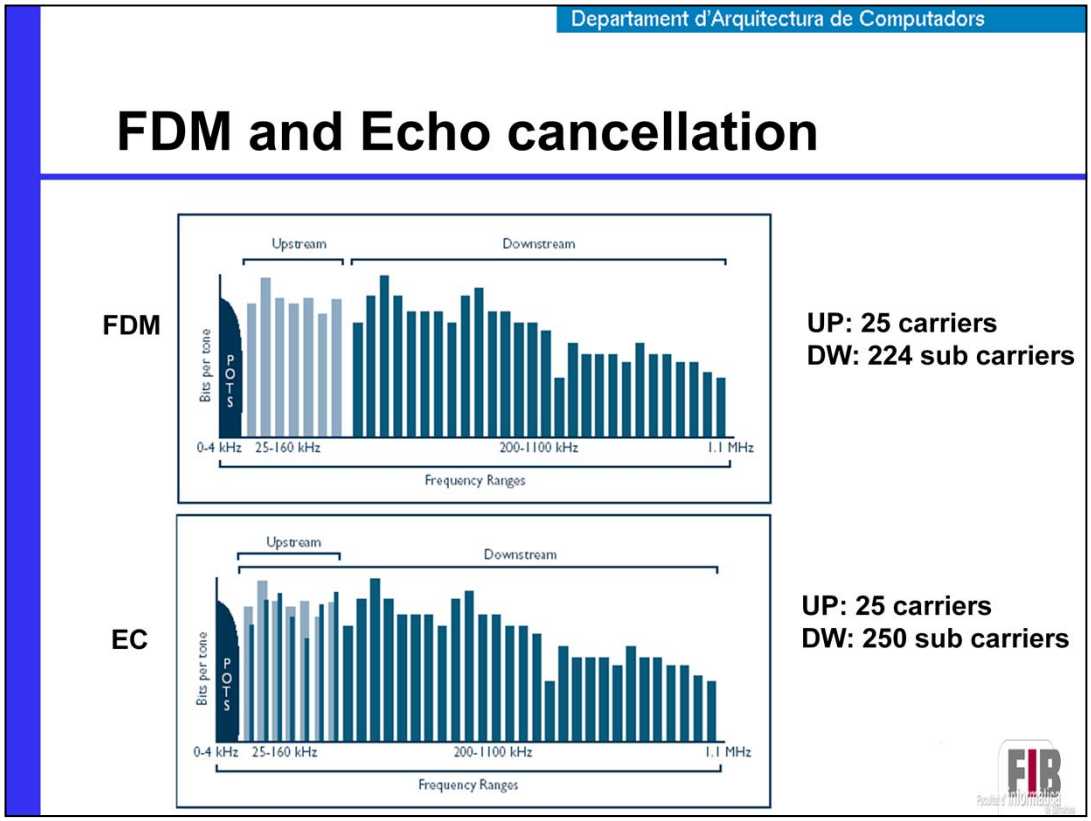
• The downstream data channel (to the user), which is carried in the band that starts at 200kHz and continues to a variable end point, depending on a number of factors, such as line length and line noise, but the maximum is about 1.1MHz. These channels are widely separated in order to minimise the possibility of interference between the channels.

Discrete Multi-Tone (DMT), the most widely used modulation method, separates the DSL signal so that the usable frequency range is separated into 256 channels of 4.3125kHz each. DMT has 224 downstream frequency bins (or carriers) and 32 upstream frequency bins. Up to 15 bits per signal can be encoded on each frequency bin on a good quality line.

Each of the 256 channels is monitored separately to ensure the data travelling along it is not impaired. DMT constantly shifts signals between different channels to ensure that the best channels are used for transmission and reception. DMT can take advantage of all usable tones in the spectrum and works around areas where interference is present. Some of the lower channels can be used as bi-directional channels for both upstream and downstream information.

The basic idea of DMT is to split the available bandwidth into a large number of subchannels. DMT is able to allocate data so that the throughput of every single subchannel is maximized. If some subchannel can not carry any data, it can be turned off and the use of available bandwidth is optimized.

Discrete multitone (DMT) uses multiple carrier signals at different frequencies, sending some of the bits on each channel. The available transmission band (upstream or downstream) is divided into a number of 4-kHz subchannels. On initialization, the DMT modem sends out test signals on each subchannel to determine the signal-to-noise ratio (SNR). The modem then assigns more bits to channels with better signal transmission qualities and less bits to channels with poorer signal transmission qualities. Stallings DCC8e Figure 8.18 illustrates this process. Each subchannel can carry a data rate of from 0 to 60 kbps. The figure shows a typical situation in which there is increasing attenuation and hence decreasing signal-to-noise ratio at higher frequencies. As a result, the higher-frequency subchannels carry less of the load. Present ADSL/DMT designs employ 256 downstream subchannels. In theory, with each 4-kHz subchannel carrying 60 kbps, it would be possible to transmit at a rate of 15.36 Mbps. In practice, transmission impairments prevent attainment of this data rate. Current implementations operate at from 1.5 to 9 Mbps, depending on line distance and quality.



DSL White Paper

Allied Telesyn | White Paper

The DMT frequency bands can be used in two different ways, which are referred to as

Frequency Division Multiplexing (FDM) and Echo Cancellation.

Frequency Division Multiplexing (FDM)

With FDM, the low-speed upstream channel is quite separate from the high-speed

downstream channel. In order to prevent interference between the frequency bands, a

space, known as the guardband, is required between the upstream and downstream

frequencies. Most ADSL modems today use FDM.

Echo Cancellation

With Echo Cancellation the downstream channel overlaps the upstream channel, so

simultaneous upstream and downstream signals are sent on the lower frequencies. An echo

on the upstream signal can cause corruption on the downstream signal. Echo cancellation is

used to obtain a clear signal in the event that both streams send data simultaneously.

Departament d'Arquitectura de Computadors

ADSL concept

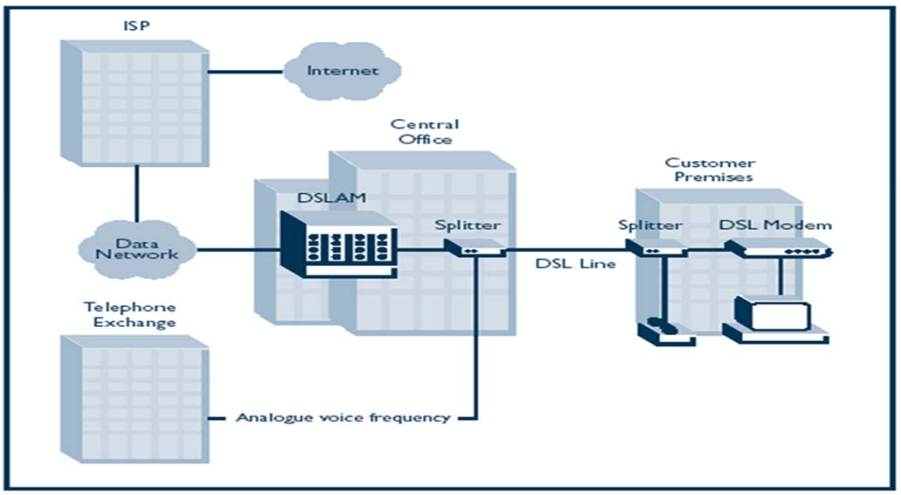
Asymmetric Digital Subscriber Line (ADSL), an important variant of the DSL family, has become very popular. With ADSL, most of the data bandwidth is devoted to sending data downstream towards the user and a smaller proportion of the bandwidth is available for sending data upstream towards the service provider. This scenario suits Internet browsing applications, which typically involve much more downstream than upstream dataflow.

Departament d'Arquitectura de Computadors

Standards

- ANSI (American National Standards Institute) in sucomité T1.143 issue 1 (1995) and T1.413 issue 2 (1998) defines the standard for the physical layer.
- ETSI (European Telecomunication Standards Institute) has contributed to including an annex with European requirements.
- ITU (International Telecommunications Union) has developed recommendations G.992.1, G.994.1, G.995.1, G.996.1 and G.997.1.
- ADSL Forum proposed protocols, interfaces and architectures necessary for the development of ADSL.
- The ATM Forum and DAVIC (Digital Audio-Visual Council) have been recognized as a transmission protocol ADSL physical layer for unshielded pairs.

ADSL network setup



When digital data is sent from a customer's premises, it travels from their computer through a DSL modem and a splitter.When analogue voice signals are sent from a customer's telephone they are also sent through the splitter, which combines the analogue voice and digital data signals, enabling them to be sent over the same line.

At the other end of the line, the local loop goes into a splitter at the local phone company's COs, which splits the digital data frequencies from the analogue voice frequencies.The voice frequencies are sent to the local telephone exchange and the digital data is sent to a Digital Subscriber Line Access Multiplexor (DSLAM) before being sent on to the Internet Service Provider (ISP).The digital data never enters the standard telephone switching system.

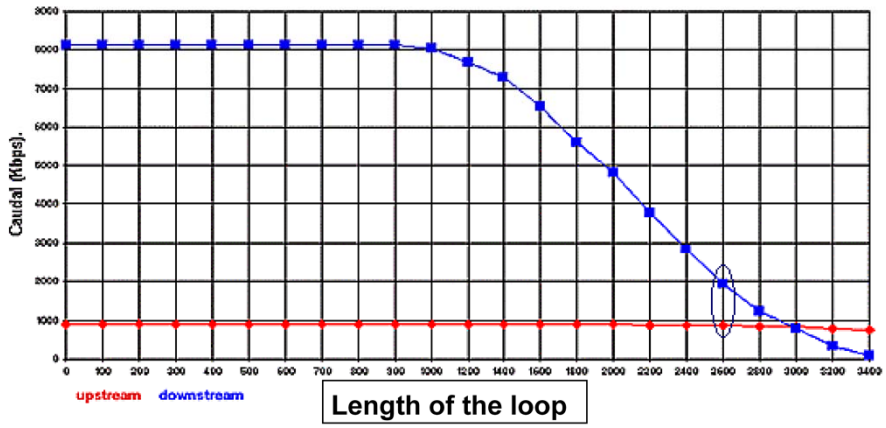
Voice and data frequencies going in the opposite direction—to the customer's premises—follow the reverse route from the ISP through a DSLAM, then a splitter at the CO, and are then sent over the copper wires to the customer's site before being split again.

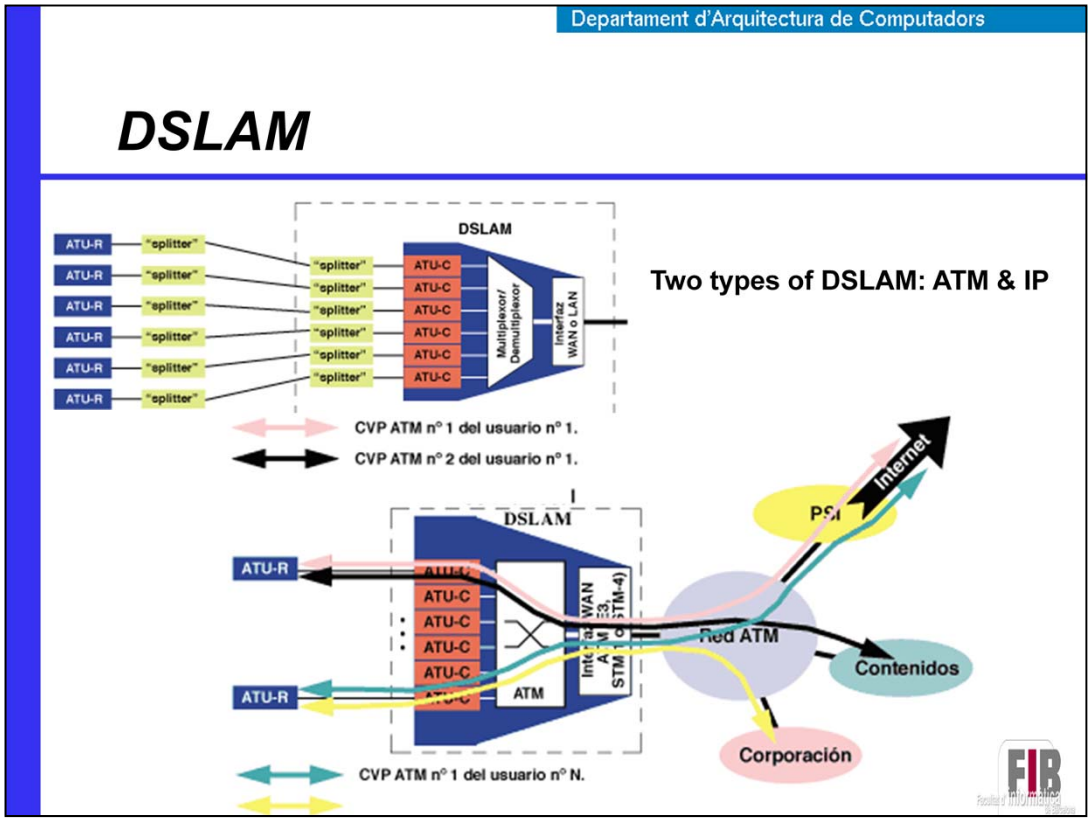
The DSLAM is the equipment that really allows DSL to happen.The DSLAM handles the highspeed

digital data stream coming from numerous customers and aggregates it onto a single high-capacity connection (ATM or Gigabit Ethernet line) to the Internet Service Provider and vice versa. DSLAMs are generally flexible and can support a number of different DSL connections as well as different protocol and modulation technologies in the same type of DSL. Figure 4 shows how an ADSL network is setup.

Departament d'Arquitectura de Computadors

Performance of ADSL. Throughput

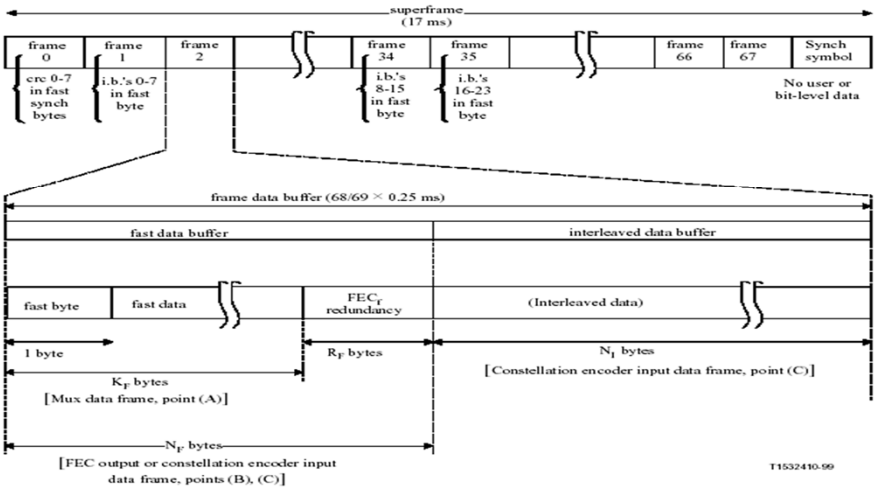




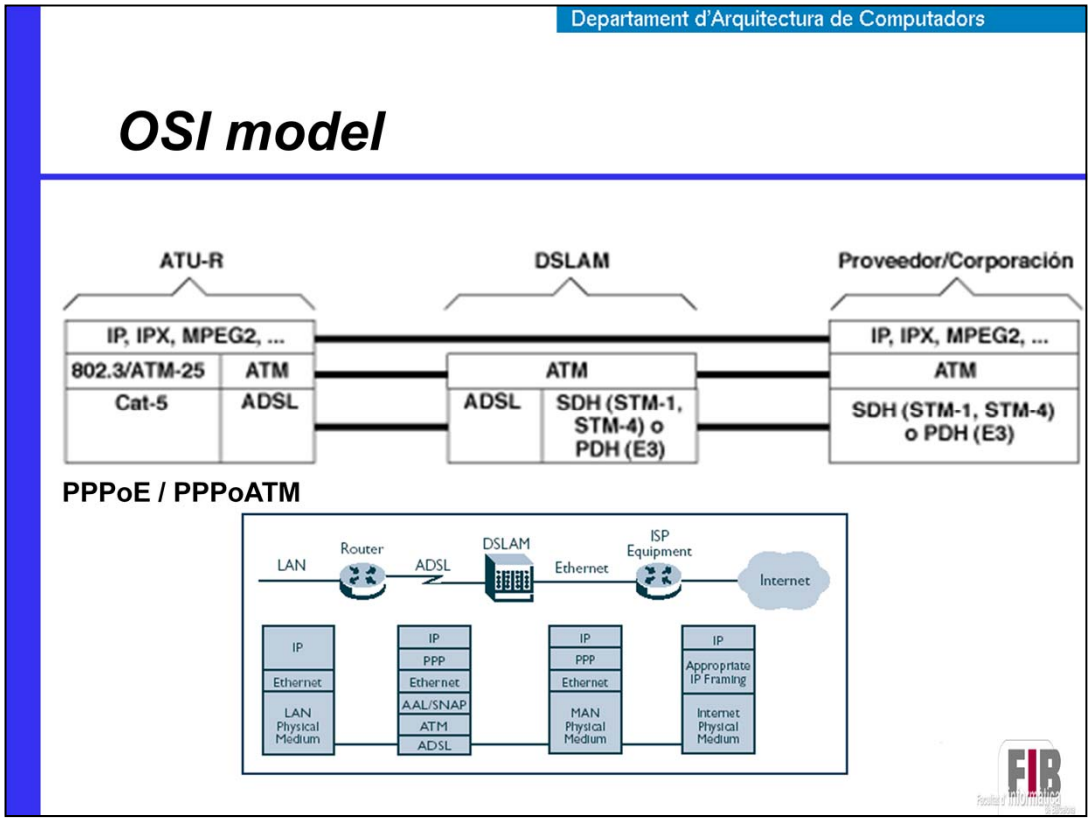
There are two main types of DSLAM—IP DSLAM and ATM DSLAM.When ADSL services first began, ATM was the main high-speed data backbone transport used in Telecommunications networks. So DSLAMs with an ATM uplink port (ATM DSLAMs) were developed to enable the ADSL link to connect quite seamlessly into the whole ATM network.The 'last mile' ATM link over the ADSL line was then just an extended finger of a telecommunications company's ATM network.

Recently, Ethernet has taken quite a step up in bandwidth capabilities (from up to one Gigabit, to 10 Gigabit) and is becoming a cheaper and more popular choice for the transport protocol in Metro Area Networks. In installations where subscribers are using DSL to access a Metro Area Network, it makes sense for the DSLAMs to have Ethernet uplink ports. DSLAMs with Ethernet uplink ports are known as IP DSLAMS.The market is rapidly moving towards IP DSLAMs because they are cheaper to implement, scale better and are easier to manage than ATM DSLAMs.

Super frame ADSL



Hay 68 tramas pero el canal adicional de sincronismo está introducido por el modulador y repartido por todas las tramas por lo que el tamaño del buffer de cada trama es 68/69x0,25ms aunque cada trama es de 250 microsegundos.



There has been no universal agreement reached over the sort of packet on which to perform RFC 1483 encapsulation, so there are now a number of different choices of protocol stack to have above the RFC 1483 Layer.

The most common protocol stack is Point-to-Point Protocol over Ethernet and ATM (PPPoEoA). Figure 9 demonstrates how PPPoEoA enables IP packets to travel over both an Ethernet and an ATM connection.

When travelling from the LAN to an ADSL connection, IP packets encapsulated in Ethernet frames pass through an ADSL router, which attaches a PPP header to the frames.The frames then undergo AAL5 encapsulation to create smaller ATM cells, which are sent over the ADSL connection to a DSLAM at the local phone company office.

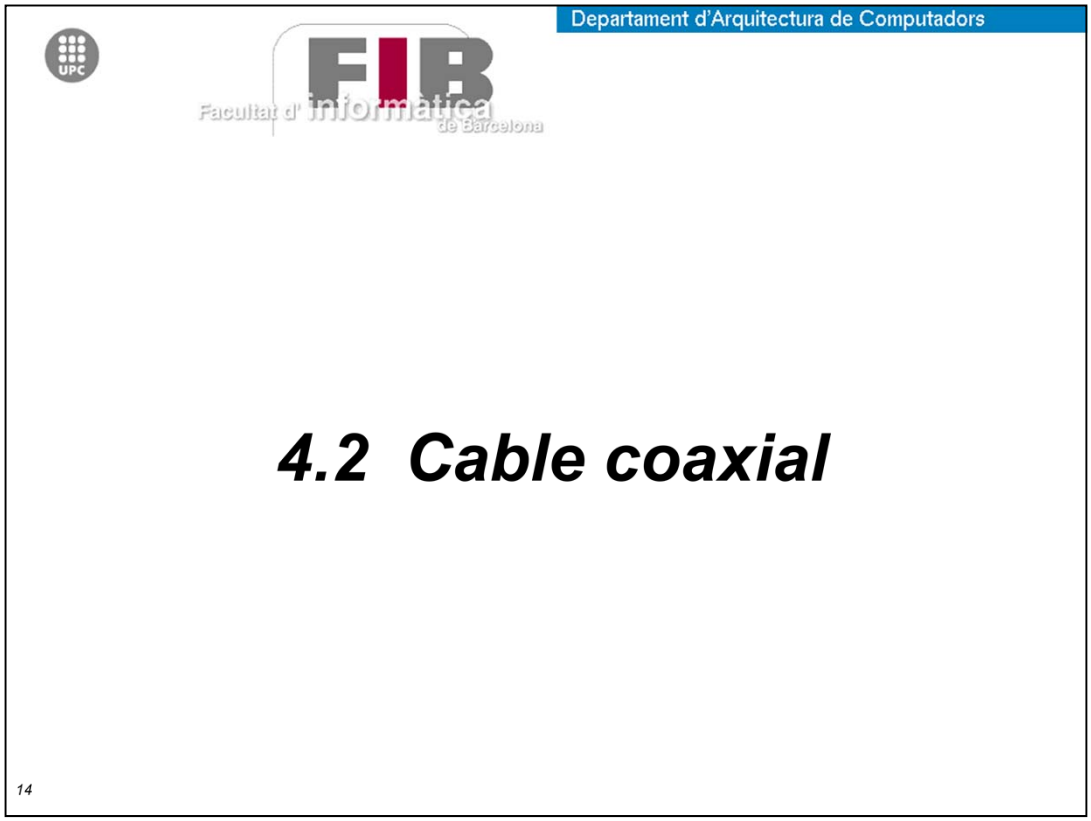
The DSLAM in this instance is connected to an Ethernet network, so the ATM cells go through the reverse process described above to reveal the Ethernet frames, which are sent on to the ISP. At the ISP, the Ethernet frames are removed to reveal the IP data, which is then framed according to the network it will continue to travel on.

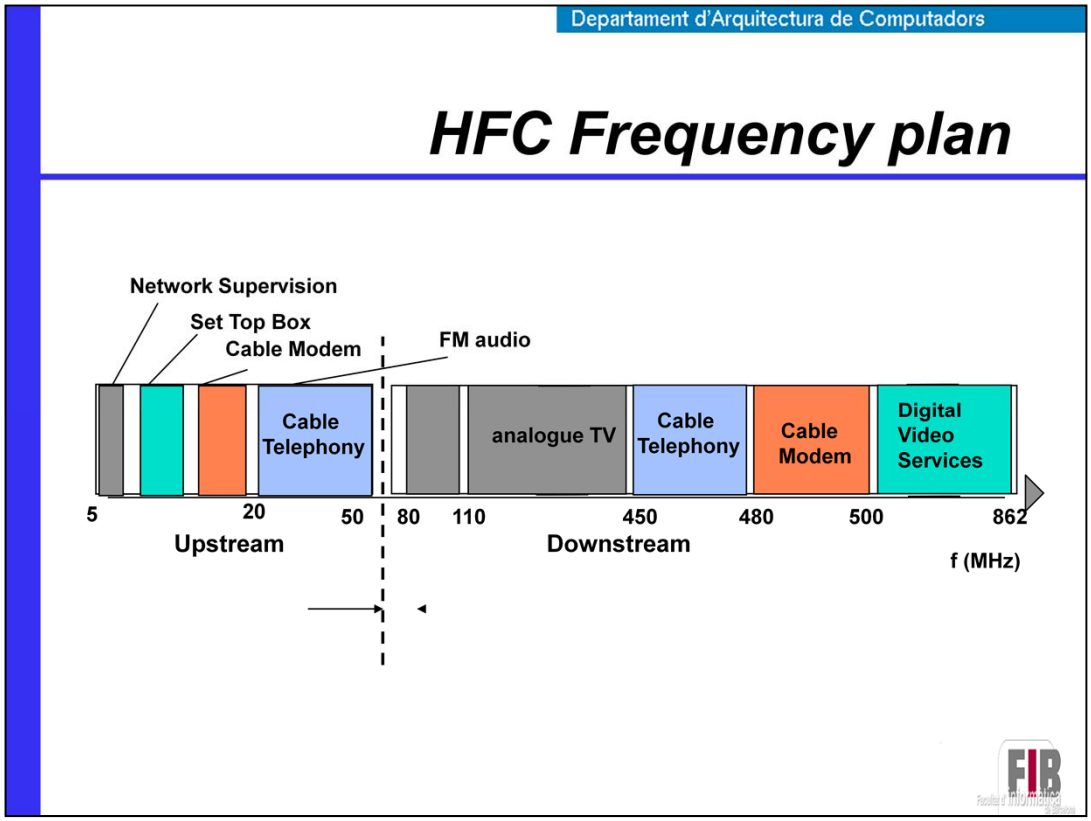
Other protocol stacks include:

IPoA, which was designed to make IP subnets map directly onto ATM networks in the same way that IP subnets map onto VLANs. So, an ATM address resolution protocol was introduced to enable the IP stack to obtain an "ATM address" for another IP host connected to its local ATM subnet (RFC 2225).The structure required for this kind of network is quite complex, mostly because trying to make a channel oriented transportation method like ATM appear like a broadcast domain is not a very natural fit.

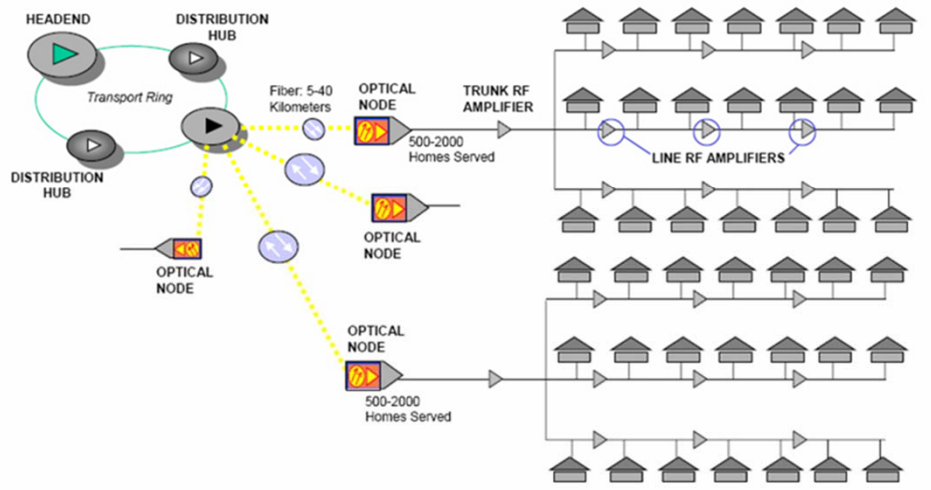
RFC 1483 Bridged, which is where the whole Ethernet packet that arrives at the ADSL router is encapsulated into AAL5, using the 'bridged-data' format defined in RFC 1483, and sent on the ADSL line.The packets are forwarded based on their MAC address, so they are bridged.

RFC 1483 Routed, which uses the same 'bridged-data' format as RFC 1483 Bridged to encapsulate Ethernet packets into AAL5. However, the packets are forwarded based on their IP address, so they are routed.


Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
4.2 Cable coaxial
14

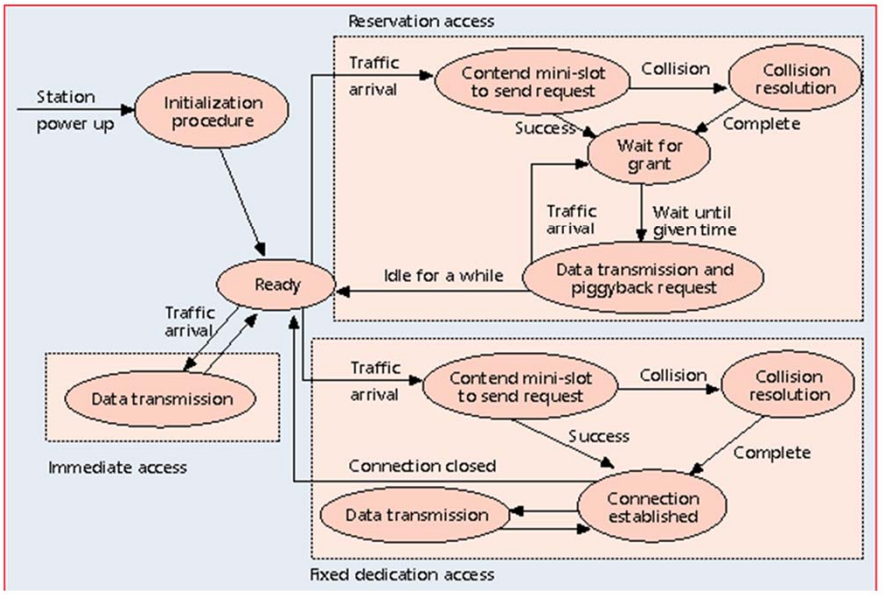

Departament d'Arquitectura de Computadors
HFC Frequency plan
Network Supervision
Set Top Box
Cable Modem
FM audio
Cable Telephony
analogue TV
Cable Telephony
Cable Modem
Digital Video Services
5
20
50
80
110
450
480
500
862
Upstream
Downstream
f (MHz)

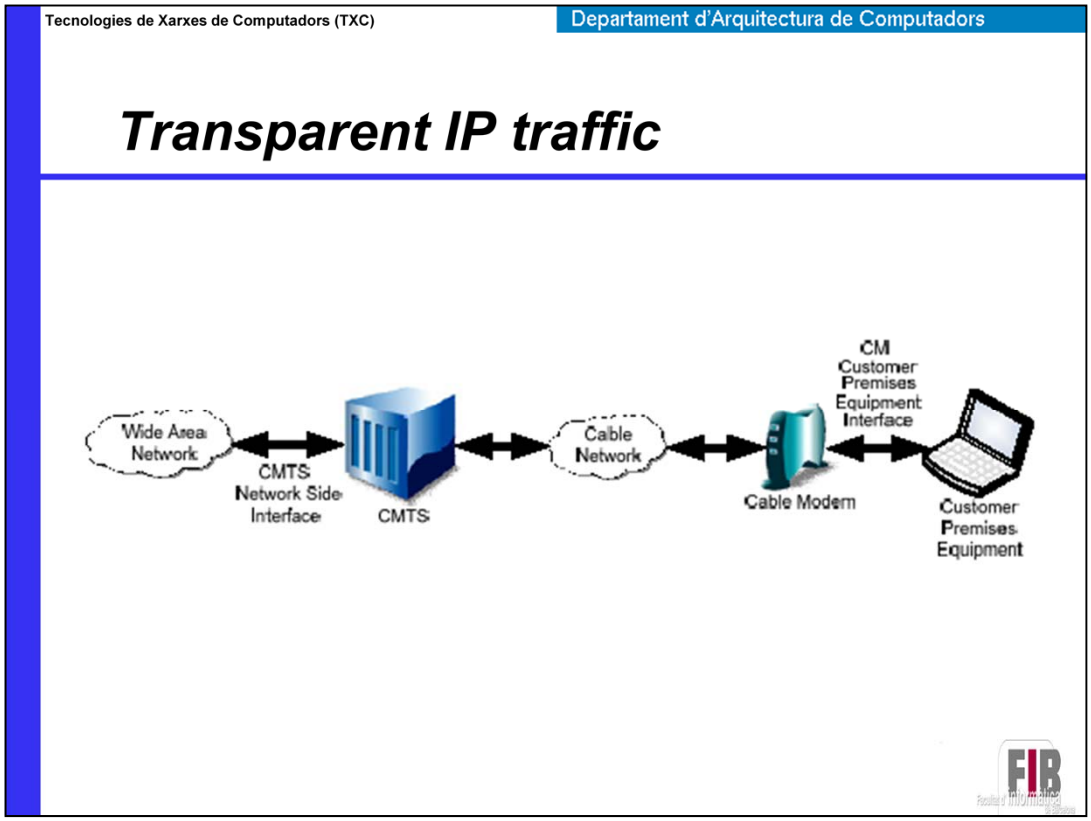
HFC Network


HEADEND
DISTRIBUTION HUB
Transport Ring
DISTRIBUTION HUB
Fiber: 5-40 Kilometers
OPTICAL NODE
TRUNK RF AMPLIFIER
500-2000 Homes Served
LINE RF AMPLIFIERS
OPTICAL NODE
OPTICAL NODE
OPTICAL NODE
500-2000 Homes Served

Departament d'Arquitectura de Computadors

MAC access mode





As cable operators have widely deployed high-speed data services on cable television systems, the demand for

bandwidth has increased. Additionally, networks have scaled to such a degree that IPv4 address constraints are

becoming a burden on network operations. To this end, CableLabs' member companies have decided to add new

features to the DOCSIS specification for the purpose of increasing channel capacity, enhancing network security,

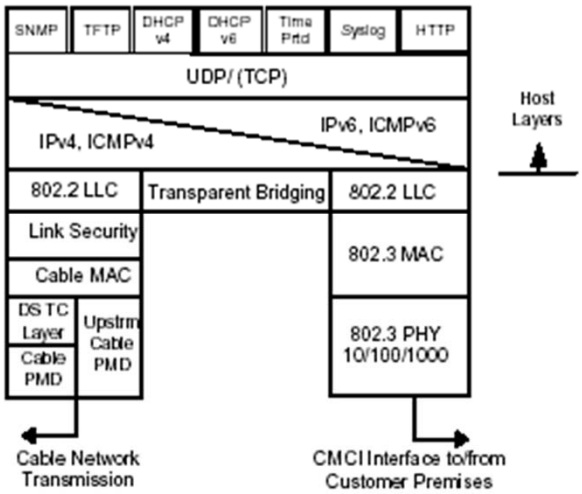
expanding addressability of network elements, and deploying new service offerings.

The DOCSIS system allows transparent bi-directional transfer of Internet Protocol (IP) traffic, between the cable

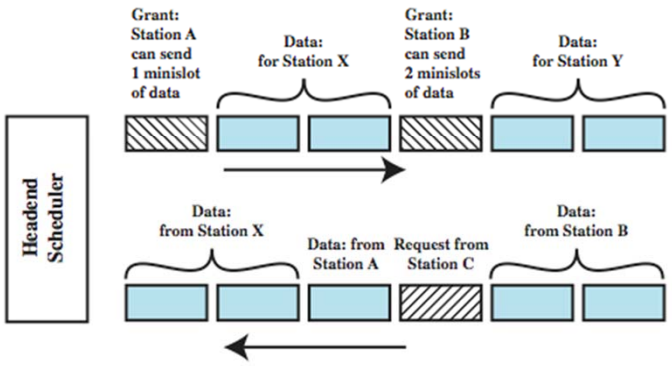
system head-end and customer locations, over an all-coaxial or hybrid-fiber/coax (HFC) cable network. This is

shown in simplified form in Figure 1–2.

Docsis Cable Modem protocols stack



Cable Modem Scheme

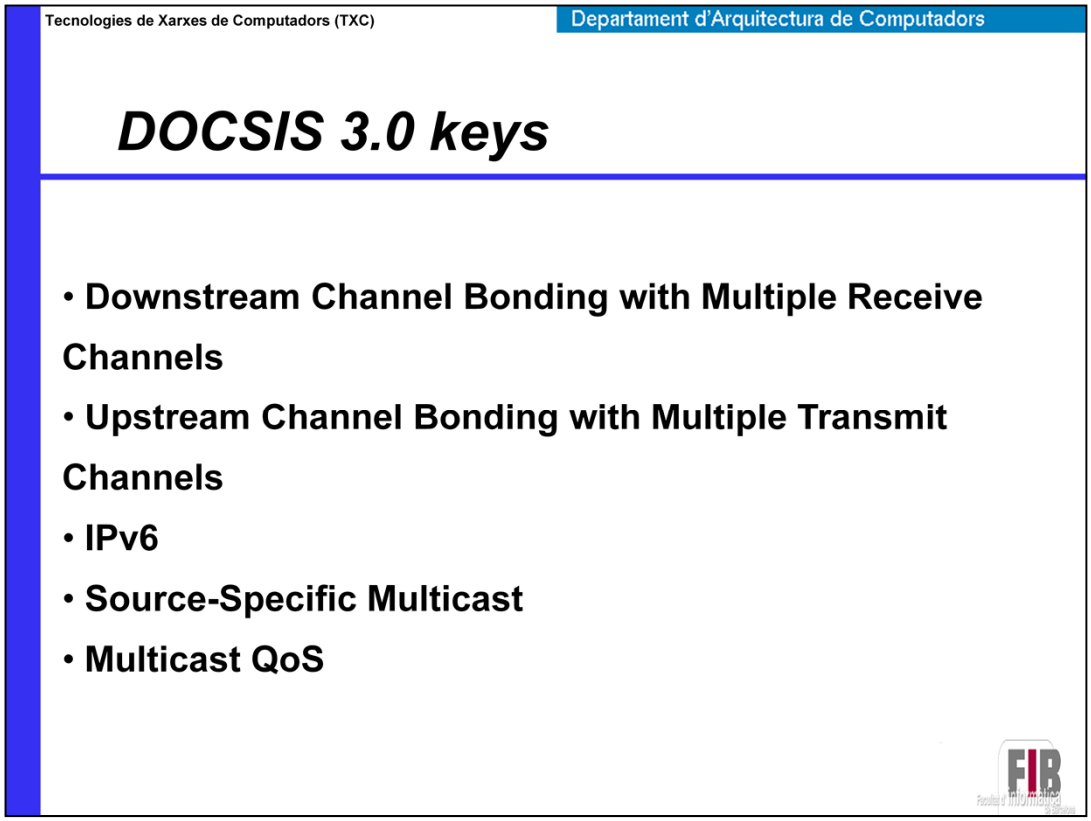


A form of statistical TDM is typically used with Cable Modems, as illustrated in Stallings DCC8e Figure 8.16. This also shows the request and allocation of upstream time slots.

Departament d'Arquitectura de Computadors

MAC functions

- Initialization.
  - Ranging. RTC correction parameter.
  - Synchronization.
- Physical layer MAC Level
- Access mode upstream channel.
  - Immediate access (not allowed)
  - Restricted access
  - Access isochronous
- Collision Resolution



• **Downstream Channel Bonding with Multiple Receive Channels:** DOCSIS 3.0 introduces the concept of a CM that receives simultaneously on multiple receive channels. Downstream Channel Bonding refers to the ability (at the MAC layer) to schedule packets for a single service flow across those multiple channels. Downstream Channel Bonding offers significant increases in the peak downstream data rate that can be provided to a single CM.

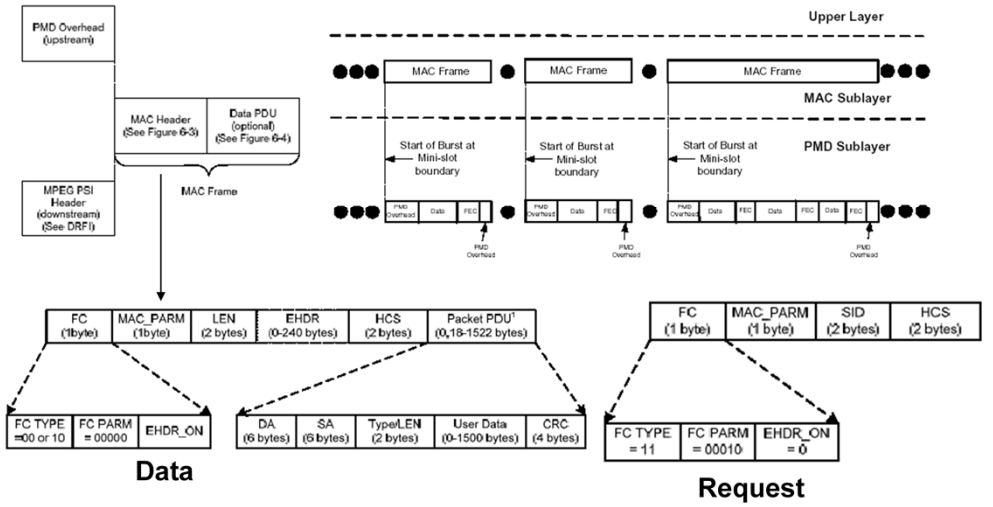
• **Upstream Channel Bonding with Multiple Transmit Channels:** DOCSIS 3.0 introduces the concept of a CM that transmits simultaneously on multiple transmit channels. Upstream Channel Bonding, refers to the ability to schedule the traffic for a single upstream service flow across those multiple channels. Upstream Channel Bonding offers significant increases in the peak upstream data rate that can be provided to a single CM. DOCSIS 3.0 also introduces other enhancements in the upstream request-grant process that improve the efficiency of the upstream link.

• **IPv6:** DOCSIS 3.0 introduces built-in support for the Internet Protocol version 6. DOCSIS 3.0 CMs can be provisioned with an IPv4 management address, an IPv6 management address, or both. Further, DOCSIS 3.0 CMs can provide transparent IPv6 connectivity to devices behind the cable modem (CPEs), with full support for Quality of Service and filtering.

• **Source-Specific Multicast:** DOCSIS 3.0 supports delivery of Source-Specific IP Multicast streams to CPEs.
Rather than extend the IP multicast protocol awareness of cable modems to support enhanced multicast control protocols, DOCSIS 3.0 takes a different approach. All awareness of IP multicast is moved to the CMTS, and a new DOCSIS-specific layer 2 multicast control protocol between the CM and CMTS is defined which works in harmony with downstream channel bonding and allows efficient and extensible support for future multicast applications.

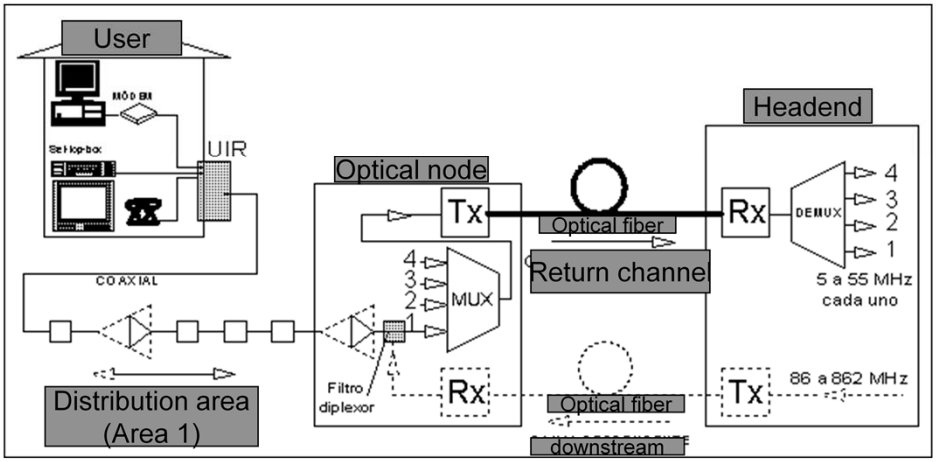
• **Multicast QoS:** DOCSIS 3.0 defines a standard mechanism for configuring the Quality of Service for IP multicast sessions. It introduces the concept of a "Group Service Flow" for multicast traffic that references a Service Class Name that defines the QoS parameters for the service flow.

DOCSIS MAC format



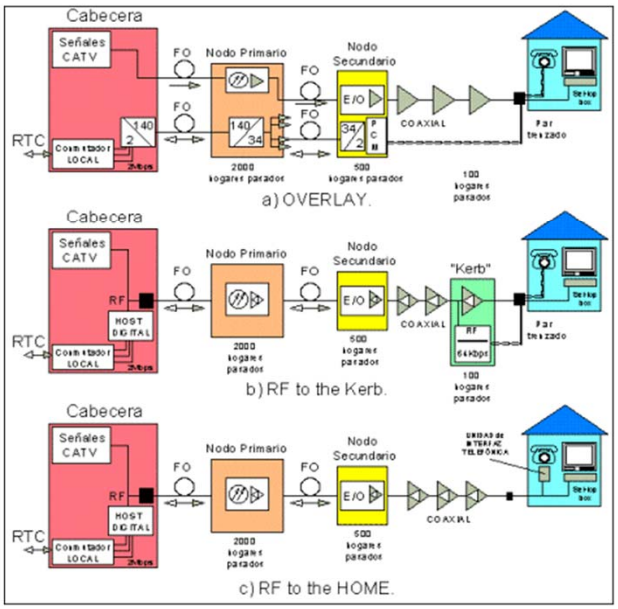
Departament d'Arquitectura de Computadors

HFC real network



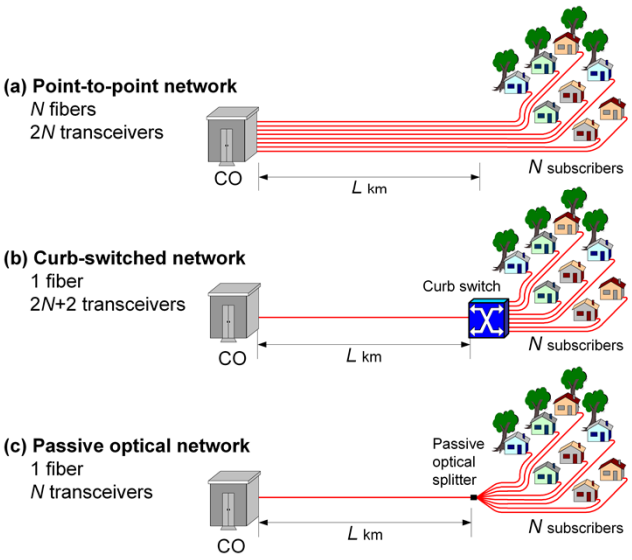
Departament d'Arquitectura de Computadors

HFC telephone




Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
4.3 Fibra òptica
26

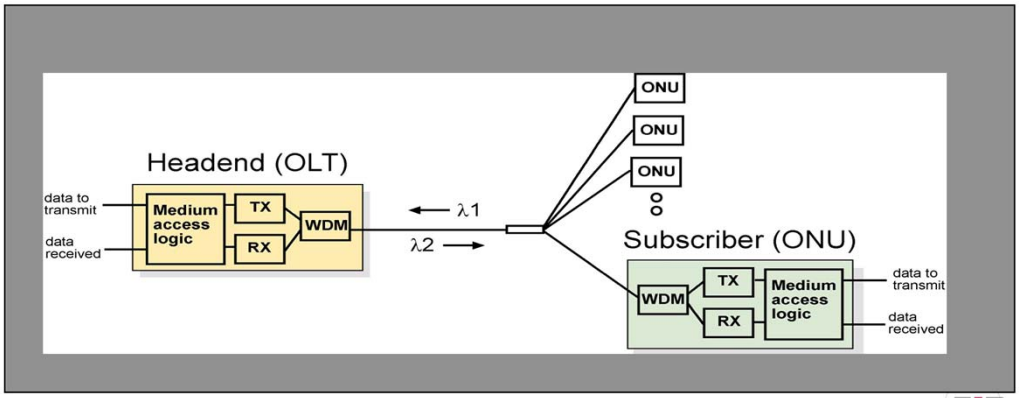
Topologies: Point-to-Point vs. PON



Departament d'Arquitectura de Computadors

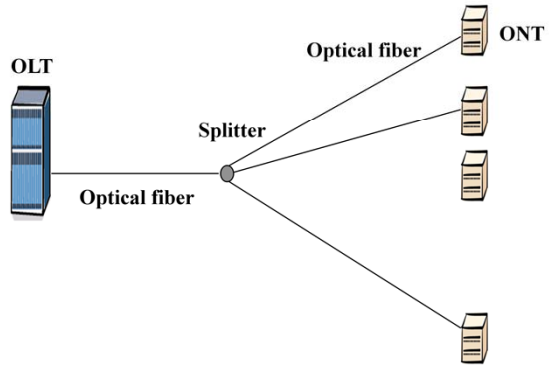
Single-Fiber PON

- Use 2 wavelength, but save fiber (repair and maintenance)
- Use TDM in the upstream to avoid collisions



GPON Technology

GPON: Gigabit Passive Optic Network



- Optical Fiber
- Point to multipoint
- Several levels of splitting
- 2.5 Gps DS and 1.25 Gbps US
- Up to 20 Km
- TDM DS and TDMA US

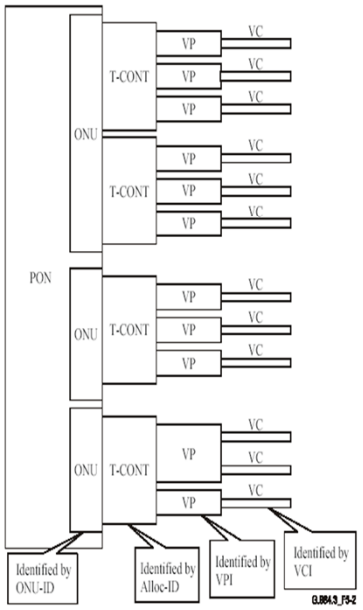
In downstream technology TDM is used. GPON frame is sloted between all users connected. Once the frame arrive to the splitter, this one sends the information that arrives to him by the entrance towards all the exits. This implies that all customers receive the same information, although each one extracts only directed to him.

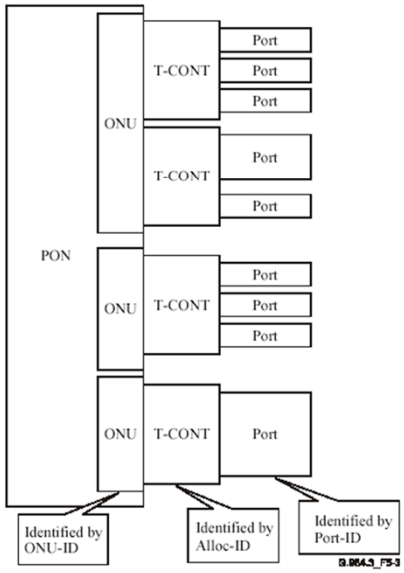
In sense upstream technology TDMA is used. This means that, each user knows the slot that he has assigned and only he transmits then. Each user knows the moment exact at which he must transmit, of such form that splitter is able to recompose the complete frame with the information of all the users.

A mechanism between OLT and ONT exists (ranging) that among them compute the range and applies the necessary delays, so splitter can reconstruct the complete frame without collisions.

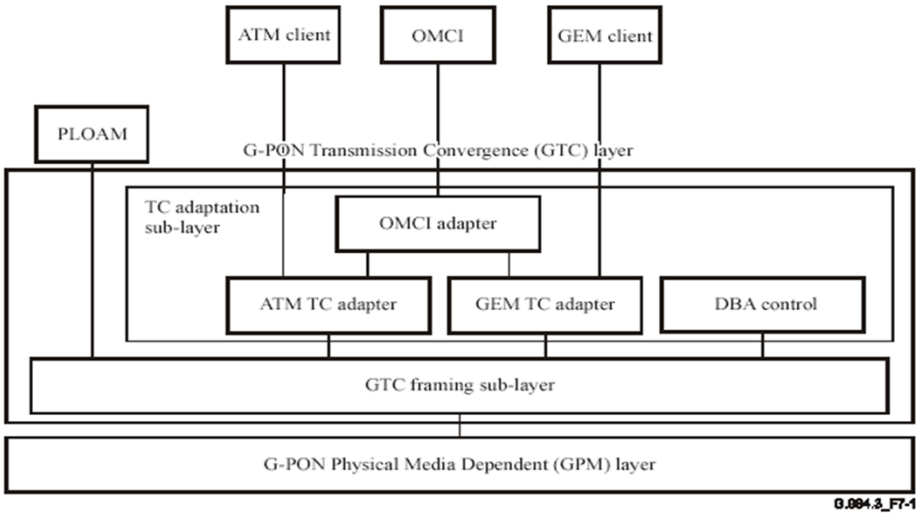
Each frame, as much upstream as downstream, use 125 µseg time range.

Multiplexed architecture

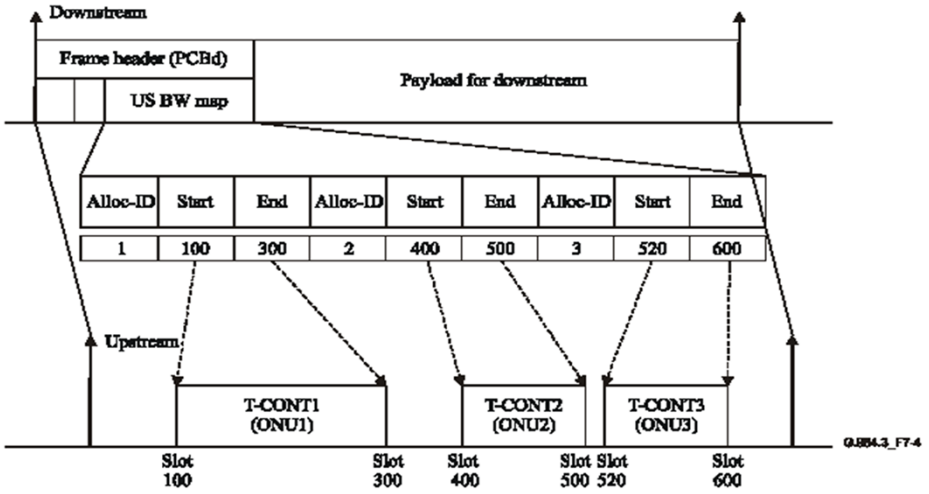




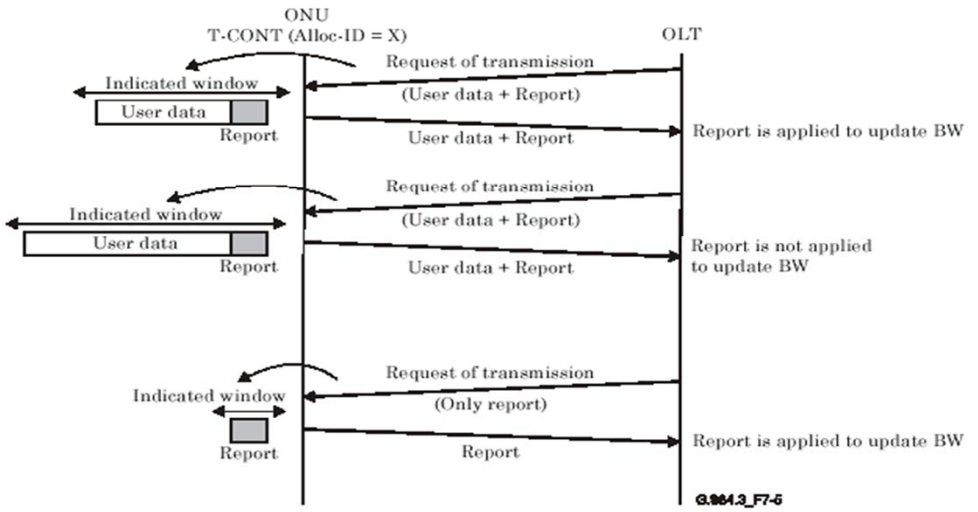
Protocol stack



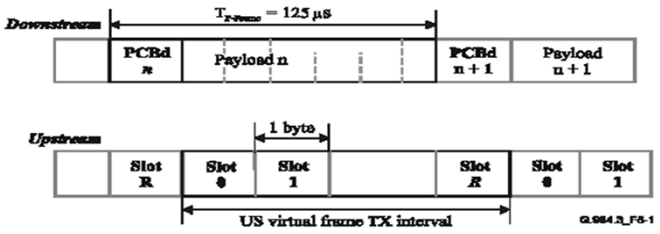
Media access control



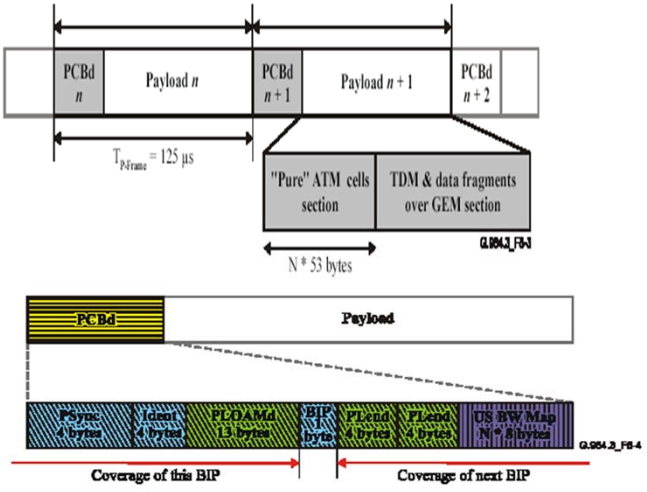
SR-DBA operation



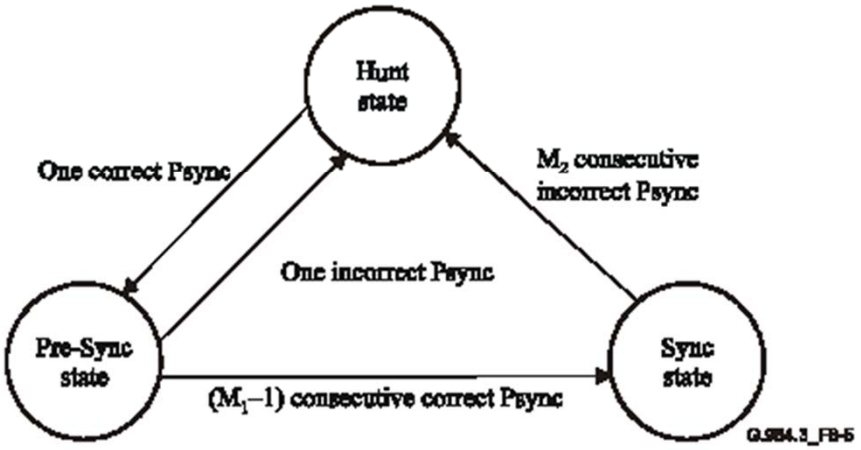
Frame structure



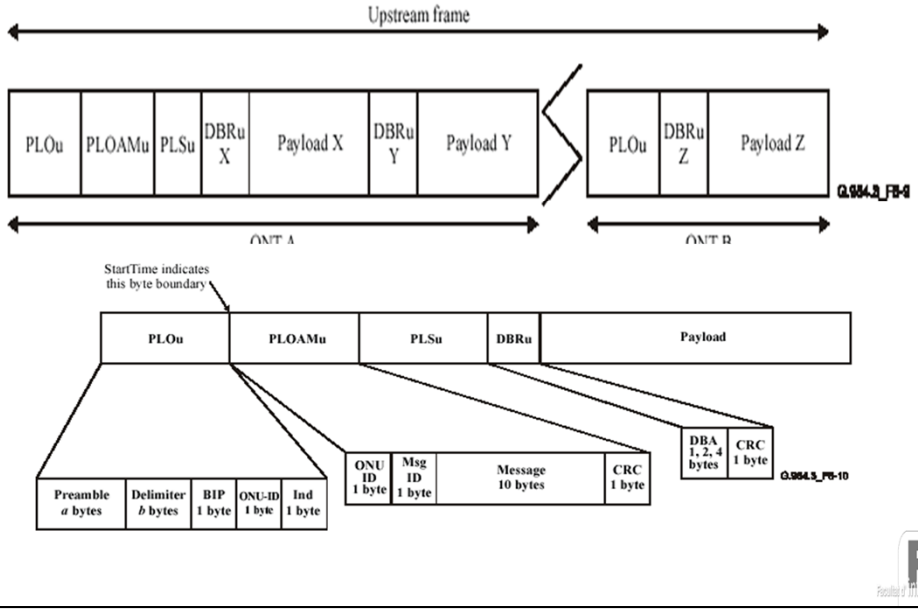
Downstream frame



Downstream synchronization



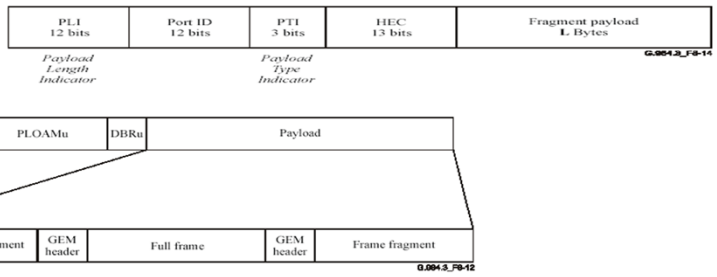
Upstream frame



IND field

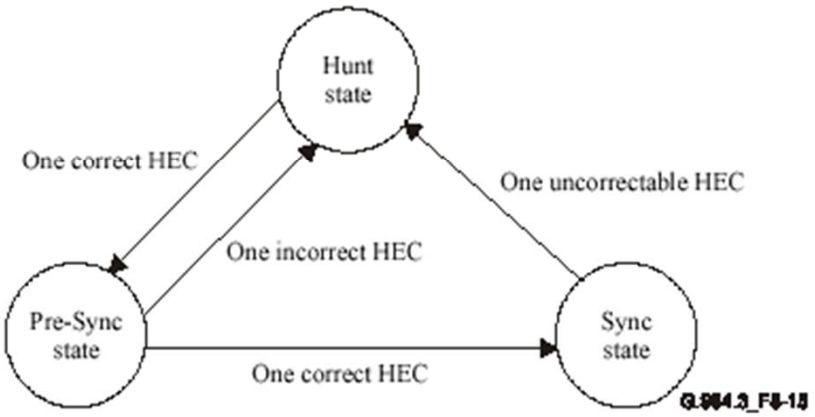
Bit position	Function
7 (MSB)	Urgent PLOAMu waiting (1 = PLOAM waiting, 0 = no PLOAMs waiting)
6	FEC status (1 = FEC ON, 0 = FEC OFF)
5	RDI status (1 = Defect, 0 = OK)
4	Traffic waiting in type 2 T-CONTs
3	Traffic waiting in type 3 T-CONTs
2	Traffic waiting in type 4 T-CONTs
1	Traffic waiting in type 5 T-CONTs
0 (LSB)	Reserved

GEM upstream payload

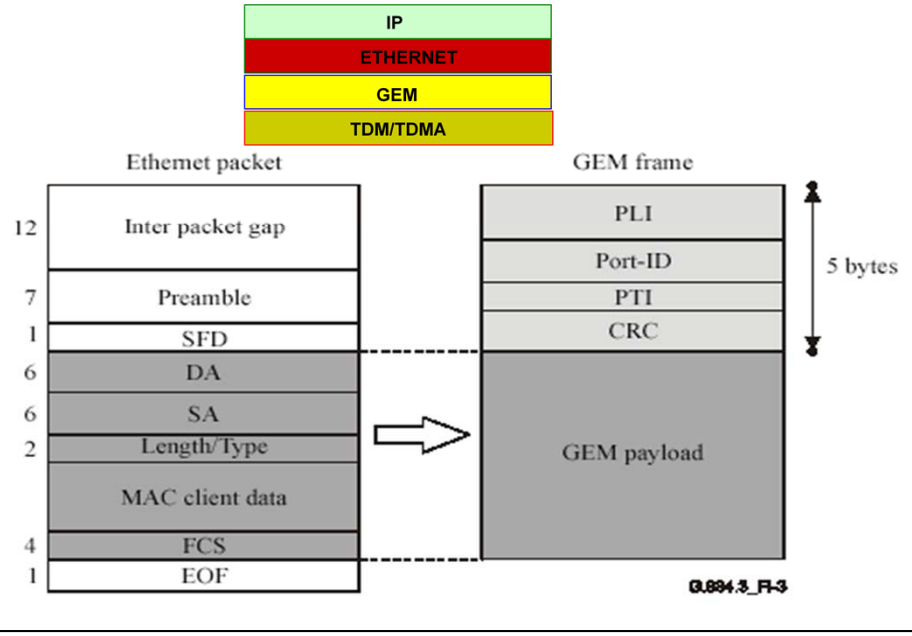


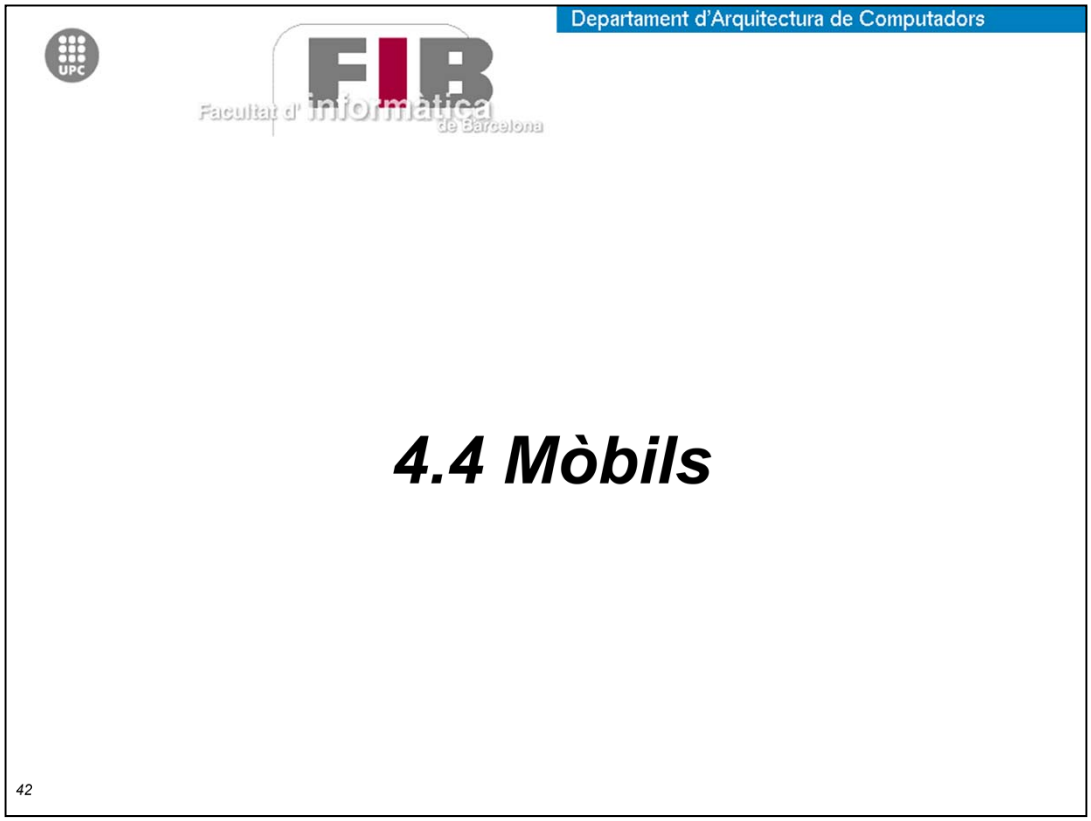
PTI code	Meaning
000	User data fragment, Congestion has Not occurred, Not the end of a frame
001	User data fragment, Congestion has Not occurred, End of a frame
010	User data fragment, Congestion Has occurred, Not the end of a frame
011	User data fragment, Congestion Has occurred, End of a frame
100	GEM OAM
101	Reserved
110	Reserved
111	Reserved

GEM delineation

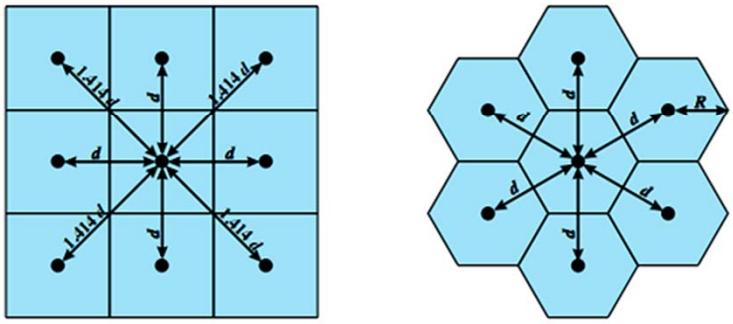


Ethernet over GEM




Departament d'Arquitectura de Computadors
Facultat d' informàtica de Barcelona
4.4 Mòbils
42

Cellular Geometries



(a) Square pattern

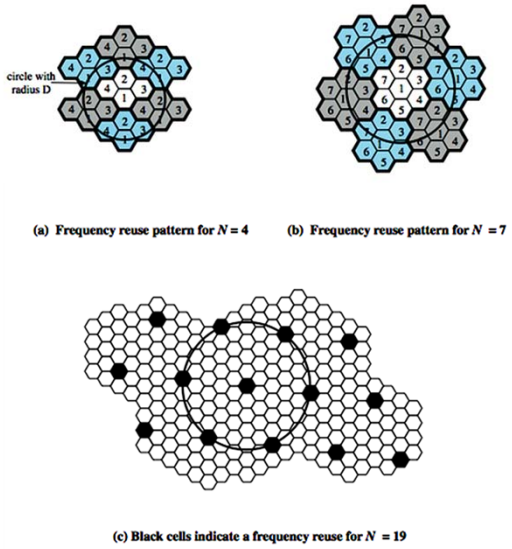
(b) Hexagonal pattern

The first design decision to make is the shape of cells to cover an area. A matrix of square cells would be the simplest layout to define (Stallings DCC9e Figure 14.1a). However, this geometry is not ideal. If the width of a square cell is *d*, then a cell has four neighbors at a distance *d* and four neighbors at a distance *d*. As a mobile user within a cell moves toward the cell's boundaries, it is best if all of the adjacent antennas are equidistant. This simplifies the task of determining when to switch the user to an adjacent antenna and which antenna to choose. A hexagonal pattern provides for equidistant antennas (Stallings DCC9e Figure 14.1b). The radius of a hexagon is defined to be the radius of the circle that circumscribes it (equivalently, the distance from the center to each vertex; also equal to the length of a side of a hexagon). For a cell radius *R*, the distance between the cell center and each adjacent cell center is $d = R$.

In practice, a precise hexagonal pattern is not used. Variations from the ideal are due to topographical limitations, local signal propagation conditions, and practical limitation on sitting antennas.

A wireless cellular system limits the opportunity to use the same frequency for different communications because the signals, not being constrained, can interfere with one another even if geographically separated. Systems supporting a large number of communications simultaneously need mechanisms to conserve spectrum.

Frequency Reuse Patterns



(a) Frequency reuse pattern for $N = 4$ (b) Frequency reuse pattern for $N = 7$

(c) Black cells indicate a frequency reuse for $N = 19$

The essential issue is to determine how many cells must intervene between two cells using the same frequency so that the two cells do not interfere with each other. Various patterns of frequency reuse are possible. Stallings DCC9e Figure 14.2 shows some examples. If the pattern consists of N cells and each cell is assigned the same number of frequencies, each cell can have K/N frequencies, where K is the total number of frequencies allotted to the system. For AMPS (Section 14.2), $K = 395$, and $N = 7$ is the smallest pattern that can provide sufficient isolation between two uses of the same frequency. This implies that there can be at most 57 frequencies per cell on average.

In characterizing frequency reuse, the following parameters are commonly used:

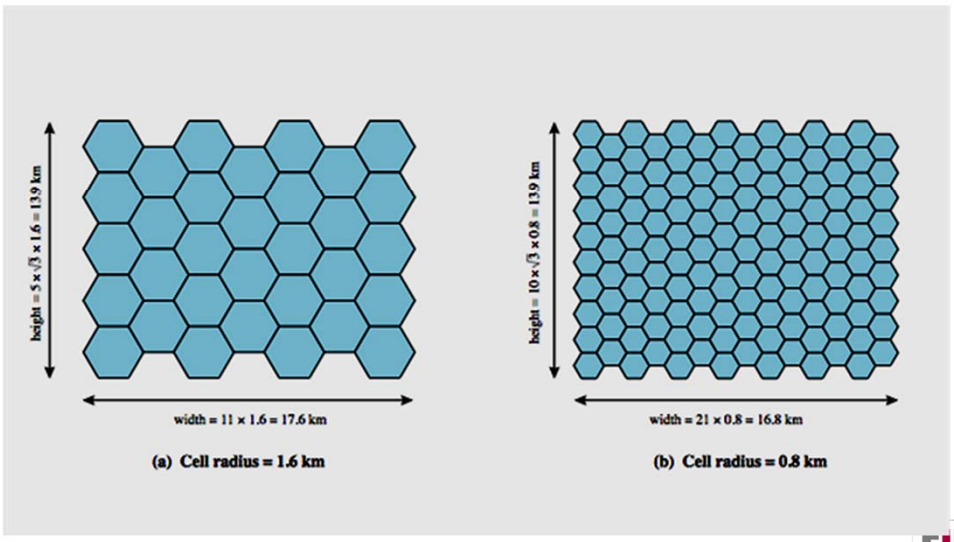
D = minimum distance between centers of cells that use the same band of frequencies (called cochannels)

R = radius of a cell

d = distance between centers of adjacent cells ($d = R$)

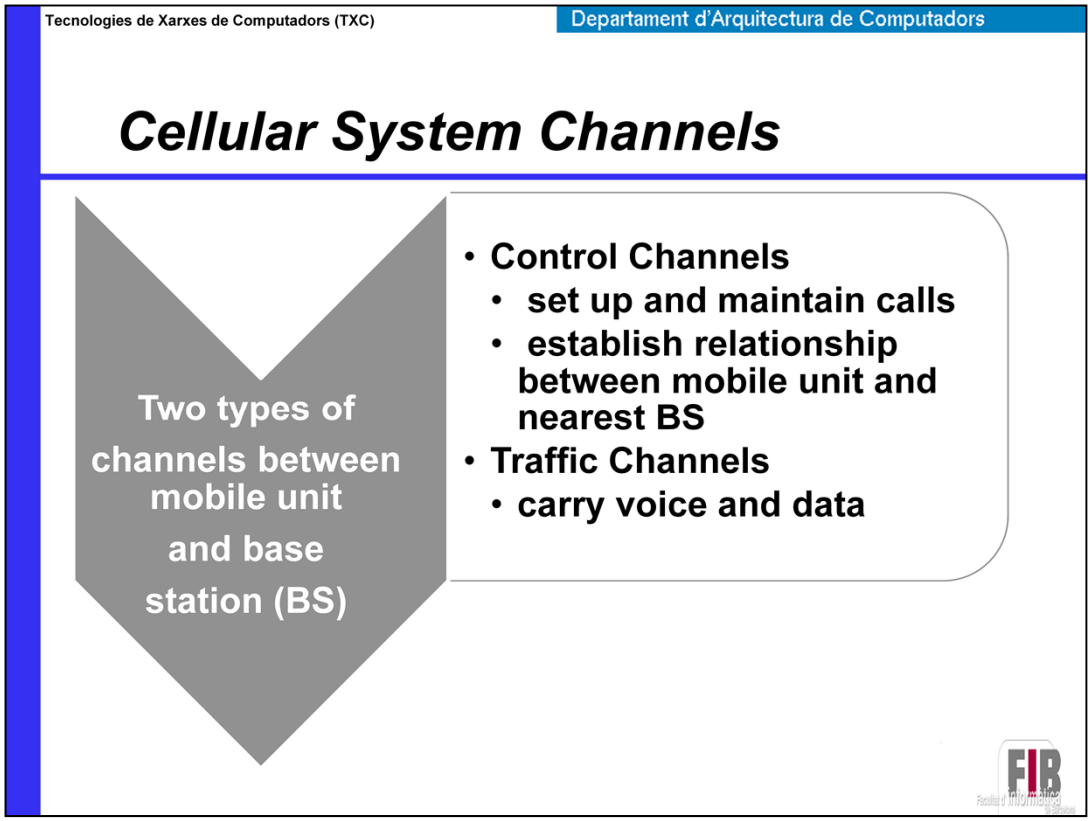
N = number of cells in a repetitious pattern (each cell in the pattern uses a unique band of frequencies), termed the **reuse factor**

Frequency Reuse Example



Assume a system of 32 cells with a cell radius of 1.6 km, a total of 32 cells, a total frequency bandwidth that supports 336 traffic channels, and a reuse factor of N = 7. If there are 32 total cells, what geographic area is covered, how many channels are there per cell, and what is the total number of concurrent calls that can be handled? Repeat for a cell radius of 0.8 km and 128 cells.

Stallings DCC9e Figure 14.4a shows an approximately square pattern. A hexagon of radius 1.6 km has an area of 6.65 km2, and the total area covered is 6.65 × 32 = 213 km2. For N = 7, the number of channels per cell is 336/7 = 48, for a total channel capacity of 48 × 32 = 1536 channels. For the layout of Figure 14.4b, the area covered is 1.66 × 128 = 213 km2. The number of channels per cell is 336/7 = 48, for a total channel capacity of 48 × 128 = 6144 channels.



The use of a cellular system is fully automated and requires no action on the part of the user other than placing or answering a call. Two types of channels are available between the mobile unit and the base station (BS): control channels and traffic channels. **Control channels** are used to exchange information having to do with setting up and maintaining calls and with establishing a relationship between a mobile unit and the nearest BS. **Traffic channels** carry a voice or data connection between users.

Wireless Network Generations

Technol ogy	1G	2G	2. 5G	3G	4G
Design began	1970	1980	1985	1990	2000
Implementation	1984	1991	1999	2002	2012
Services	Analog voice	Digital voice	Higher capacity packetized data	Higher capacity, broadband	Completely IP based
Data rate	1.9. kbps	14.4 kbps	384 kbps	2 Mbps	200 Mbps
Multiplexing	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	OFDMA, SC-FDMA
Core network	PSTN	PSTN	PSTN, packet network	Packet network	IP backbone

Since their introduction in the mid-1980s, cellular networks have evolved rapidly.

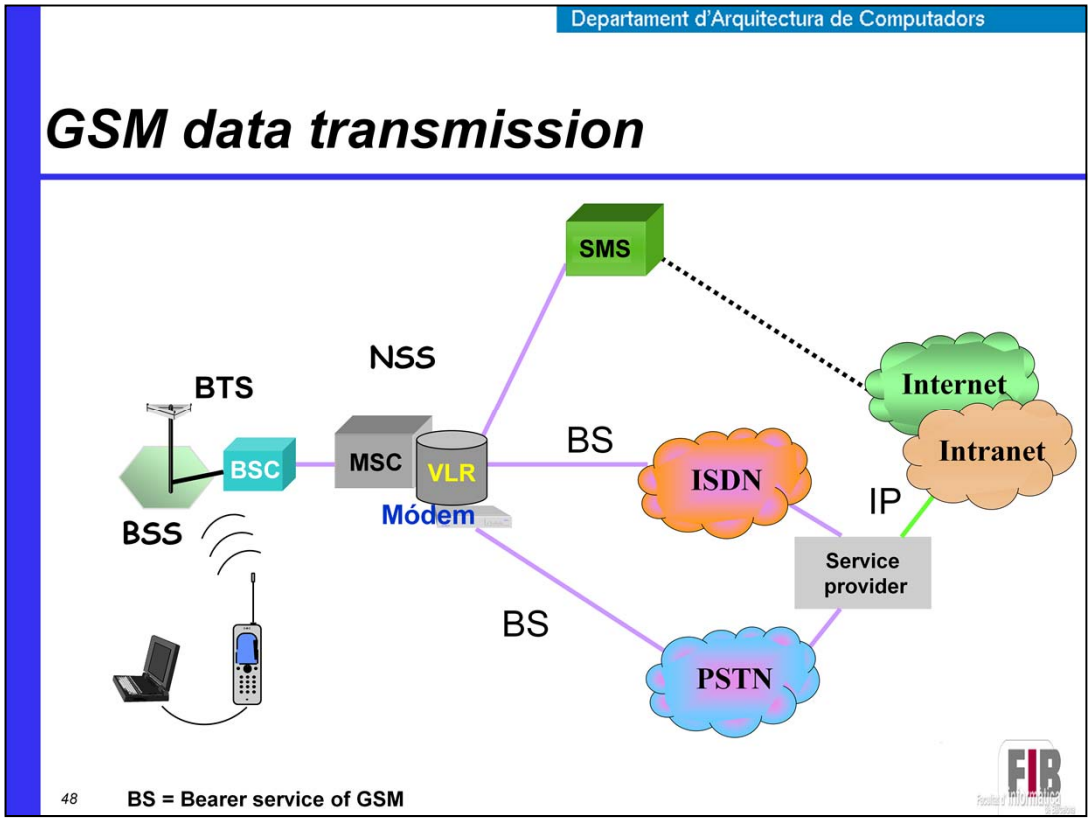
For convenience, industry and standards bodies group the technical advances into

"generations." We are now up to the fourth generation (4G) of cellular network

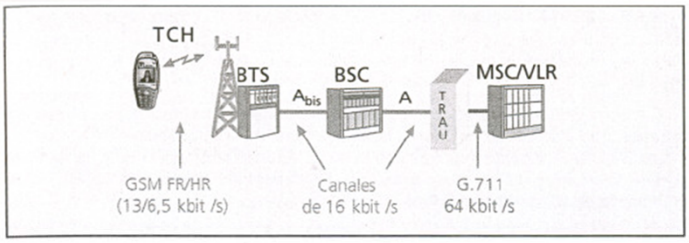
technology. In this section, we give a brief overview of the first three generations.

The following section is devoted to 4G.

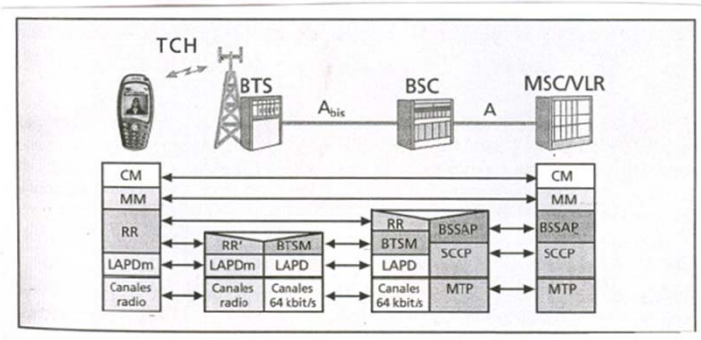
Table 10.1 lists some of the key characteristics of the cellular network generations.


Departament d'Arquitectura de Computadors
GSM data transmission
SMS
NSS
Internet
BTS
Intranet
BS
BSC
MSC
VLR
ISDN
IP
Módem
BSS
Service provider
BS
PSTN
48
BS = Bearer service of GSM

GSM



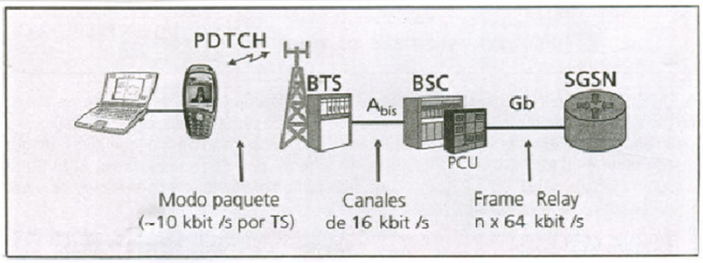
Voice transport GSM



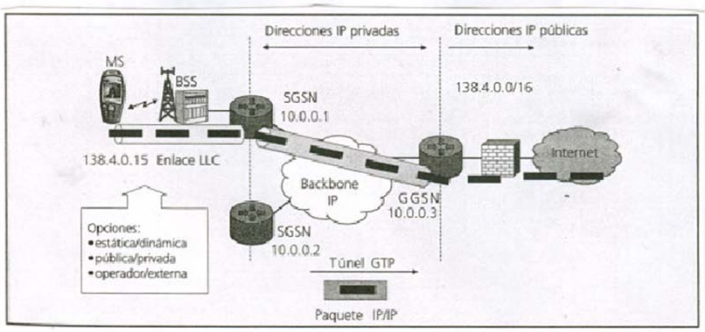
Signaling architecture GSM access network

49

GPRS

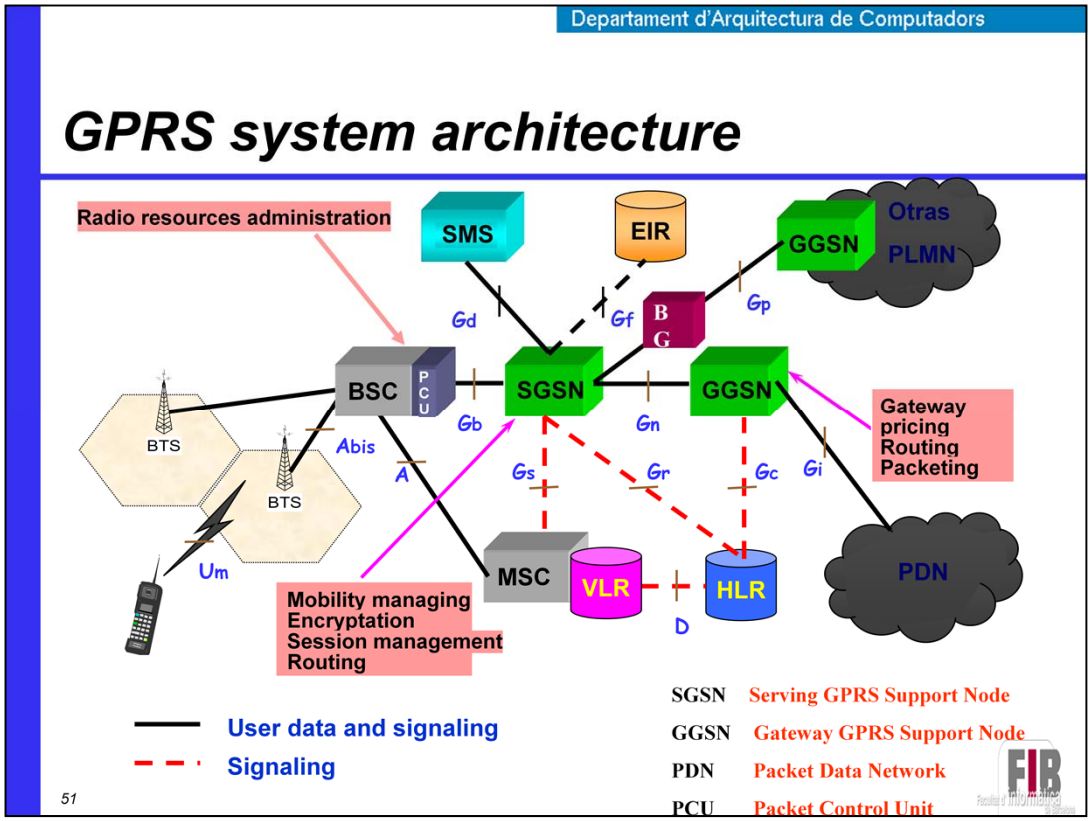


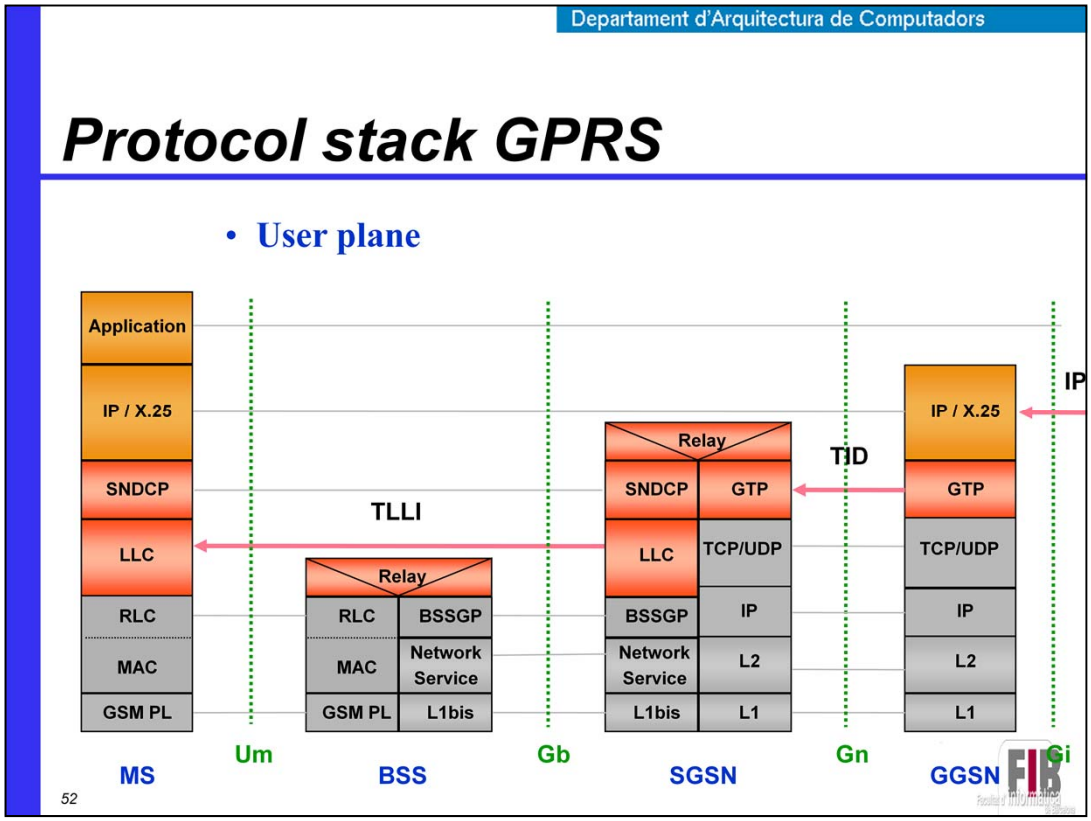
Data transport



Tunneling

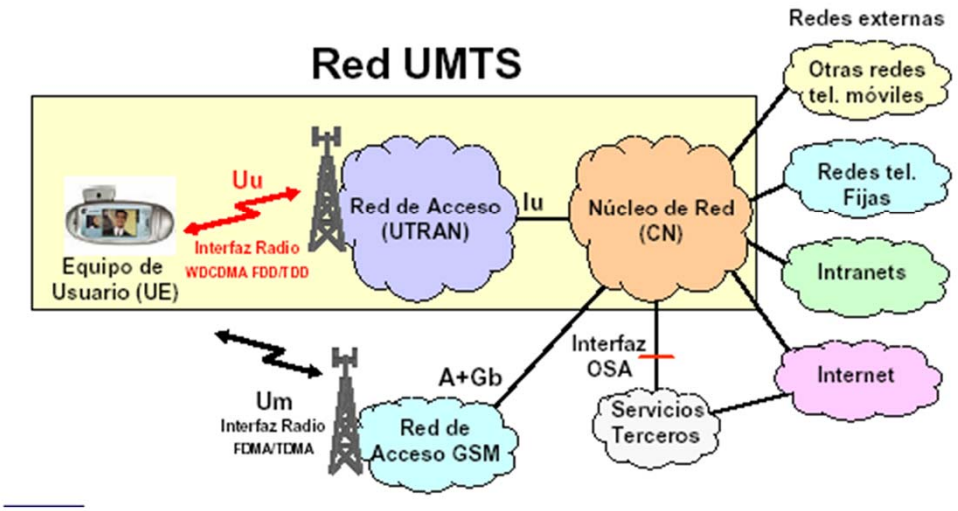
50


Departament d'Arquitectura de Computadors
GPRS system architecture
Radio resources administration
SMS
EIR
GGSN
Otras
PLMN
Gd
Gf
B
G
Gp
BSC
P
C
U
SGSN
GGSN
Gateway
pricing
Routing
Packeting
BTS
BTS
Abis
A
Gb
Gn
Gs
Gr
Gc
Gi
Um
MSC
VLR
HLR
D
PDN
Mobility managing
Encryptation
Session management
Routing
User data and signaling
Signaling
SGSN Serving GPRS Support Node
GGSN Gateway GPRS Support Node
PDN Packet Data Network
PCU Packet Control Unit
51


Departament d'Arquitectura de Computadors
Protocol stack GPRS
• User plane
Application
IP / X.25
SNDCP
LLC
RLC
MAC
GSM PL
TLLI
Relay
RLC
BSSGP
MAC
Network Service
GSM PL
L1bis
Relay
SNDCP
GTP
LLC
TCP/UDP
BSSGP
IP
Network Service
L2
L1bis
L1
TID
IP / X.25
GTP
TCP/UDP
IP
L2
L1
IP
MS
Um
BSS
Gb
SGSN
Gn
GGSN
Gi
52

Departament d'Arquitectura de Computadors

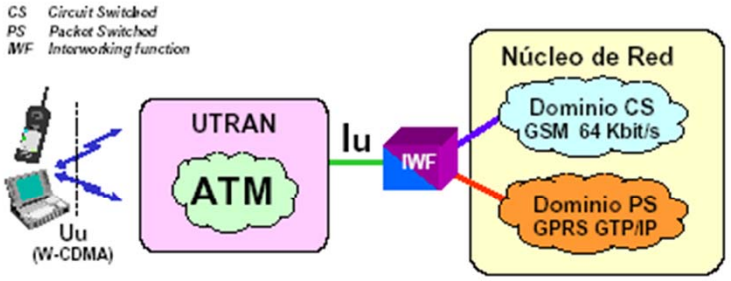
UMTS architecture



53

Departament d'Arquitectura de Computadors

UMTS switching

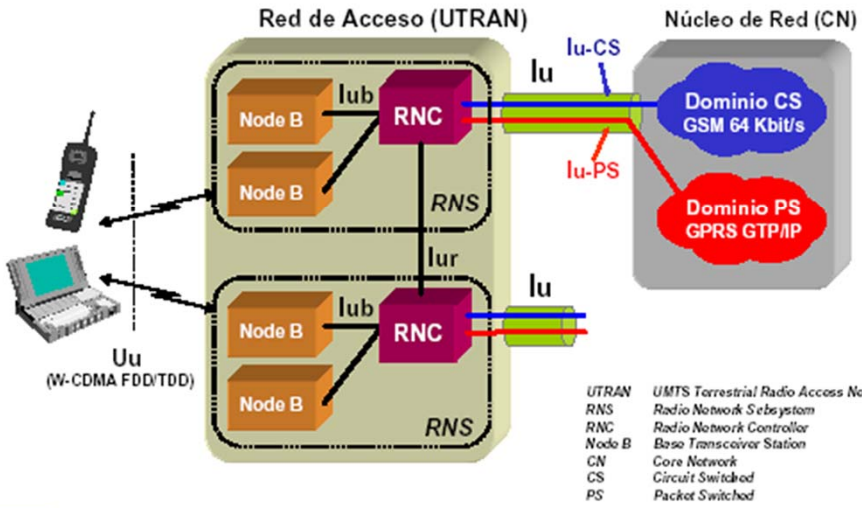


- Interfaz radio (Uu) WCDMA FDD/TDD
- Red de acceso radio basada en ATM / Ethernet
- Núcleo de red basado en GSM/GPRS
  - Reutilización de infraestructura disponible
  - Necesidad de adaptación en el interfaz Iu

54

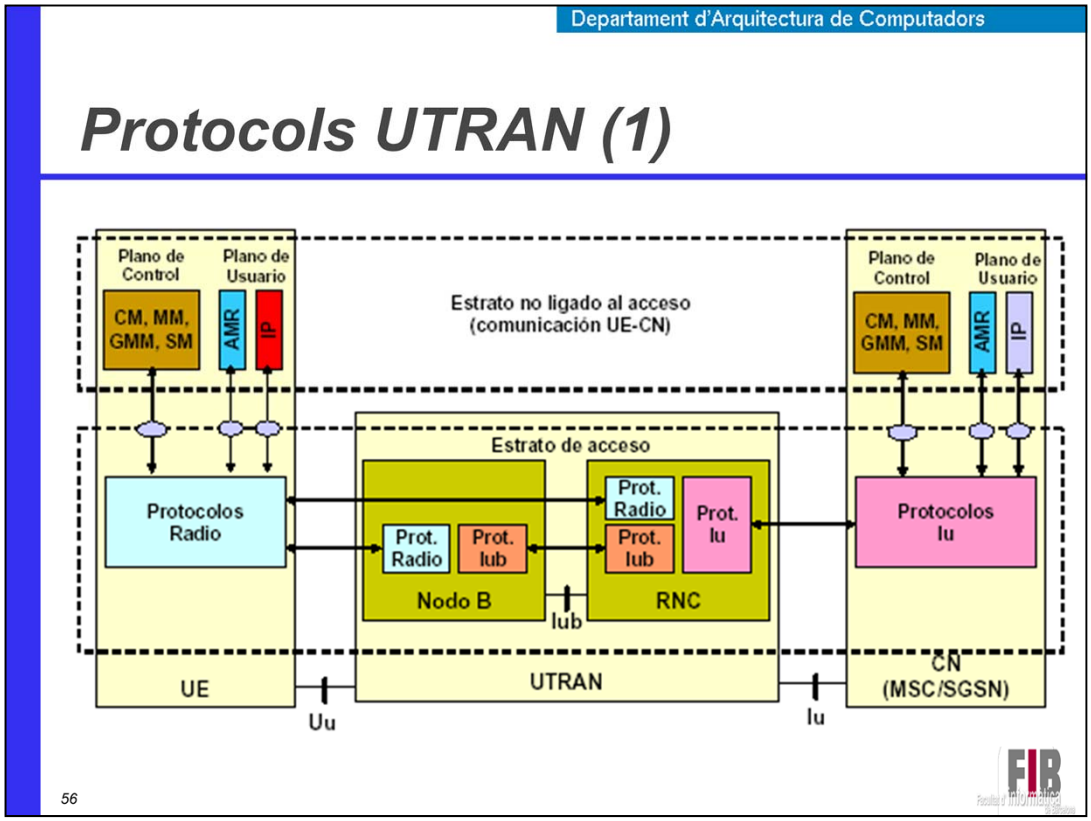
Departament d'Arquitectura de Computadors

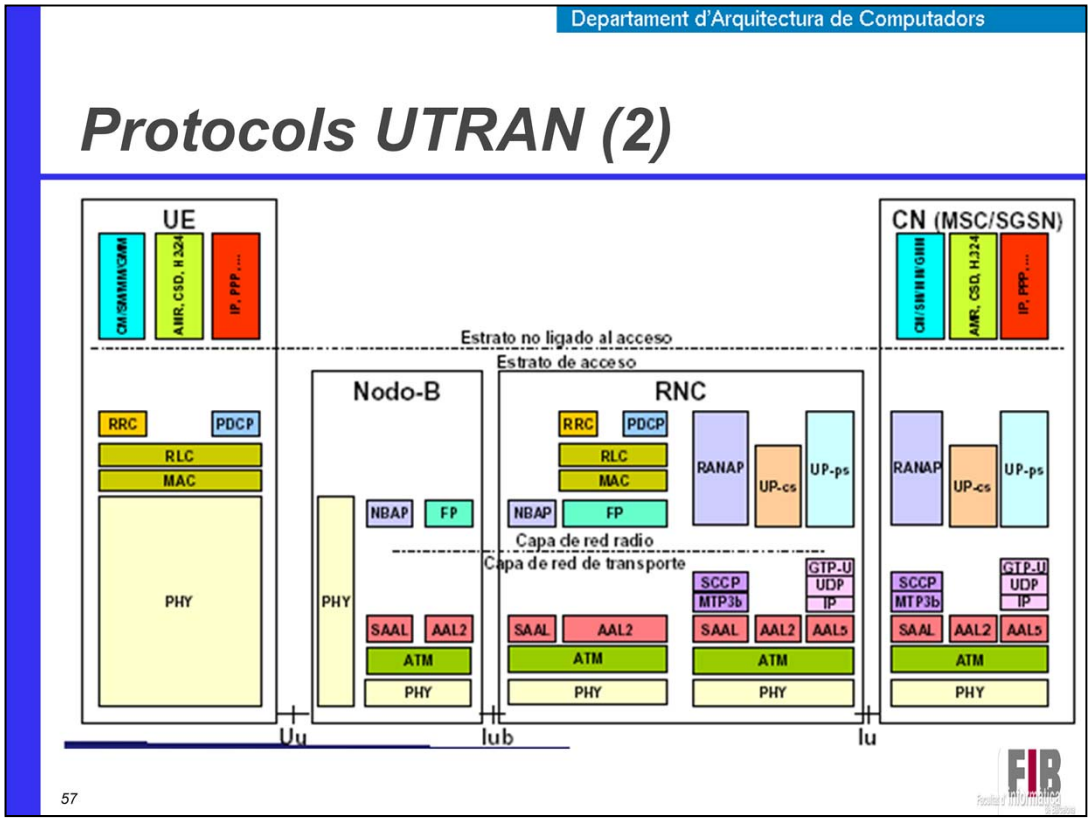
Access network



UTRAN	UMTS Terrestrial Radio Access Network
RNS	Radio Network Subsystem
RNC	Radio Network Controller
Node B	Base Transceiver Station
CN	Core Network
CS	Circuit Switched
PS	Packet Switched

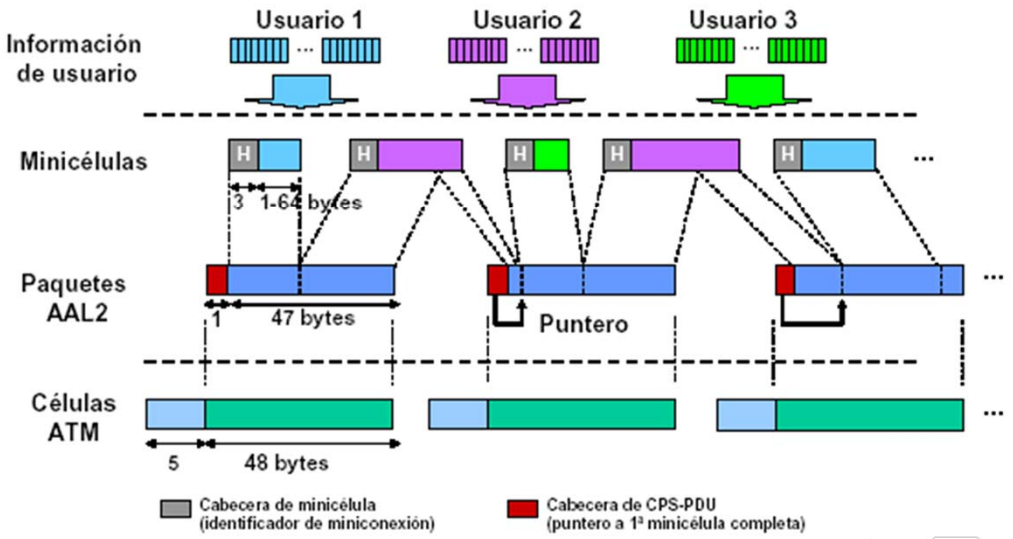
55


Departament d'Arquitectura de Computadors
Protocols UTRAN (1)
Plano de Control
Plano de Usuario
CM, MM, GMM, SM
AMR
IP
Estrato no ligado al acceso (comunicación UE-CN)
Estrato de acceso
Protocolos Radio
Prot. Radio
Prot. Iub
Prot. Iu
Nodo B
RNC
Iub
UE
UTRAN
CN (MSC/SGSN)
Uu
Iu
56


Departament d'Arquitectura de Computadors
Protocols UTRAN (2)
UE
CM/SM/MM/GMM
AMR, CSD, H.324
IP, PPP, ...
CN (MSC/SGSN)
CM/SM/MM/GMM
AMR, CSD, H.324
IP, PPP, ...
Estrato no ligado al acceso
Estrato de acceso
Nodo-B
RNC
RRC
PDCP
RLC
MAC
PHY
NBAP
FP
RANAP
UP-cs
UP-ps
Capa de red radio
Capa de red de transporte
SCCP
MTP3b
GTP-U
UDP
IP
SAAL
AAL2
AAL5
ATM
Uu
Iub
Iu
57

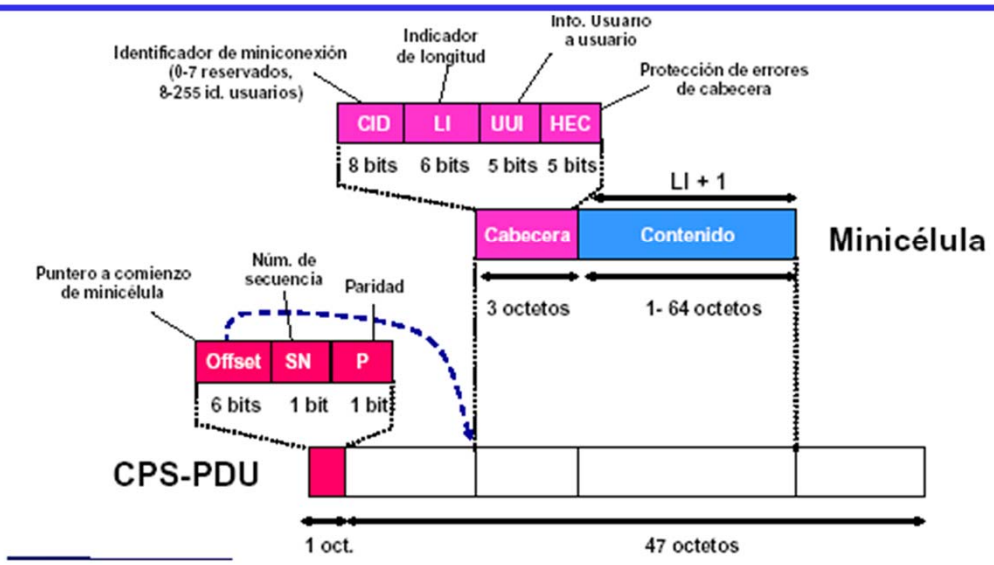
Departament d'Arquitectura de Computadors

Protocol AAL2



58

AAL2 header

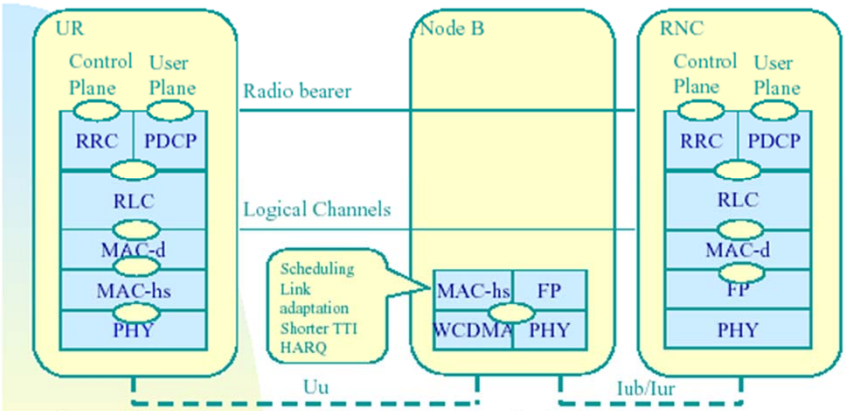


59

HSPA (High Speed Packet Access)

- In order to improve the packet data performance, the UMTS systems have been enhanced with HSPA.
- HSPA consists of two components, HSDPA and HSUPA:
- In the DL a new shared transport channel, the HS-DSCH
  - It allows to assign all available resource to one or more users in an efficient manner.
  - HS-DSCH does no adjust to transmission power for each user, but rather adapts the rate to match the current channel conditions.
- In the UL dedicated channels have been enhanced: E-DCHs
  - Even though the UL channels are dedicated, the UL resources can be shared between users in an efficient manner.

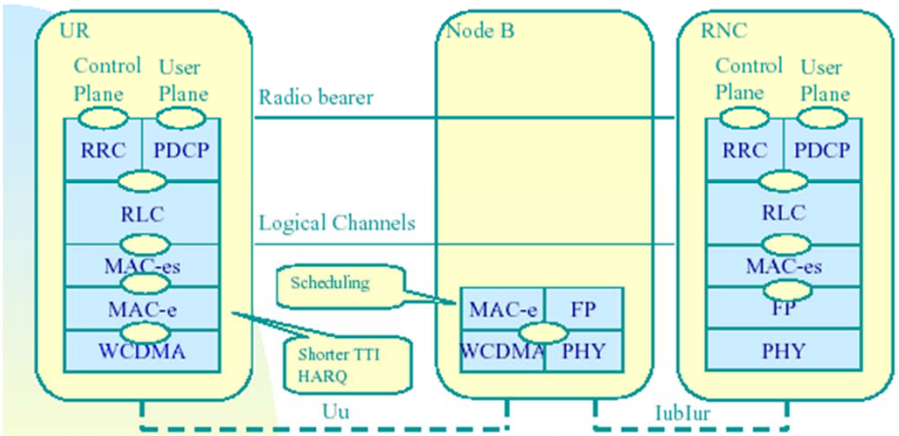
HSDPA: Protocol architecture



- Most of the features of HSDPA are implemented in the Node B:
  - Physical layer implementation
  - MAC-hs implements the HARQ protocol, making scheduling decisions as well as for the fast link adaptation.

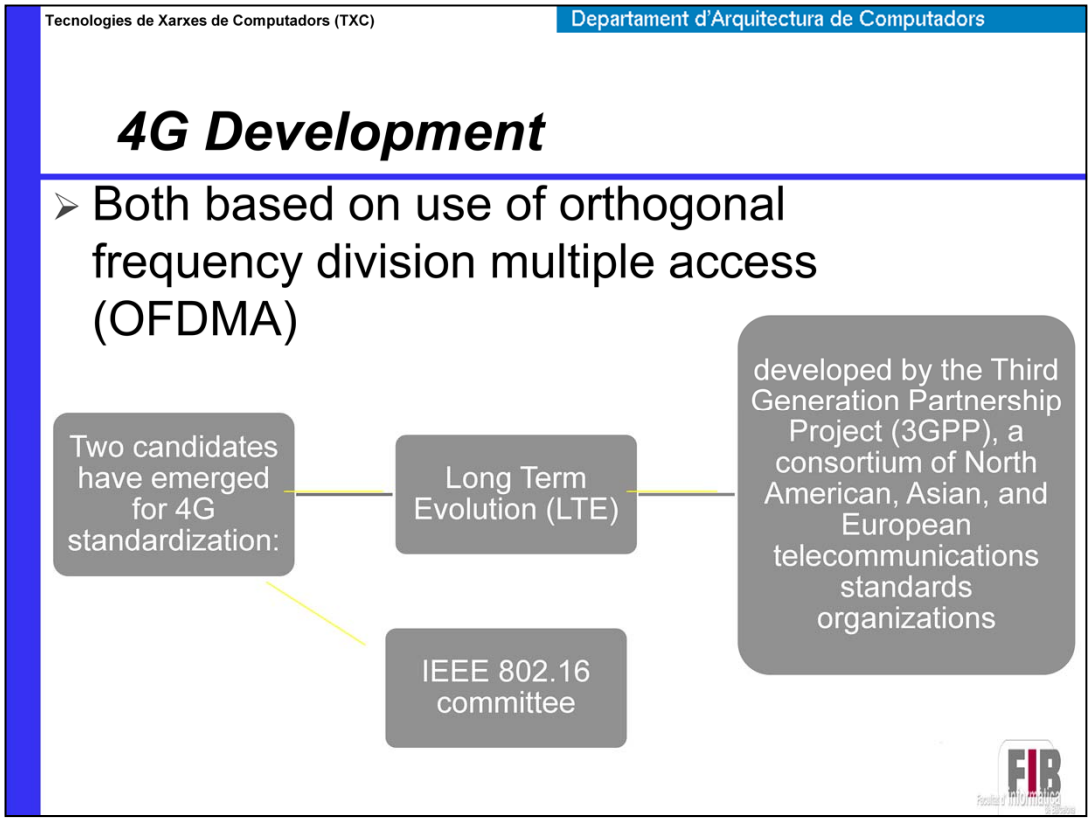
61

HSUPA: Protocol architecture



- Most of the features of HSUPA are implemented in the Node B:
  - Physical layer implementation
  - MAC-e implements the HARQ protocol, making scheduling decisions aw well as for the fast link adaptation.

62



Two candidates have emerged for 4G standardization. One is known as Long Term Evolution (LTE), which has been developed by the Third Generation Partnership Project (3GPP), a consortium of Asian, European, and North American telecommunications standards organizations. The other effort is being made by the IEEE 802.16 committee, which has developed standards for high-speed fixed wireless operations known as WiMax. The committee has specified an enhancement of WiMax to meet 4G needs. The two efforts are similar both in terms of performance and technology. Both are based on the use of orthogonal frequency division multiple access (OFDMA) to support multiple access to network resources. WiMax uses a pure OFDMA approach of both uplink and downlink. LTE uses pure OFDMA on the downlink but a technique that is based on OFDMA but that offers enhanced power efficiency. It appears likely that LTE will become the universal standard for 4G wireless.

6.1.2.6.2 Type 4 Logical Upstreams[29]

Type 4 Logical Upstreams are identified by UCD Type 35 and may additionally have UCD Type 29. The presence of UCD Type 29 allows use of these logical upstream channels by DOCSIS 2.0 CMs. If the UCD Type 29 is not present, the channel is restricted to use by DOCSIS 3.0 CMs only.

This channel type allows the operator to define burst profiles for five data IUCs (5, 6, 9, 10 and 11) for use by DOCSIS 3.0 CMs. The CMTS is free to select, using proprietary criteria, the most appropriate data IUC for each data burst for 3.0 CMs operating in Multiple Transmit Channel Mode. If UCD Type 29 is present, the operator should configure IUCs 9 and 10 to be appropriate for short and long data bursts for DOCSIS 2.0 CMs.

Additionally, Type 4SR logical upstreams allow the use of Selectable Active Codes Mode 2 and Code Hopping Mode 2 (see Section 6.4.3 and [DOCSIS PHY]).

6.1.3 Future Use

A number of fields are defined as being "for future use" or Reserved in the various MAC frames described in this document. These fields will not be interpreted or used in any manner by this version (3.0) of the MAC protocol.

The CMTS MUST transmit all Reserved or "for future use" fields as zero. The CM MUST silently ignore all Reserved or "for future use" fields.

The CM MUST transmit all Reserved or "for future use" fields as zero. The CMTS MUST silently ignore all Reserved or "for future use" fields.

6.2 MAC Frame Formats

6.2.1 Generic MAC Frame Format

A MAC frame is the basic unit of transfer between MAC sublayers at the CMTS and the cable modem. The same basic structure is used in both the upstream and downstream directions. MAC frames are variable in length. The term "frame" is used in this context to indicate a unit of information that is passed between MAC sublayer peers. This is not to be confused with the term "framing" that indicates some fixed timing relationship.

There are three distinct regions to consider, as shown in Figure 6–1. Preceding the MAC frame is either PMD sublayer overhead (upstream) or an MPEG transmission convergence header (downstream). The first part of the MAC frame is the MAC Header. The MAC Header uniquely identifies the contents of the MAC frame. Following the header is the optional Data PDU region. The format of the Data PDU and whether it is even present is described in the MAC Header.

[29] Section modified per MULPIv3.0-N-08.0629-3 on 5/1/08 by KN.

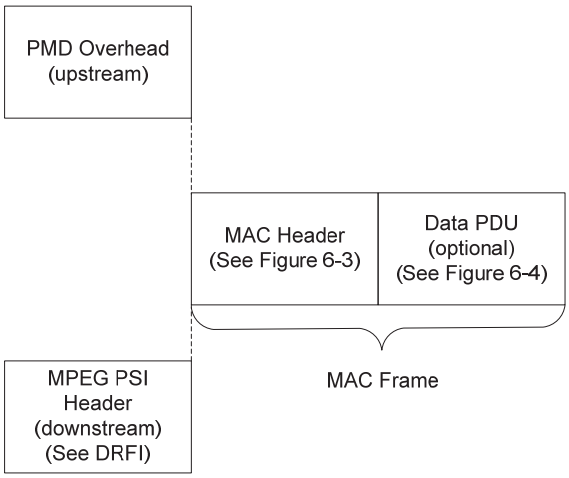


Figure 6–1 - Generic MAC Frame Format

6.2.1.1 PMD Overhead

In the upstream direction, the PHY layer indicates the start of the MAC frame to the MAC sublayer. From the MAC sublayer's perspective, it only needs to know the total amount of overhead so it can account for it in the Bandwidth Allocation process. More information on this may be found in the PMD Sublayer section of [DOCSIS DRFI].

The FEC overhead is spread throughout the MAC frame and is assumed to be transparent to the MAC data stream. The MAC sublayer does need to be able to account for the overhead when doing Bandwidth Allocation. More information on this may be found in the Upstream Bandwidth Allocation section of this document (refer to Section 7.2.1).

6.2.1.2 MAC Frame Transport

The transport of MAC frames by the PMD sublayer for upstream channels is shown in Figure 6–2.

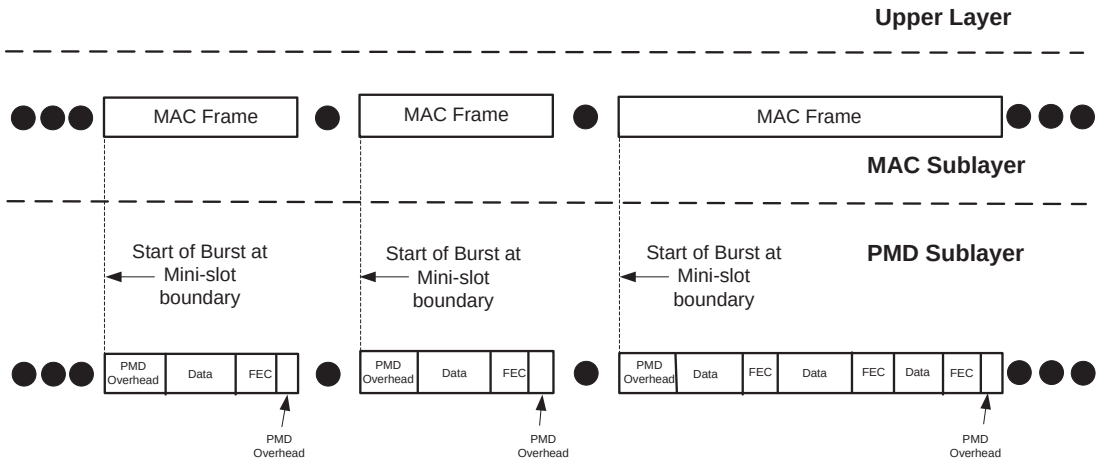


Figure 6–2 - Upstream MAC/PMD Convergence

The layering of MAC frames over MPEG in the downstream channel is described in [DOCSIS DRFI].

Note that the CMTS PHY ensures that, for a given channel, the CMTS MAC receives upstream MAC frames in the same order the CM mapped the MAC frames onto mini-slots. That is to say that if MAC frame X begins in mini-slot n and MAC frame Y begins in mini-slot n+m, then the CMTS MAC will receive X before it receives Y. This is true even when, as is possible with S-CDMA, mini-slots n and n+m are actually simultaneously transmitted within the PHY layer.

6.2.1.3 Ordering of Bits and Octets[30]

Within an octet, the least-significant bit is the first transmitted on the wire. This follows the convention used by Ethernet and [ISO/IEC 8802-3]. This is often called bit-little-endian order.

This applies to the upstream channel only. For the downstream channel, the MPEG transmission convergence sublayer presents an octet-wide interface to the MAC, so the MAC sublayer does not define the bit order.

Within the MAC layer, when numeric quantities are represented by more than one octet (i.e., 16-bit and 32-bit values), the octet containing the most-significant bits is the first transmitted on the wire. This is sometimes called byte-big-endian order.

This specification uses the following textual conventions:

- When tables describe bit fields within an octet, the most significant bits are topmost in the table. For example, in Table 6–2, FC_TYPE occupies the two most-significant bits and EHDR_ON occupies the least-significant bit.
- When figures depict bit positions within an octet, the most significant bits are leftmost in the figure. For example, see the locations of the FC_TYPE and EHDR_ON bits in Figure 6–3.
- When bit-strings are presented in text, the most significant bit is leftmost in the string.
- Unless explicitly indicated otherwise, when bits are enumerated in a bit-field, the least significant bit of the bit-field is bit # 0. The exceptions are certain fields that utilize the BITS Encoding convention.
- When message formats are presented in figures, the message octets are shown in the order in which they are transmitted on the wire, beginning with the field in the upper left and reading left-to-right, one row at a time. For example, in Figure 6–13, the FC byte is transmitted first, followed by the MAC PARM and LEN fields. As mentioned above, the LEN field is transmitted with most-significant octet first, and each octet is transmitted with least-significant bit first.

6.2.1.3.1 Representing Negative Numbers

Signed integer values MUST be transmitted and received by the CM and CMTS in two's complement format.

6.2.1.3.2 Type-Length-Value Fields[31]

Many MAC messages incorporate Type-Length-Value (TLV) fields. Except for the cases of Primary Service Flow selection and MIC calculation among the TLVs encoded in a CM Configuration File, TLV fields are unordered lists of TLV-tuples. Some TLVs are nested (see Annex C). The CM or CMTS MUST set all TLV Length fields, except for EH_LEN (see Section 6.2.5), to be greater than zero. Unless otherwise specified, Type is one byte and Length is one byte.

Using this encoding, new parameters may be added which some devices cannot interpret. A CM or CMTS which does not recognize a parameter type MUST skip over this parameter and not treat the event as an error condition.

[30] Section modified per MULPIv3.0-N-07.0544-2 on 10/31/07 by KN.
[31] Modified per MULPIv3.0-N-08.0687-3 on 1/6/09 by JS.

6.2.1.4 MAC Header Format

The CM or CMTS MUST use the MAC Header format as shown in Figure 6–3.

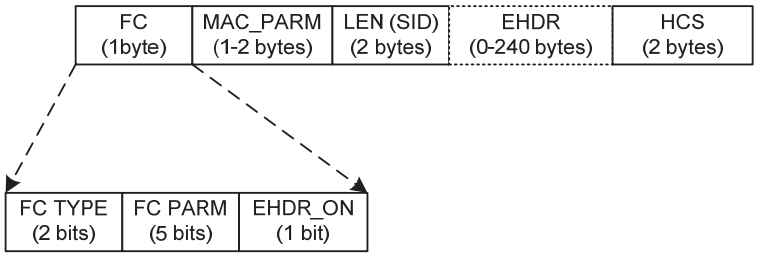


Figure 6–3 - MAC Header Format

The CM MUST comply with Table 6–1 for all MAC Headers. The CMTS MUST comply with Table 6–1 for all MAC Headers. The Frame Control (FC) field is the first byte and uniquely identifies the rest of the contents within the MAC Header. The FC field is followed by 3 bytes of MAC control; an optional Extended Header field (EHDR); plus a Header Check Sequence (HCS) to ensure the integrity of the MAC Header.

Table 6–1 - Generic MAC Header Format

MAC Header Field	Usage	Size
FC	Frame Control: Identifies type of MAC Header	8 bits
MAC_PARM	Parameter field whose use is dependent on FC: if EHDR_ON=1; used for EHDR field length (ELEN) else if for concatenated frames (see Table 6–10) used for MAC frame count else (for Requests only) indicates the number of mini-slots requested	8 bits for all headers except for the Queue-Depth based request header in which this field is 16 bits.
LEN (SID)	The length of the MAC frame. The length is defined to be the sum of the number of bytes in the extended header (if present) and the number of bytes following the HCS field. (For a REQ Header, this field is the Service ID instead).	16 bits
EHDR	Extended MAC Header (where present; variable size).	0-240 bytes
HCS	MAC Header Check Sequence	2 bytes
	Length of a MAC Header	6 bytes + EHDR

FC Field: The FC field is broken down into the FC_TYPE sub-field, FC_PARM sub-field and an EHDR_ON indication flag. The CM MUST comply with the FC field in Table 6–2. The CMTS MUST comply with the FC field in Table 6–2 for the FC field.

Table 6–2 - FC Field Format

FC Field	Usage	Size
FC_TYPE	MAC Frame Control Type field: 00: Packet PDU MAC Header 01: ATM PDU MAC Header 10: Isolation Packet PDU MAC Header 11: MAC Specific Header	2 bits
FC_PARM	Parameter bits, use dependent on FC_TYPE.	5 bits
EHDR_ON	When = 1, indicates that EHDR field is present. [Length of EHDR (ELEN) determined by MAC_PARM field]	1 bit

The FC_TYPE sub-field includes the two MSBs of the FC field. These bits MUST always be interpreted by CMs and CMTSs in the same manner to indicate one of four possible MAC frame formats. These types include: MAC Header with Packet PDU; MAC Header with ATM cells; MAC Header with packet PDU Isolation from Pre-3.0 DOCSIS cable modems; or a MAC Header used for specific MAC control purposes. These types are spelled out in more detail in the remainder of this section.

The five bits following the FC_TYPE sub-field is the FC_PARM sub-field. The use of these bits is dependent on the type of MAC Header. The LSB of the FC field is the EHDR_ON indicator. If this bit is set, then an Extended Header (EHDR) is present. The EHDR provides a mechanism to allow the MAC Header to be extensible in an inter-operable manner.

Note that the Transmission Convergence Sublayer stuff-byte pattern is defined to be a value of 0xFF, which precludes the use of FC byte values which have FC_TYPE = ‘11’ and FC_PARM = ‘11111’.

MAC_PARM: The MAC_PARM field of the MAC Header serves several purposes depending on the FC field. If the EHDR_ON indicator is set, then the MAC_PARM field MUST be used by the CM and CMTS as the Extended Header length (ELEN). The EHDR field may vary from 0 to 240 bytes. If this is a concatenation MAC Header, then the MAC_PARM field represents the number of MAC frames (CNT) in the concatenation (see Section 6.2.5.6). If this is a Request MAC Header (REQ), (see Section 6.2.4.3), then the MAC_PARM field represents the amount of bandwidth being requested. In all other cases, the MAC_PARM field is reserved for future use.

LEN (SID): The third field has two possible uses. In most cases, it indicates the length (LEN) of this MAC frame. In one special case, the Request MAC Header, it is used to indicate the cable modem’s Service ID since no PDU follows the MAC Header.

EHDR: The Extended Header (EHDR) field provides extensions to the MAC frame format. It is used to implement data link security as well as frame fragmentation, and can be extended to add support for additional functions in future releases.

HCS: The HCS field is a 16-bit CRC that ensures the integrity of the MAC Header, even in a collision environment. The CM or CMTS MUST include the entire MAC Header, starting with the FC field and including any EHDR field that may be present for HCS field coverage. The HCS is calculated using CRC-CCITT (x16 + x12 + x5 + 1) as defined in [ITU-T X.25].

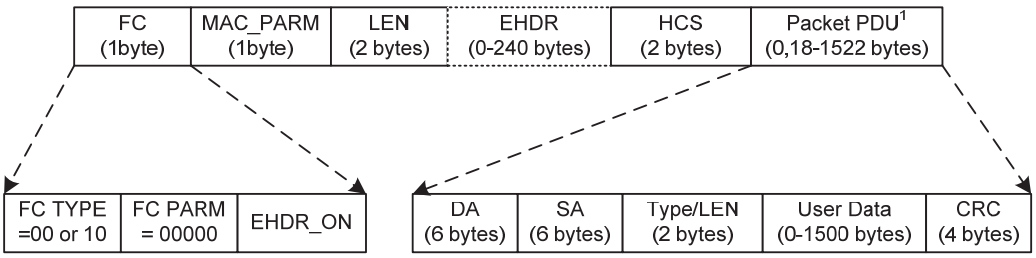
6.2.1.5 Data PDU

The MAC Header may be followed by a Data PDU. The type and format of the Data PDU is defined in the Frame Control field of the MAC Header. The FC field explicitly defines a Packet Data PDU, an ATM Data PDU, an Isolation Packet Data PDU, and a MAC-Specific Frame. All CMs MUST use the length in the MAC Header to skip over any reserved data.

6.2.2 Packet-Based MAC Frames

6.2.2.1 Packet PDU and Isolation Packet PDU

The CM or CMTS MAC sublayer MUST support both, a variable-length Ethernet/[ISO/IEC 8802-3]-type Packet Data PDU MAC Frame and a variable-length Ethernet/[ISO/IEC 8802-3]-type Isolation Packet Data PDU MAC Frame. The Isolation Packet Data PDU MAC Frame is used to prevent certain downstream packets from being received and forwarded by Pre-3.0 DOCSIS cable modems, as described in Section 9.2.2.2.1.[32] Both the Packet PDU and the Isolation Packet PDU can be used to send packets of any type (unicast, multicast, and broadcast). With the exception of packets which have been subject to Payload Header suppression, the Packet PDU MUST be passed across the network in its entirety, including its original CRC. In the case where Payload Header Suppression has been applied to the Packet PDU, all bytes except those suppressed MUST be passed across the network by the CM and CMTS, and the CRC covers only those bytes actually transmitted (refer to Section 6.2.5.4.1). A unique Packet MAC Header is appended to the beginning. The CM MUST comply with Figure 6–4 and Table 6–3 for Packet PDUs and Isolation Packet PDUs. The CMTS MUST comply with Figure 6–4 and Table 6–3 for Packet PDUs and Isolation Packet PDUs.



[1] Packet PDU length is limited to 1518 bytes in the absence of VLAN tagging. When PHS is applied, it is possible for the Packet PDU length to be less than 18 bytes.

Figure 6–4 - Packet PDU or Isolation Packet PDU MAC Frame Format

Table 6–3 - Packet PDU or Isolation Packet PDU MAC Frame Format

Field	Usage	Size
FC	FC_TYPE = 00; Packet PDU MAC Header FC_TYPE = 10; Isolation Packet PDU MAC Header FC_PARM[4:0] = 00000; other values reserved for future use and ignored EHDR_ON = 0 if there is no extended header, 1 if there is an EHDR	8 bits
MAC_PARM	MAC_PARM = x; MUST be set to zero if there is no EHDR; Otherwise set to length of EHDR	8 bits
LEN	LEN = n+x; length of Packet PDU in bytes + length of EHDR	16 bits
EHDR	Extended MAC Header, if present	x (0-240) bytes

[32] Modified per MULPIv3.0-N-06.0371-4 by KN on 1/26/07.

Field	Usage	Size
HCS	MAC Header Check Sequence	16 bits
Packet Data Packet PDU:	DA - 48 bit Destination Address SA - 48 bit Source Address Type/Len - 16 bit Ethernet Type or [ISO/IEC 8802-3] Length Field User Data (variable length, 0-1500 bytes) CRC - 32-bit CRC over packet PDU (as defined in Ethernet/[ISO/IEC 8802-3])	n bytes
	Length of Packet PDU or Isolation Packet PDU MAC frame	6 + x + n bytes

Under certain circumstances it may be necessary to transmit a packet PDU MAC frame without an actual PDU. This is done so that the extended header can be used to carry certain information about the state of the service flow, e.g., a 5-byte Downstream Service Extended Header containing the current Sequence Number for a particular DSID (also known as a "null packet"), or a Service Flow Extended Header containing the number of active grants for a UGS-AD service flow. This could also happen as a result of PHS in the upstream direction (see PHS Section 6.2.5.4.1).[33]

Such a frame will have the length field in the MAC header set to the length of the extended header and will have no packet data, and therefore no CRC.

6.2.3 ATM Cell MAC Frames

The FC_TYPE 0x01 is reserved for future definition of ATM Cell MAC Frames. This FC_TYPE field in the MAC Header indicates that an ATM PDU is present. This PDU MUST be silently discarded by CMs and CMTSs compliant with this version (3.0) of the specification. Compliant version 3.0 CM and CMTS implementations MUST use the length field to skip over the ATM PDU.

6.2.4 MAC-Specific Headers

There are several MAC Headers which are used for very specific functions. These functions include support for downstream timing and upstream ranging/power adjustment, requesting bandwidth, fragmentation and concatenating multiple MAC frames.

Table 6–4 describes FC_PARM usage within the MAC Specific Header.

Table 6–4 - MAC-Specific Headers and Frames

FC_PARM	Header/Frame Type
00000	Timing Header
00001	MAC Management Header
00010	Request Frame
00011	Fragmentation Header
00100	Queue Depth-based Request Frame
11100	Concatenation Header

[33] This paragraph and next modified per MULPIv3.0-N-08.0694-4 on 1/6/09 by JS.

6.2.4.1 Timing Header

A specific MAC Header is identified to help support the timing and adjustments required. In the downstream, this MAC Header MUST be used by the CMTS to transport the Global Timing Reference to which all cable modems synchronize. In the upstream, this MAC Header MUST be used by the CM as part of the Ranging message needed for a cable modem's timing and power adjustments. The Timing MAC Header is followed by a Packet Data PDU. The CM MUST comply with Figure 6–5 and Table 6–5 for Timing Headers. The CMTS MUST comply with Figure 6–5 and Table 6–5 for Timing Headers.

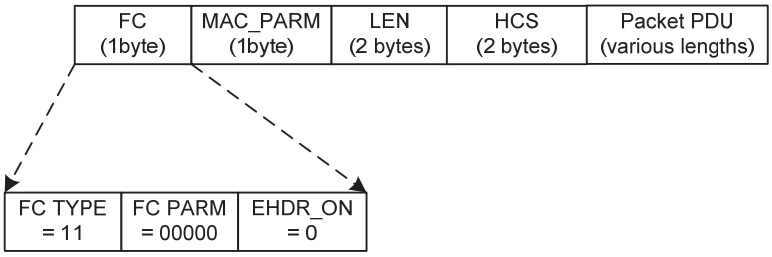


Figure 6–5 - Timing MAC Header

Table 6–5 - Timing MAC Header Format

Field	Usage	Size
FC	FC_TYPE = 11; MAC Specific Header FC_PARM[4:0] = 00000; Timing MAC Header EHDR_ON = 0; Extended header prohibited for SYNC and RNG-REQ	8 bits
MAC_PARM	Reserved for future use	8 bits
LEN	LEN = n; Length of Packet PDU in bytes	16 bits
EHDR	Extended MAC Header not present	0 bytes
HCS	MAC Header Check Sequence	2 bytes
Packet Data	MAC Management Message: SYNC message (downstream only) RNG-REQ (upstream only)	n bytes
	Length of Timing Message MAC frame	6 + n bytes

6.2.4.2 MAC Management Header

A specific MAC Header is identified to help support the MAC management messages required. This MAC Header MUST be used by CMs and CMTSs to transport all MAC management messages (refer to Section 6.4). The CM MUST comply with Figure 6–6 and Table 6–6 for MAC Management Headers. The CMTS MUST comply with Figure 6–6 and Table 6–6 for MAC Management Headers.

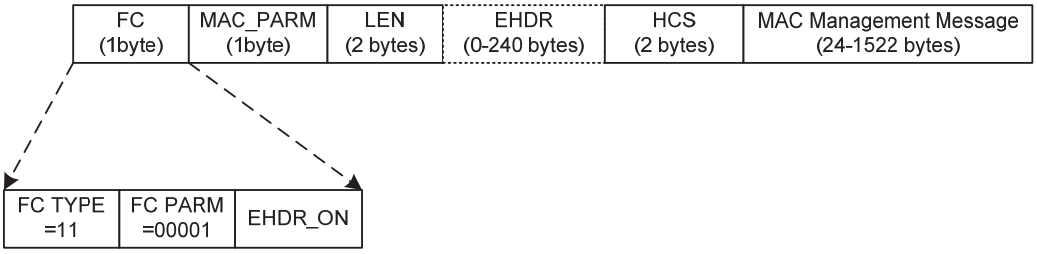


Figure 6–6 - Management MAC Header

Table 6–6 - MAC Management Format

Field	Usage	Size
FC	FC_TYPE = 11; MAC Specific Header FC_PARM[4:0] = 00001; Management MAC Header EHDR_ON = 0 if there is no extended header, 1 if there is an EHDR	8 bits
MAC_PARM	MAC_PARM = x; MUST be set to zero if there is no EHDR; Otherwise set to length of EHDR	8 bits
LEN	LEN = n+x; length of MAC management message + length of EHDR in bytes	16 bits
EHDR	Extended MAC Header, if present	x (0-240) bytes
HCS	MAC Header Check Sequence	16 bits
Packet Data	MAC management message	n bytes
	Length of Packet MAC frame	6 + x + n bytes

6.2.4.3 Request Frame[34]

The Request Frame is the basic mechanism that a cable modem uses to request bandwidth. As such, it is only applicable in the upstream. The CM MUST NOT include any Data PDUs following the Request Frame. The CM MUST comply with Figure 6–7 and Table 6–7 for Request Frames.

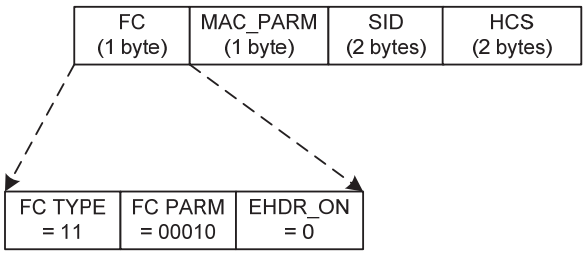


Figure 6–7 - Request Frame Format

Table 6–7 - Request Frame (REQ) Format

Field	Usage	Size
FC	FC_TYPE = 11; MAC-Specific Header FC_PARM[4:0] = 00010; MAC Header only; no data PDU following EHDR_ON = 0; No EHDR allowed	8 bits
MAC_PARM	REQ, total number of mini-slots requested	8 bits
SID	Service ID used for requesting bandwidth. For valid SID ranges, see Section 7.2.1.2.	16 bits
EHDR	Extended MAC Header not allowed	0 bytes
HCS	MAC Header Check Sequence	2 bytes
	Length of a REQ MAC Header	6 bytes

Because the Request Frame does not have a Data PDU following it, the LEN field is not needed. The CM MUST replace the LEN field with a SID. The SID uniquely identifies a particular Service Flow within a given CM.

The CM MUST specify the bandwidth request, REQ, in mini-slots. The CM MUST indicate the current total amount of bandwidth requested for this service queue including appropriate allowance for the PHY overhead in the MAC_PARM field.

The Request Frame is for Pre-3.0 DOCSIS support and MUST NOT be used by CMs operating in Multiple Transmit Channel Mode. CMs operating in Multiple Transmit Channel Mode MUST use queue depth based requests as defined in Section 6.2.4.5.

6.2.4.4 Fragmentation Header

The Fragmentation MAC Header provides the basic mechanism to split a larger MAC PDU into smaller pieces that are transmitted individually and then re-assembled at the CMTS. As such, Fragmentation is only applicable in the upstream. The CM MUST comply with Figure 6–8 and Table 6–8 for Fragmentation MAC Headers.

[34] Revised per MULPIv3.0-N-07.0427-3 by ab on 4/30/07.

A compliant CM MUST support fragmentation. A compliant CMTS MUST support fragmentation. To decrease the burden on the CMTS and to reduce unnecessary overhead, fragmentation headers MUST NOT be used by a CM on unfragmented frames.

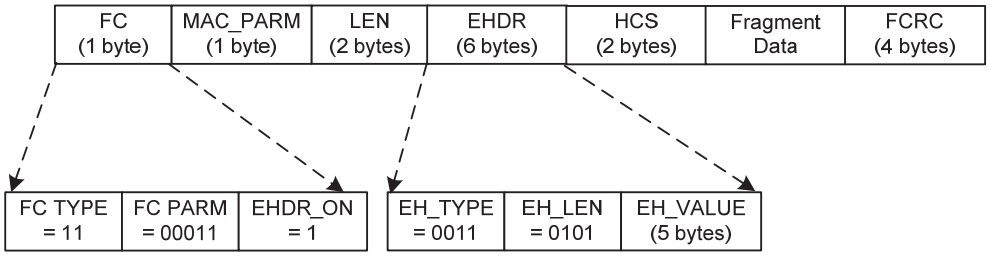


Figure 6–8 - Fragmentation MAC Header Format

Table 6–8 - Fragmentation MAC Frame (FRAG) Format

Field	Usage	Size
FC	FC_TYPE = 11; MAC-Specific Header FC_PARM [4:0] = 00011; Fragmentation MAC Header EHDR_ON = 1; Fragmentation EHDR follows	8 bits
MAC_PARM	ELEN = 6 bytes; length of Fragmentation EHDR	8 bits
LEN	LEN = length of fragment payload + EHDR length + FCRC length	16 bits
EHDR	Refer to Section 6.2.5.3	6 bytes
HCS	MAC Header Check Sequence	2 bytes
Fragment Data	Fragment payload; portion of total MAC PDU being sent	n bytes
FCRC	CRC - 32-bit CRC over Fragment Data payload (as defined in Ethernet/[ISO/IEC 8802-3])	4 bytes
	Length of a MAC Fragment Frame	16 + n bytes

The Fragmentation MAC Frame is for Pre-3.0 DOCSIS support and MUST NOT be used by CMs operating in Multiple Transmit Channel Mode.

6.2.4.5 Queue-depth Based Request Frame

The Queue-depth Based Request Frame is the mechanism that a cable modem uses to request bandwidth in terms of bytes, not including or assuming any physical layer overhead (preamble, FEC, physical layer padding, guard time), which is used when the CM is in Multiple Transmit Channel Mode. This is unlike the Request Frame in which requests are made in units of mini-slots that include physical layer overhead. The Queue-depth Based Request Frame is only applicable in the upstream. The CM MUST NOT include any Data PDUs following the Queue-depth Based Request Frame. The CM MUST comply with Figure 6–9 and Table 6–9 for Queue-depth Based Request Frames.

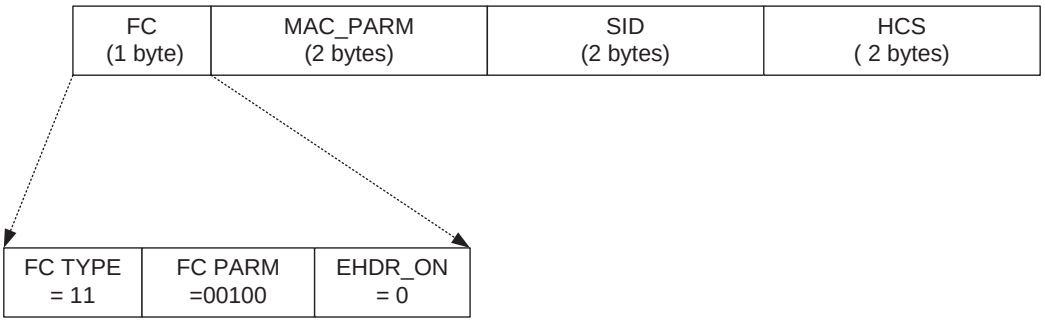


Figure 6–9 - Queue-depth Based Request Frame Format

Table 6–9 - Queue-depth Based Request Frame Format

Field	Usage	Size
FC	FC_TYPE = 11; MAC-Specific Header FC_PARM[4:0] = 00100; MAC Header only; no data PDU following EHDR_ON = 0; No EHDR allowed	1 byte
MAC_PARM	Total number of bytes requested in units of N bytes, where N is a parameter of the service flow for which this request is being made	2 bytes
SID	Service ID (0...0x3DFF)	2 bytes
EHDR	Extended MAC Header not allowed	0 bytes
HCS	MAC Header Check Sequence	2 bytes
	Length of a Queue-depth Based REQ MAC Header	7 bytes

Because the Queue-depth Based Request Frame does not have a Data PDU following it, the LEN field is not needed. The CM MUST replace the LEN field with a SID. The SID uniquely identifies a particular Service Flow within a given CM.

Note: The Queue-depth Based Request Frame is one byte longer than the Pre-3.0 DOCSIS Request Frame.

Queue-depth Based Request Frames MUST NOT be used by CMs operating with Multiple Transmit Channel Mode disabled.

6.2.4.6 Concatenation Header

A Specific MAC Header is defined to allow multiple MAC frames to be concatenated.

The CM MUST comply with Figure 6–10 and Table 6–10 for Concatenation MAC Headers.

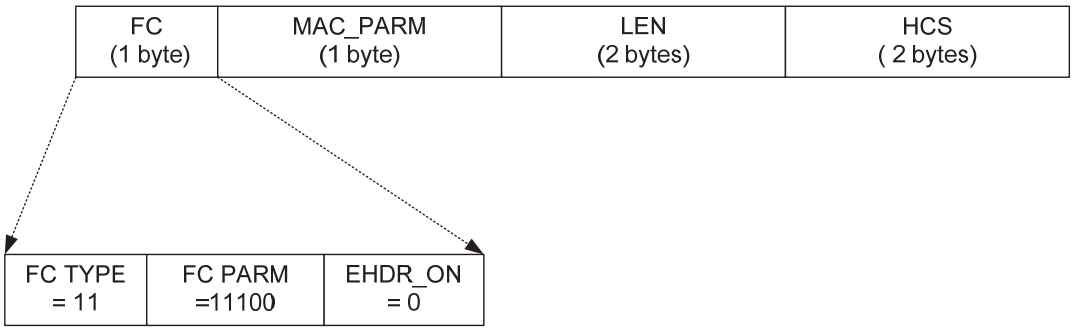


Figure 6–10 - Concatenation MAC Header Format [35]

Table 6–10 - Concatenated MAC Frame Format

Field	Usage	Size
FC	FC_TYPE = 11; MAC Specific Header FC_PARM[4:0] = 11100; Concatenation MAC Header EHDR_ON = 0; No EHDR with Concatenation Header	8 bits
MAC_PARM	CNT, number of MAC frames in this concatenation CNT = 0 indicates unspecified number of MAC frames	8 bits
LEN	LEN = x +... + y; length of all following MAC frames in bytes	16 bits
EHDR	Extended MAC Header MUST NOT be used	0 bytes
HCS	MAC Header Check Sequence	2 bytes
MAC frame 1	First MAC frame: MAC Header plus OPTIONAL data PDU	x bytes
MAC frame n	Last MAC frame: MAC Header plus OPTIONAL data PDU	y bytes
	Length of Concatenated MAC frame	6 + LEN bytes

The MAC_PARM field in the Concatenation MAC header provides a count of MAC frames as opposed to EHDR length or REQ amount as used in other MAC headers. If the field is non-zero, then it indicates the total count of MAC Frames (CNT) in this concatenation burst.

The Concatenation Frame is for Pre-3.0 DOCSIS support and MUST NOT be used by CMs operating in Multiple Transmit Channel Mode.

6.2.5 Extended MAC Headers

Every MAC Header, except the Timing, Concatenation MAC Header, Request Frame, and Queue-depth Based Request Frame, has the capability of defining an Extended Header field (EHDR). The CM or CMTS MUST indicate the presence of an EHDR field by the EHDR_ON flag in the FC field being set. Whenever this bit is set, then the CM or CMTS MUST use the MAC_PARM field as the EHDR length (ELEN). The minimum defined EHDR is 1 byte. The maximum EHDR length is 240 bytes.

A compliant CMTS and CM MUST support extended headers.

The CM MUST comply with Figure 6–11 and Table 6–11 for MAC Headers with an Extended Header. The CMTS MUST comply with Figure 6–11 and Table 6–11 for MAC Headers with an Extended Header.

[35] Figure revised per MULPIv3.0-N-06.0313-5 by GO on 11/20/06.

Note: The CM MUST NOT use Extended Headers in a Concatenation MAC Header, but may be included as part of the MAC Headers within the concatenation.

The CM MUST NOT use Extended Headers in Request Frames or Queue-depth Based Request Frames. The CM and CMTS MUST NOT use Extended Headers in Timing MAC Headers.

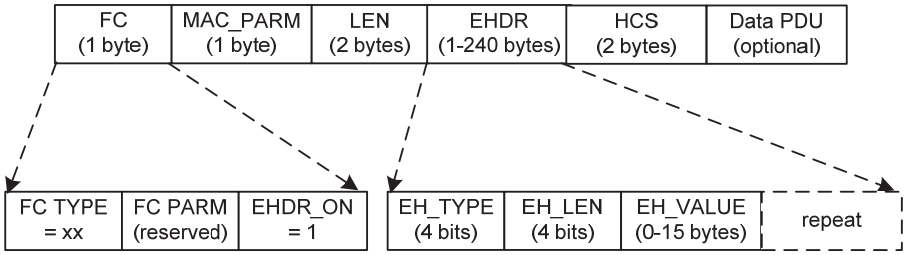


Figure 6–11 - Extended MAC Format

Table 6–11 - Example Extended Header Format

Field	Usage	Size
FC	FC_TYPE = XX; Applies to all MAC Headers FC_PARM[4:0] = XXXXX; dependent on FC_TYPE EHDR_ON = 1; EHDR present this example	8 bits
MAC_PARM	ELEN = x; length of EHDR in bytes	8 bits
LEN	LEN = x + y; length of EHDR plus optional data PDU in bytes	16 bits
EHDR	Extended MAC Header present in this example	x bytes
HCS	MAC Header Check Sequence	2 bytes
PDU	OPTIONAL data PDU	y bytes
	Length of MAC frame with EHDR	6 + x + y bytes

Since the EHDR increases the length of the MAC frame, the CM or CMTS MUST increase the value of the LEN field to include both the length of the Data PDU and the length of the EHDR.

The EHDR field consists of one or more EH elements. The size of each EH element is variable. The CM or CMTS MUST set the first byte of the EH element to contain a type and a length field. Every CM MUST use this length to skip over any unknown EH elements. The CM MUST comply with Table 6–12 for EH elements. The CMTS MUST comply with Table 6–12 for EH elements.

Table 6–12 - EH Element Format

EH Element Fields	Usage	Size
EH_TYPE	EH element Type Field	4 bits
EH_LEN	Length of EH_VALUE	4 bits
EH_VALUE	EH element data	0-15 bytes

The CM MUST support the types of EH element defined in Table 6–13. The CMTS MUST support the types of EH element defined in Table 6–13. The CM MUST comply with Table 6–13 for Extended Header Types. The CMTS MUST comply with Table 6–13 for Extended Header Types. Reserved and extended types are undefined at this point and MUST be ignored by CMs and CMTSs.

The first ten EH element types are intended for one-way transfer between the cable modem and the CMTS. The next five EH element types are for end-to-end usage within a MAC-sublayer domain. Thus, the information attached to EHDR elements 10-14 on the upstream MUST also be left attached by the CMTS when the information is forwarded within a MAC-sublayer domain. The final EH element type is an escape mechanism that allows for more types and longer values, and MUST be used by CMs and CMTSs as shown in Table 6–13.

Table 6–13 - Extended Header Types[36]

EH_TYPE	EH_LEN	EH_VALUE
0	0	Null configuration setting; may be used to pad the extended header. The EH_LEN is zero, but the configuration setting may be repeated.
1	3	Request: mini-slots requested (1 byte); SID (2 bytes) [CM→CMTS]
2	2	Acknowledgment requested; SID (2 bytes) [CM→CMTS]
3 (= BP_UP)	4	Upstream Privacy EH Element [DOCSIS SECv3.0]
	5	Upstream Privacy with Fragmentation[1] EH Element (See [DOCSIS SECv3.0] and Section 7.2.5.2)
4 (= BP_DOWN)	4	Downstream Privacy EH Element[DOCSIS SECv3.0]
5	1	Service Flow EH Element; Payload Header Suppression Header Downstream
6	1	Service Flow EH Element; Payload Header Suppression Header Upstream
	2	Service Flow EH Element; Payload Header Suppression Header Upstream (1 byte), Unsolicited Grant Synchronization Header (1 byte)
7 (= BP_UP2)	3	Upstream Privacy EH version 2 Element with no piggyback request
8	varies	Downstream Service EH Element
9	5	DOCSIS Path Verify EH Element
10 - 14		Reserved [CM <-> CM]
15	XX	Extended EH Element: EHX_TYPE (1 byte), EHX_LEN (1 byte), EH_VALUE (length determined by EHX_LEN)

[1] An Upstream Privacy with Fragmentation EH Element only occurs within a Fragmentation MAC-Specific Header. (Refer to Section 6.2.5.4)

6.2.5.1 Piggyback Requests[37]

Several Extended Headers can be used to request bandwidth for subsequent transmissions. These requests are generically referred to as "piggyback requests". They are extremely valuable for performance because they are not subject to contention as Request Frames generally are (refer to Section 7.2.2).

Requests for additional bandwidth can be included in Request, Upstream Privacy, and Upstream Privacy with Fragmentation Extended Header elements, as well as in Segment Headers.

[36] Table modified per MULPIv3.0-N-07.0487-2 on 7/11/07 and MULPIv3.0-N-0493-4 on 7/13/07 by KN.
[37] Section modified per MULPIv3.0-N-07.0487-2 on 7/11/07 by KN.

6.2.5.2 Request Extended Header[38]

The Request Extended Header (EH_TYPE=1) is used to piggyback requests on packets that do not have the Baseline Privacy extended headers. In that case, when operating with Multiple Transmit Channel Mode disabled, the CM MUST use either the Request Extended Header with EH_LEN=3 or the BP_UP Extended Header to send piggyback requests. When the CM is operating with Multiple Transmit Channel Mode enabled and segment headers are disabled, the CM MUST NOT use piggyback requests. When the CM is operating with Multiple Transmit Channel Mode enabled and segment headers are enabled, the CM MUST only use the request field in the segment header to send a piggyback request.

6.2.5.3 Fragmentation Extended Header

Pre-3.0 DOCSIS fragmented packets use a combination of the Fragmentation MAC header and a modified version of the Upstream Privacy Extended header. Section 6.2.5.4 describes the Fragmentation MAC header. The Upstream Privacy Extended Header with Fragmentation, also known as the Fragmentation Extended Header, transmitted by the CM MUST comply with Table 6–14. CMs operating in Multiple Transmit Channel Mode MUST NOT use fragmentation extended headers.

Table 6–14 - Fragmentation Extended Header Format

EH Element Fields	Usage	Size
EH_TYPE	Upstream Privacy EH element = 3	4 bits
EH_LEN	Length of EH_VALUE = 5	4 bits
EH_VALUE	Key_seq; same as in BP_UP	4 bits
	Ver = 1; version number for this EHDR	4 bits
	BPI_ENABLE If BPI_ENABLE=0, BPI disabled If BPI_ENABLE=1, BPI enabled	1 bit
	Toggle bit; same as in BP_UP [DOCSIS SECv3.0]	1 bit
	SID; Service ID associated with this fragment	14 bits
	REQ; number of mini-slots for a piggyback request	8 bits
	Reserved; set to zero	2 bits
	First_Frag; set to one for first fragment only	1 bit
	Last_Frag; set to one for last fragment only	1 bit
	Frag_seq; fragment sequence count, incremented for each fragment.	4 bits

6.2.5.4 Service Flow Extended Header

The Service Flow EH Element is used to enhance Service Flow operations. It may consist of one or two bytes in the EH_VALUE field. The Payload Header Suppression Header is the only byte in a one byte field or the first byte in a two byte field. The Unsolicited Grant Synchronization Header is the second byte in a two byte field.

[38] Section modified per MULPIv3.0-N-07.0487-2 on 7/11/07 by KN.

6.2.5.4.1 Payload Header Suppression Header

In Payload Header Suppression (PHS), a repetitive portion of the payload headers following the HCS is suppressed by the sending entity and restored by the receiving entity. In the upstream, the sending entity is the CM and the receiving entity is the CMTS. In the downstream, the sending entity is the CMTS and the receiving entity is the CM.

For small payloads, Payload Header Suppression provides increased bandwidth efficiency without having to use compression. Payload Header Suppression may be separately provisioned in the upstream and downstream, and is referenced with an extended header element.

A compliant CM MUST support both PHSI-indexed Payload Header Suppression[39] and DSID-indexed Payload Header Suppression. A CMTS MUST support PHSI-indexed Payload Header Suppression. A CMTS SHOULD support DSID-indexed Payload Header Suppression.

The CM MUST comply with Table 6–15 for Payload Header Suppression Extended Header sub-elements. The CMTS MUST comply with Table 6–15 for Payload Header Suppression Extended Header sub-elements.

Table 6–15 - Payload Header Suppression EHDR Sub-Element Format

EH Element Fields	Usage		Size
EH_TYPE	Service Flow EH_TYPE=5 for downstream and EH_TYPE=6 for upstream		4 bits
EH_LEN	Length of EH_VALUE = 1		4 bits
EH_VALUE	0	Indicates no payload header suppression on current packet.	8 bits
	1-254	Payload Header Suppression Index (PHSI)	
	255	Indicates DSID-indexed PHS	

For PHSI-indexed PHS the Payload Header Suppression Index is unique per service flow in the upstream and unique per CM in the downstream. Payload Header Suppression is disabled if this Extended Header element is omitted or, if included, with the PHSI value set to 0. The Payload Header Suppression Index (PHSI) references the suppressed byte string known as a Payload Header Suppression Field (PHSF).

For DSID-indexed PHS, the EH_VALUE field of the Payload Header Suppression EHDR is set to the static value of 255. Payload Header Suppression is disabled if this Extended Header element is omitted or, if included, with the EH_Value field set to 0. In DSID-indexed PHS, the DSID references the Payload Header Suppression Field (PHSF).

The CM MUST begin the Upstream Suppression Field with the first byte following the MAC Header Checksum. The CMTS MUST begin the Downstream Suppression Field with the thirteenth byte following the MAC Header Checksum. This allows the Ethernet SA and DA to be available for filtering by the CM.

The operation of Baseline Privacy (refer to [DOCSIS SECv3.0]) is not affected by the use of PHS. When Fragmentation is inactive, Baseline Privacy begins encryption and decryption with the thirteenth byte following the MAC Header checksum.

Unless the entire Packet PDU is suppressed, the Packet PDU CRC is always transmitted, and MUST be calculated only on the bytes transmitted. The bytes that are suppressed MUST NOT be included by the CM or CMTS in the CRC calculation.

[39] This is not intended to imply that the CM must be capable of determining when to invoke Payload Header Suppression. Payload Header Suppression support is only required for the explicitly signaled case.

6.2.5.4.2 Unsolicited Grant Synchronization Header

The Unsolicited Grant Synchronization Header may be used to pass status information regarding Service Flow scheduling between the CM and CMTS. It is currently only defined for use in the upstream with Unsolicited Grant and Unsolicited Grant with Activity Detection scheduling services. (Refer to Section 7.2.3.3.)

This extended header is similar to the Payload Suppression EHDR except that the EH_LEN is 2, and the EH_VALUE has one additional byte which includes information related to Unsolicited Grant Synchronization. For all other Service Flow Scheduling Types, the field SHOULD NOT be included by the CM in the Extended Header Element. The CMTS MAY ignore this field.

Table 6–16 - Unsolicited Grant Synchronization EHDR Sub-Element Format

EH Element Fields	Usage		Size
EH_TYPE	Service Flow EH_TYPE = 6		4 bits
EH_LEN	Length of EH_VALUE = 2		4 bits
EH_VALUE	0	Indicates no payload header suppression on current packet.	8 bits (always present)
	1-254	Payload Header Suppression Index (PHSI)	
	Queue Indicator		1 bit
	Active Grants		7 bits

6.2.5.5 BP_UP2 Extended Header[40]

The BP_UP2 EHDR is used when Multiple Transmit Channel Mode is enabled and Baseline Privacy is enabled. When Multiple Transmit Channel Mode is enabled for the CM and segment headers are enabled for a given service flow, the CM MUST use the piggyback opportunity in the segment header for any piggyback requests for that service flow. If segment headers are not enabled for a service flow, the CM is not permitted to create piggyback requests for that service flow. Thus, a piggyback field is not needed in the BP_UP2 EHDR for any service flows. The CM operating in Multiple Transmit Channel Mode with Baseline Privacy Enabled MUST use the BP_UP2 EHDR with a length of 3 for all service flows. The CM MUST comply with Table 6–17 for the BP_UP2 EHDR with length of 3.

Table 6–17 - BP_UP2 EHDR with Length 3

EH Element Fields	Usage	Size
EH_TYPE	Upstream Privacy EH_TYPE = 7	4 bits
EH_LEN	Length of EH_VALUE = 3	4 bits
EH_VALUE	Key_seq; same as in BP_UP	4 bits
	Ver = 1; version number for this EHDR	4 bits

[40] Paragraph and table in section deleted per MULPIv3.0-N-07.0487-2 on 7/11/07 by KN, and modified per MULPIv3.0-N-08.0694-4 on 1/6/09 by JS.

EH Element Fields	Usage	Size
	BPI_ENABLE If BPI_ENABLE=0, BPI disabled If BPI_ENABLE=1, BPI enabled	1 bit
	Toggle bit; same as in BP_UP [DOCSIS SECv3.0]	1 bit
	Reserved, set to zero[41]	14 bits

6.2.5.6 Downstream Service Extended Header

The Downstream Service Extended Header (DS EHDR) communicates to the CM information on how to process downstream packets. The DS EHDR contents vary depending on the EH_LEN, which may be one, three, or five bytes. The CMTS MUST comply with Table 6–18, Table 6–19, and Table 6–20 for DS EHDRs. This header is ignored by CMs which do not implement Downstream Channel Bonding.

Table 6–18 - One-byte DS EHDR Sub-Element Format

EH Element Fields	Usage	Size
EH_TYPE	Downstream Service EH_TYPE = 8	4 bits
EH_LEN	1	4 bits
EH_VALUE	Traffic Priority	3 bits
	Reserved	5 bits

Table 6–19 - Three-byte DS EHDR Sub-Element Format

EH Element Fields	Usage	Size
EH_TYPE	Downstream Service EH_TYPE = 8	4 bits
EH_LEN	3	4 bits
EH_VALUE	Traffic Priority	3 bits
	Reserved	1 bit
	Downstream Service ID (DSID)	20 bits

Table 6–20 - Five-byte DS-EHDR Sub-Element Format

EH Element Fields	Usage	Size
EH_TYPE	Downstream Service EH_TYPE = 8	4 bits
EH_LEN	5	4 bits
EH_VALUE	Traffic Priority	3 bits
	Sequence Change Count	1 bit
	Downstream Service ID (DSID)	20 bits
	Packet Sequence Number	16 bits

[41] Table row text modified per MULPIv3.0-N-07.0529-1 on 10/30 by KN.

When the CMTS classifies a packet to a service flow with a nonzero Traffic Priority (see Annex C.2.2.5.1), it MUST add a DS EHDR and set the Traffic Priority sub-element to the value of the service flow's Traffic Priority parameter.

When the CMTS transmits a packet from a Group Service Flow assigned to a single downstream channel (i.e., non-bonded) it MUST include a three-byte DS EHDR with a DSID. Refer to Section 9.2.2.

When the CMTS transmits a packet from a Service Flow assigned to a Downstream Bonding Group, the CMTS MUST include a five-byte DS EHDR (except if there is a vendor specific configuration to permit the Service Flow to send non-sequenced packets). The DSID in a five-byte DS EHDR is a Resequencing DSID, which identifies a resequencing context. The Packet Sequence Number identifies the sequence number of a packet within the resequencing context identified by the DSID.

A Sequenced Null Packet is defined as a variable-length packet-based MAC frame (Section 6.2.2.1) which includes a five-byte Downstream Service EHDR, does not include any other Extended Header, and has a Packet PDU length of zero. A CMTS MAY send Sequenced Null Packets. A CM MUST accept Sequenced Null Packets. [42]

For a Resequencing DSID, a packet received with a 3-byte DS EHDR MUST be processed by the CM as a non-sequenced packet. For a non-resequencing DSID, a packet received with 5-byte DS EHDR MUST be processed by the CM as a non-sequenced packet. A packet received with a 2-byte DS EHDR MUST be treated by the CM identically to the 1-byte DS EHDR (the extra byte is ignored). A packet received with a 4-byte DS EHDR MUST be treated by the CM identically to the 3-byte DS EHDR (the extra byte is ignored). A packet received with a 6-byte or greater DS EHDR MUST be treated by the CM identically to the 5-byte DS EHDR (the extra byte(s) are ignored).

6.2.5.7 DPV Extended Header

Table 6–21 - DPV Extended Header Format

EH Element Fields	Usage	Size
EH_TYPE	DPV EHDR = 9	4 bits
EH_LEN	Length of EH_VALUE = 5 bytes	4 bits
EH_VALUE	Start Reference Point	8 bits
	Timestamp Start	32 bits

Start Reference Point This is the DPV Reference Point that the DPV measurement originates from (see Section 10.4.2).

Timestamp Start This is the local timestamp at the sender when the DPV packet gets injected into the data stream and departs from the DPV reference point.

The CMTS MAY support the generation of the DPV Extended Header. The CMTS MAY place a DPV EHDR on any packet within any DSID or any Service Flow. The CMTS MUST comply with Table 6–21 for DPV EHDRs. A Modular CMTS Core MAY choose to place a DPV EHDR on any packet within any DEPI flow. This may be done in order to compare the average latency between different Service Flows and/or DEPI flows.

The CM MAY support the generation of the DPV Extended Header.

The CMTS and CM are not required to take any action upon receiving a DPV EHDR other than silently discarding it.

[42] Revised per MULPIv3.0-N-06.0313-5 by GO on 11/21/06.

6.3 Segment Header Format[43]

The CM MUST use a Segment Header when transmitting packets in Multiple Transmit Channel Mode for service flows where use of the segment header is enabled. For these service flows, a Segment Header must appear at the beginning of any transmission made with IUCs 5,6,9,10, or 11. Figure 6–12 shows the segment header format. The segment header is 8 bytes in length. Table 6–22 describes the segment header fields. The CM MUST comply with Figure 6–12 and Table 6–22 for segment headers. [44]

PFI (1 bit)	R (1 bit)	Pointer Field (14 bits)	Sequence # (13 bits)	SC (3 bits)	Request (2 Bytes)	HCS (2 Bytes)

Figure 6–12 - Segment Header Format

Table 6–22 - Segment Header Fields

Field	Usage	Size
PFI	Pointer Field Indicator. This bit is set to a one, to indicate that the pointer field is relevant. When cleared to a zero, this bit indicates that there is no DOCSIS MAC frame starting within this segment and the pointer field is ignored.	1 bit
R	Reserved. This field should be set to a zero by the CM.	1 bit
Pointer Field	When the PFI bit is a one, the value in this field is the number of bytes past the end of the segment header that the receiver will skip when looking for a DOCSIS MAC Header. Thus, a value of zero in the pointer field with the PFI set to one would designate a DOCSIS MAC header beginning just after the segment header.	14 bits
Sequence #	Sequence number that increments by 1 for every segment of a particular service flow.	13 bits
SC	SID Cluster ID of the SID Cluster associated with the Request field of the segment header. The valid SID Cluster ID range is 0 to M-1, where M is the number of SID Clusters per Service Flow supported by the CM.	3 bits
Request	The total number of bytes requested in units of N bytes where N is a parameter of the service flow for which the request is being made. See Annex C.2.2.6.12.	2 bytes
HCS	MAC Header Check Sequence. Similar to HCS used on all MAC headers and is calculated over all other fields in the segment header.	2 bytes

The HCS field is a 16-bit CRC that ensures the integrity of the segment header, even in a collision environment. The CM MUST include all fields within the segment header for the HCS field coverage except the HCS field itself. The HCS is calculated using CRC-CCITT ($x^{16} + x^{12} + x^5 + 1$) as defined in [ITU-T X.25].

For segment header ON operation, the CM may use the piggyback field in the segment header to make piggyback requests for the service flow and MUST NOT use any request EHDR fields within the segment payload.

6.4 MAC Management Messages

6.4.1 MAC Management Message Header[45]

CMs and CMTSs MUST encapsulate MAC Management Messages in an LLC unnumbered information frame per [ISO/IEC 8802-2], which in turn is encapsulated within the cable network MAC framing, as shown in Figure 6–13.

[43] Revised per MULPIv3.0-N-07.0426-1 by ab on 4/30/07.
[44] Revised per MULPIv3.0-N-06.0313-5 by GO on 11/21/06.
[45] Section revised per MULPIv3.0-N-07.0427-3 by ab on 4/30/07 and MULPIv3.0-N-07.0493-4 on 7/13/07 by KN.

2) *DBA sin informe de estado (NSR-DBA)*

La OLT reconoce el estado de congestión de cada T-CONT supervisando los flujos de tráfico entrantes. En este modo, nunca se envía el campo DBA en DBRu, ya que la OLT no debería solicitarlo. En el caso excepcional de que la OLT solicite la DBRu, la ONU debe enviarla, aunque la OLT ignore su contenido.

7.7.4 Aspectos de gestión

Para el funcionamiento de la DBA, las funcionalidades de gestión deben proveer o negociar determinados parámetros. Mediante dichos medios, la OLT y la ONU acuerdan el modo de funcionamiento DBA, y responden correctamente a las solicitudes que se realizan mutuamente. La OMCI G-PON debe proveer o negociar todos los parámetros de la DBA.

8 Trama de convergencia de transmisión (TC) GTC

La figura 8-1 muestra la estructura de trama de TC GTC en los sentidos descendente y ascendente. La trama descendente consta de bloque de control físico descendente (PCBd), partición ATM y partición GEM. La trama ascendente consta de múltiples ráfagas de transmisión. Cada ráfaga ascendente contiene como mínimo la tara de la capa física (PLOu, *physical layer overhead*). Además de la cabida útil, también puede contener las secciones PLOAMu, PLSu, y DBRu. La trama descendente proporciona la referencia de tiempo común para la PON, y proporciona la señalización de control común para el sentido ascendente.

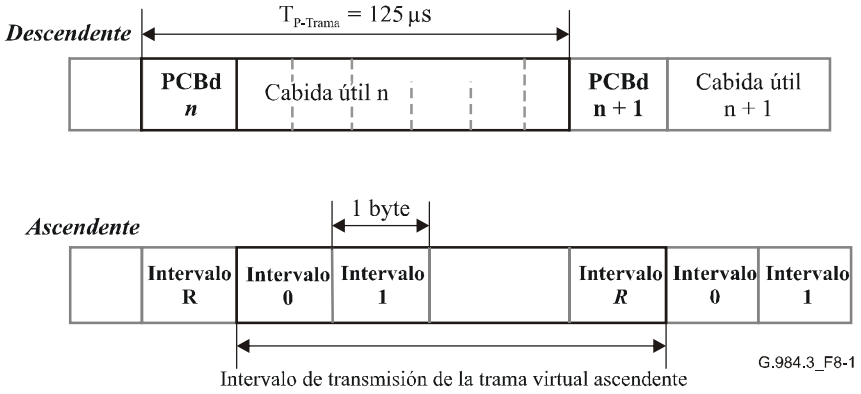


Figura 8-1/G.984.3 – Estructura de la trama de convergencia de transmisión (TC) GTC

En la figura 8-2 se ilustra el concepto de control de acceso al medio aplicable a este sistema.

NOTA – La disposición de los campos de la figura 8-2 se ha simplificado en aras de una mayor claridad. Para una descripción completa de los campos y de sus funciones véanse las figuras siguientes.

La OLT envía punteros en el PCBd que indican el momento en que cada ONU puede iniciar y terminar sus transmisiones en sentido ascendente. De esta forma, en un momento dado sólo una ONU accede al medio, no produciéndose contención en un funcionamiento normal. Las unidades de los punteros son bytes, lo cual permite que la OLT controle el medio con una granularidad de anchura de banda estática de 64 kbit/s. No obstante, algunas implementaciones de OLT pueden optar por fijar los punteros y el tamaño de los intervalos de tiempo con una granularidad mayor, consiguiendo un control de anchura de banda fino con una programación dinámica. Nótese que si bien la figura 8.2 muestra el caso en el que los punteros se transmiten en un orden ascendente ello no constituye un requisito del protocolo.

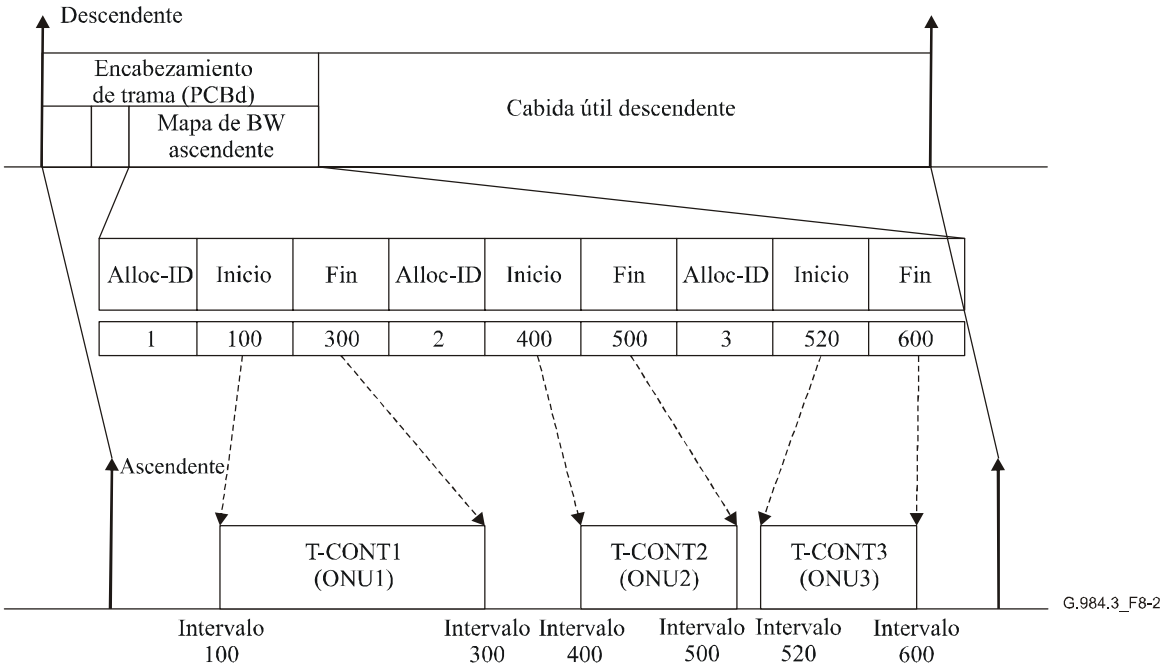


Figura 8-2/G.984.3 – Concepto de control de acceso al medio de TC GTC

8.1 Estructura de trama descendente

En la figura 8.3 se muestra la estructura de trama descendente. La trama es de 125 µs tanto para las velocidades binarias descendentes de 1,24416 Gbit/s como de 2,48832 Gbit/s. Por tanto, la trama tiene una longitud de 19 440 bytes en el sistema de 1,24416 Gbit/s, y de 38 880 bytes en un sistema de 2,48832 Gbit/s. La gama de valores de longitud de la PCBd es la misma para ambas velocidades, y es función del número de estructuras de atribución por cada trama.

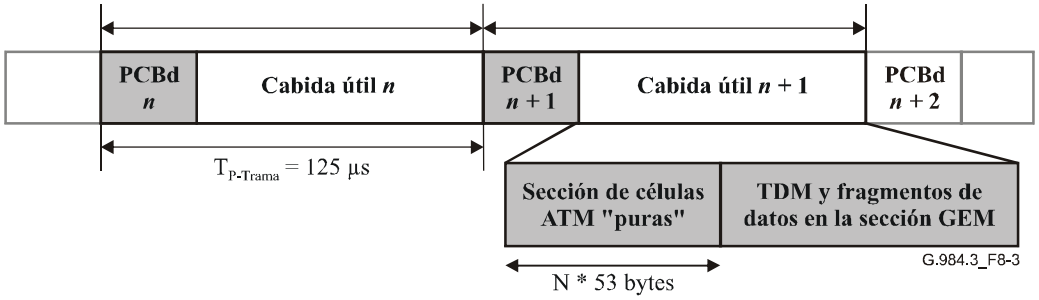


Figura 8-3/G.984.3 – Trama descendente de TC GTC

8.1.1 Orden de bits y bytes

A lo largo de esta Recomendación se utiliza el convenio de que para todos los campos siempre se transmite en primer lugar el bit más significativo. Por ejemplo, el número 0xF0 indica una secuencia que comienza por uno y termina por cero.

8.1.2 Aleatorización de la trama

La trama descendente se aleatoriza utilizando un polinomio de aleatorización con sincronismo de trama. El polinomio utilizado es x^7+x^6+1. Dicho patrón de datos se suma módulo dos a los datos descendentes. Los bits del registro de desplazamiento utilizado para calcular este polinomio se ponen todos a uno cuando se recibe el primer bit después del campo Psync del PCBd, continuando su funcionamiento hasta el último bit de la trama descendente.

8.1.3 Bloque de control físico descendente (PCBd, *physical control block downstream*)

En la figura 8-4 se muestra un diagrama del PCBd. El PCBd contiene varios campos, cada uno de los cuales se describe a continuación. La OLT realiza una transmisión en difusión del PCBd, de forma que cada ONU recibe el PCBd completo. Las ONU actúan consecuentemente con la información relevante de dicho campo.

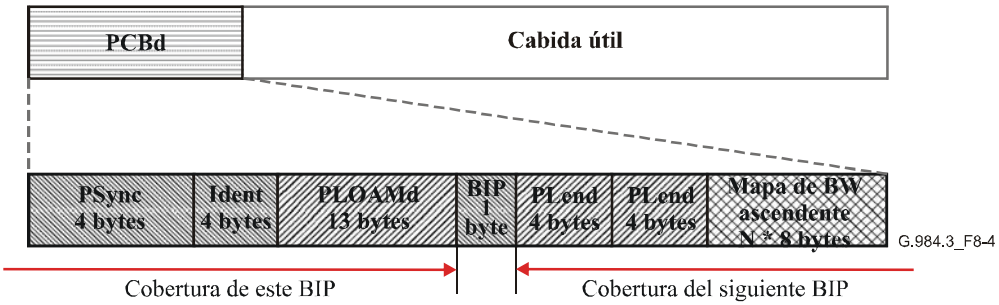


Figura 8-4/G.984.3 – Bloque de control físico descendente (PCBd) de TC de GTC

8.1.3.1 Campo sincronización física (Psync, *physical synchronization*)

El campo sincronización física es un patrón fijo de 32 bits con el que comienza cada PCBd. La lógica de la ONU utiliza este patrón para identificar el comienzo de la trama. La codificación del campo Psync es 0xB6AB31E0. Nótese que el campo Psync no está aleatorizado.

La ONU implementa la máquina de estado de sincronización que se muestra en la figura 8-5. La ONU comienza en un estado de captura y busca el patrón Psync en todas las alineaciones posibles (de bit y de byte) mientras permanece en el estado de captura. Una vez que identifica un patrón Psync correcto, la ONU cambia al estado pre-sync (presincronismo) y arranca un contador, N, que toma el valor 1. La ONU busca otro patrón Psync que siga al anterior transcurridos 125 µs. Con cada campo Psync correcto identificado, el contador se aumenta en uno. Si se detecta un campo Psync incorrecto, la ONU vuelve al estado de captura. Si estando en el estado pre-sync, el contador alcanza el valor M_1, la ONU pasa el estado sync (sincronismo). Una vez que la ONU alcanza el estado sync, declara que ha encontrado la estructura de trama descendente, y comienza el procesamiento de la información del PCBd. Si la ONU detecta M_2 campos Psync incorrectos consecutivos, puede declarar que ha perdido la alineación de trama descendente y retorna al estado de captura.

El valor recomendado de M_1 es 2. El valor recomendado M_2 es 5.

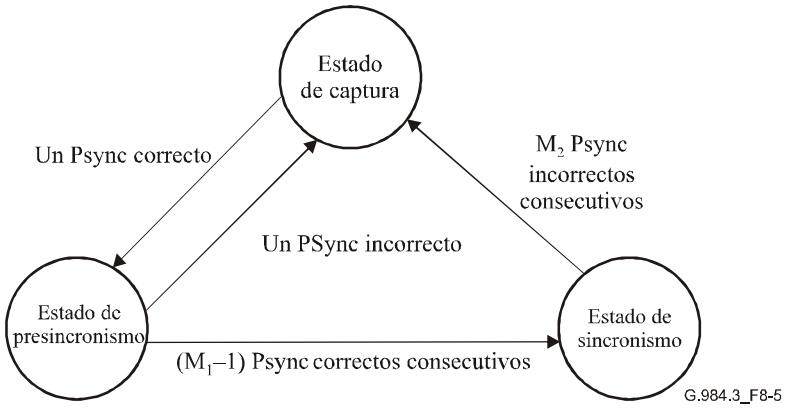


Figura 8-5/G.984.3 – Máquina de estados de sincronización de ONU descendente GTC TC

8.1.3.2 Campo Ident

El campo Ident de 4 bytes sirve para identificar estructuras de trama de mayor tamaño. Este contador de supertramas es utilizado por el sistema de criptación de datos de usuario y también puede ser utilizado para proporcionar señales de referencia síncronas de menor velocidad binaria. Los 30 bits menos significativos del campo Ident contienen un contador, y el valor de Ident de cada trama es superior en uno al anterior. Cuando el contador alcanza su valor máximo, se pone a cero en la trama siguiente.

Para permitir una cierta tolerancia frente a errores, la ONU debe implementar un contador de supertrama local y una máquina de estados de sincronización de supertrama. Esta máquina de estados es idéntica a la máquina de estados de sincronización descrita anteriormente. Cuando se encuentra en el estado de captura, la ONU carga el valor del contador de supertrama recibido en el campo Ident en su contador local. Cuando se encuentra en los estados Pre-sync y sync, la ONU compara su valor local con el valor de contador recibido. La concordancia significa una correcta sincronización, mientras que la discordancia indica un error de transmisión o una pérdida de sincronización.

El bit más significativo del campo Ident se utiliza para indicar si se utiliza FEC en sentido descendente. Existen otros bits del campo Ident que están reservados. En la figura 8-6 se muestra el campo Ident.

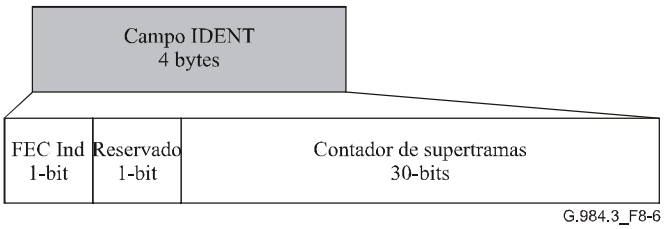


Figura 8-6/G.984.3 – Campo IDENT

8.1.3.3 Campo PLOAMd

El campo PLOAM descendente tiene 13 bytes y contiene el mensaje PLOAM. El formato de estos mensajes se describe en la cláusula 9.

8.1.3.4 Campo BIP

El campo BIP tiene 8 bits y contiene la paridad de entrelazado de bits (BIP, *bit interleaved parity*) de todos los bytes transmitidos desde el último BIP. El receptor calcula la paridad de entrelazado de bits y compara el resultado con el BIP transmitido a fin de medir el número de errores en el enlace.

8.1.3.5 Campo Plend

El campo longitud de la cabida útil descendente (Plend, *payload lenght downstream*) especifica la longitud del mapa de anchura de banda y la partición ATM. Se envía dos veces para conseguir robustez frente a errores, indicándose a continuación el procedimiento utilizado para asegurar dicha robustez.

La longitud del mapa de anchura de banda (Blen, *bandwidth length*) está incluido en los primeros 12 bits. Ello limita a 4095 el número de los ID de atribución (Alloc-ID) que pueden concederse durante un intervalo de tiempo de 125 µs. La longitud real del mapa de anchura de banda (BW-MAP) medido en bytes es 8 veces el valor de Blen.

La longitud de la partición ATM (Alen, *ATM length*) viene dada por los 12 bits siguientes del campo Plend. Ello permite que existan hasta 4095 células ATM en una trama, lo cual es suficiente para velocidades de hasta 10 Gbit/s. La longitud de la partición ATM en bytes es, por tanto, 53 veces el valor de Alen.

Los últimos 8 bits del campo Plend consisten en un CRC-8, con el mismo polinomio que en la Rec. UIT-T I.432.1 ($g(x) = x^8 + x^2 + x + 1$). Sin embargo, a diferencia de la Rec. UIT-T I.432.1, no se realiza la operación OR exclusivo del CRC con 0x55. El receptor del campo Plend implementa las funciones de detección y corrección de errores del CRC-8. El receptor intenta decodificar las dos copias del campo Plend enviadas, y en función del resultado del proceso de detección CRC-8, utiliza el campo Plend de mayor calidad. A tal fin, la clasificación de la calidad, de superior e inferior, es la siguiente: 'libre de errores', 'con capacidad para corregir un error, y 'sin capacidad para corregir un error'. Si los dos campos Plend son incorregibles, o son de la misma calidad pero con diferentes valores, el receptor no puede realizar el análisis sintáctico de la trama, ya que lo más probable es que haya una combinación indetectable de errores. Con la transmisión dual, el número mínimo de errores que ocasionaría tal circunstancia es de cuatro bits.

La figura 8-7 describe el campo Plend.

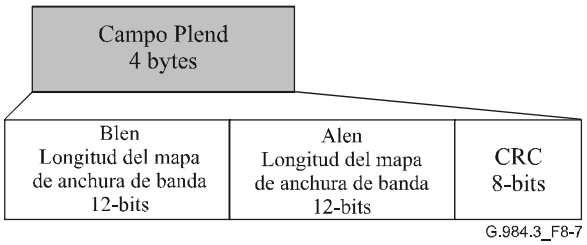


Figura 8-7/G.984.3 – Campo Plend (longitud de la cabida útil descendente)

8.1.3.6 Campos BWmap

El mapa de anchura de banda (BWmap, *bandwidth map*) es una matriz escalar de estructuras de atribución de 8 bytes. Cada entrada a dicha matriz representa una única atribución de anchura de banda a un T-CONT en concreto. El número de entradas del mapa viene dado por el campo Plend. El formato de cada entrada se indica a continuación, y se representa en la figura 8-8.

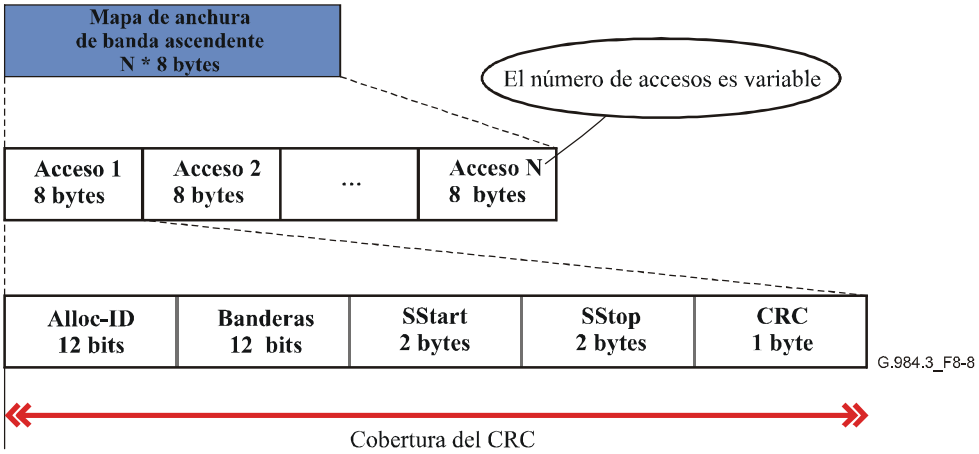


Figura 8-8/G.984.3 – Estructura de atribución del mapa de anchura de banda GTC

8.1.3.6.1 Campo ID de atribución

El campo ID de atribución (Alloc-ID) contiene un número de 12 bits que identifica el T-CONT específico al que se concede tiempo en sentido ascendente de la PON. En general, este campo de doce bits no está estructurado, pero se aplican algunas normas básicas. En primer lugar, los 254 valores inferiores del ID de atribución se utilizan para direccionar la ONU directamente. Durante el procedimiento de determinación de distancia, el primer Alloc-ID que se asigna a la ONU debe pertenecer a este rango. Si se necesitasen valores adicionales de Alloc-ID para dicha ONU, deben utilizarse valores superiores a 255. Asimismo, el valor Alloc-ID = 254 es el ID de activación de la ONU, que se utiliza para las ONU hasta entonces desconocidas, y el valor Alloc-ID = 255 es un valor de Alloc-ID que no se asigna. Se utiliza para indicar que ningún T-CONT puede utilizar la estructura de atribución asociada.

8.1.3.6.2 Campo banderas

El campo de banderas tiene 12 bits y contiene 4 indicaciones diferentes sobre como debe utilizarse la atribución. El significado de dichas indicaciones es el siguiente:

– Bit 11 (MSB): Envío de PLSu (secuencia de nivelación de potencia): Si este bit está puesto a uno, la ONU transmite su información de PLSu durante esta atribución. Si no lo está, la ONU no enviará la información de PLSu en la misma.

– Bit 10: Envío de PLOAMu: Si este bit está puesto a uno, la ONU transmite su información de PLOAMu durante esta atribución. Si no lo está, la ONU no transmite la información de PLOAMu en la misma.

– Bit 9: Utilización de FEC: Si este bit está puesto a uno, la ONU calcula e inserta la paridad FEC durante esta atribución. Nótese que debe ser el mismo durante toda la vida del ID de atribución, y es solamente una confirmación dentro de banda de datos previamente conocidos.

– Bits 8 y 7: Envío de DBRu (modo): En función del contenido de estos dos bits, la ONU trasmite o no el DBRu correspondiente al ID de atribución. Los puntos de código definidos son los siguientes:

  00: No enviar ninguna DBRu.

  01: Enviar DBRu en 'modo 0' (dos bytes).

  10: Envía DBRu en 'modo 1' (tres bytes).

  11: Envía DBRu en 'modo 2' (cinco bytes).

La descripción de la sintaxis de los diferentes DBRu se presenta en 8.4. Nótese que la ONU debe responder con el número requerido de bytes, con independencia del modo que realmente soporta.

Bits 6-0: Reservados para utilización futura.

8.1.3.6.3 Campo hora de inicio

El campo hora de inicio (*StartTime*) contiene un número de 16 bits que indica el momento en el que se inicia la atribución. Este tiempo se mide en bytes, comenzando por cero al inicio de la trama ascendente. Con ello se limita el tamaño de la trama ascendente a 65 536 bytes, cantidad suficiente para velocidades binarias ascendentes de hasta 2,488 Gbit/s.

La hora de inicio señala el comienzo de la transmisión de datos válidos y no incluye el tiempo de tara de la capa física. Ello permite que el significado del puntero sea el mismo con independencia de su posición en una ráfaga de atribuciones para la misma ONU. El tiempo de tara de la capa física se define incluyendo el tiempo necesario para las tolerancias (tiempo de guarda), recuperación del receptor, recuperación del nivel de señal, recuperación de temporización, delimitador y los campos PLOu, tal como se define en 8.2.2. En la Rec. UIT-T G.984.2 se incluyen los valores recomendados para los tiempos de la capa física que varían en función de la velocidad binaria ascendente. La OLT

y la ONU deben estar ambas diseñadas para incluir el tiempo de la tara de la capa física. Es responsabilidad de la OLT disponer de una mapa de anchura de banda que permita contabilizar adecuadamente el tiempo de tara de la capa física.

8.1.3.6.4 Campo hora de parada

El campo instante de parada (*StopTime*) contiene un número de 16 bits que indica el momento en que se detiene la atribución. Este tiempo se mide en bytes, comenzando por cero al inicio de la trama ascendente. El instante de parada señala el último byte de datos válido asociado a esta atribución.

8.1.3.6.5 Campo CRC

La estructura de atribución está protegida mediante un CRC-8, que utiliza el mismo polinomio que el indicado en la Rec. UIT-T I.432.1 ($g(x) = x^8 + x^2 + x + 1$). No obstante, a diferencia de la Rec. UIT-T I.432.1, no se realiza un OR exclusivo del CRC con 0x55. El receptor del campo Bwmap implementa las funciones de detección y corrección de errores del CRC-8. Si el CRC-8 indica que se ha producido un error no corregible, se descarta la estructura de atribución.

8.1.4 Campos de cabida útil de TC

Inmediatamente después del último dato del mapa de anchura de banda se encuentran las particiones de GTC. Tal como se describe a continuación, existen dos particiones.

8.1.4.1 Partición ATM

La partición ATM contiene un número de células ATM de 53 bytes. La longitud de esta partición (en células) viene dado por el campo Plend/Alen. Por tanto, el campo siempre tiene una longitud que es un entero múltiplo de 53 bytes, y las células siempre están alineadas con la partición. Por consiguiente, la delimitación de las células es trivial, y se confirma asegurando que el byte HEC verifica el resto del encabezamiento de la célula.

El flujo de células descendente se filtra en la ONU en función del VPI contenido en cada célula. Las ONT se configuran para poder reconocer los VPI que les pertenecen y las células que pertenecen a la ONU se transfieren al proceso cliente ATM.

8.1.4.2 Partición GEM

La partición GEM contiene cualquier número de tramas GEM delimitadas en modo trama. La longitud de la partición GEM es lo que queda después de haber sustraído las particiones PCBd y ATM de la longitud de trama completa. En 8.3 se describe el funcionamiento de la delimitación de trama en GEM.

El flujo de tramas descendente se filtra en la ONU sobre la base del valor del campo Port-ID de 12 bits de cada fragmento de trama. Las ONT se configuran para reconocer los Port-ID que les pertenecen, transfiriéndose al proceso cliente GEM las tramas que pertenecen a la ONU.

8.2 Estructura de trama ascendente

En la figura 8-9 se muestra un diagrama de la estructura de trama ascendente. La longitud de la trama es la misma que en sentido descendente para todas las velocidades binarias. Cada trama contiene un conjunto de transmisiones procedentes de una o varias ONU. El BWmap determina la configuración adoptada para dichas transmisiones. De acuerdo con el control ejercido por la OLT, durante cada periodo de atribución la ONU puede transmitir uno de los cuatro tipos de taras de PON y datos de usuario. Los cuatro tipos de tara son los siguientes:

1) Tara de capa física ascendente (PLOu, *physical layer overhead*).
2) Operaciones de gestión y administración de capa física ascendente (PLOAMu, *physical layer operations, administration and management upstream*).

3) Secuencia de nivelación de potencia ascendente (PLSu, *power levelling sequence upstream*).

4) Informe de anchura de banda dinámica ascendente (DBRu, *dynamic bandwidth report upstream*).

En la figura 8-10 se muestra en detalle el contenido de dichas taras.

La OLT indica mediante el campo banderas del BWmap si en una atribución debe transmitirse la información de PLOAMu, PLSu, o DBRu. El mecanismo de programación de la OLT debe tener en cuenta las necesidades de anchura de banda y latencia de dichos canales auxiliares para fijar su frecuencia de transmisión.

El estado de la información PLOu está implícito en la configuración de las propias atribuciones. La regla es que cada vez que una ONU toma el medio de la PON en lugar de otra ONU, debe transmitir una nueva copia de los datos PLOu. Si la ONU recibe dos ID de atribución contiguos (la hora de parada de una atribución tiene un valor inferior en 1 a la hora de inicio de la siguiente), la ONU suprime la transmisión de los datos PLOu de la segunda atribución. Esta supresión tiene lugar para todos los ID de atribución contiguos que la ONU reciba de la OLT. Obsérvese que el requisito necesario para realizar atribuciones contiguas no permite que la OLT deje espacios entre las transmisiones de una misma ONU. Las atribuciones deben ser exactamente contiguas, o deben programarse como si procedieran de dos ONU diferentes.

Después de la transmisión de dichas taras, se transmiten los datos de la cabida útil de usuario existentes hasta la posición indicada por el puntero hora de parada.

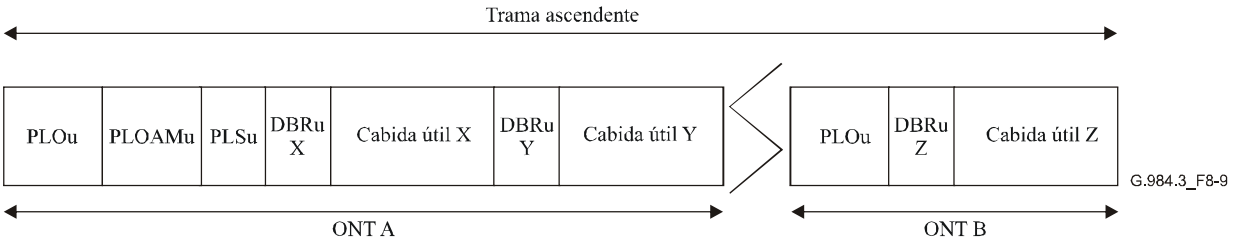


Figura 8-9/G.984.3 – Trama ascendente GTC

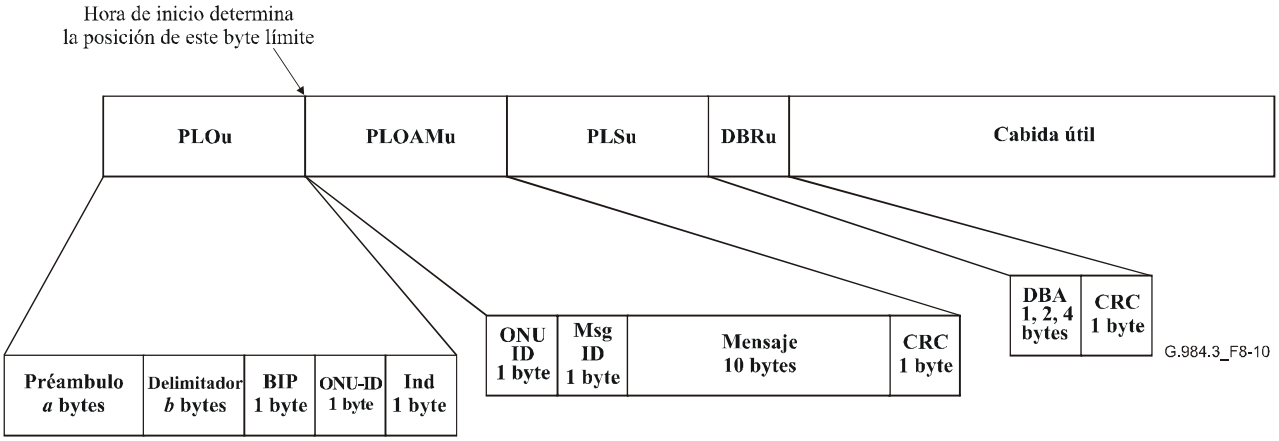


Figura 8-10/G.984.3 – Descripción detallada de las taras ascendentes GTC

8.2.1 Aleatorización de la trama

La trama ascendente se aleatoriza mediante un polinomio de aleatorización sincronizado con la trama. El polinomio utilizado es $x^7 + x^6 + 1$. Este patrón se suma en módulo dos a los datos ascendentes. El registro de desplazamiento utilizado para el cálculo de este polinomio se reinicializa a todos unos cuando se recibe el primer bit después del campo delimitador de la PLOu de la primera atribución ascendente, y se sigue ejecutando hasta el último bit de la transmisión. Si la ONU transmite varias atribuciones contiguas, el aleatorizador ascendente no debe reiniciarse en ninguno de los límites internos.

8.2.2 Tara de la capa física ascendente (PLOu)

Los datos de la PLOu incluyen la tara de la capa física (preámbulo y delimitador), y tres campos de datos relativos a la ONU en su conjunto. Estos datos se transmiten al comienzo de cualquier transmisión de ráfaga de una ONU. Nótese que para mantener la conectividad con la ONU, la OLT debe intentar atribuir una transmisión ascendente a cada ONU con un intervalo mínimo entre ellas. La duración de dicho intervalo está determinado por parámetros de servicio de la ONU.

La capa GTC alimenta la PLOu. El preámbulo y el delimitador se forman tal como determina la OLT en el mensaje tara ascendente (*upstream_overhead*). Nótese que estos bytes se transmiten en el instante inmediatamente anterior al byte que ha sido identificado por el puntero hora de inicio (*StartTime*).

8.2.2.1 Campo BIP

El campo BIP tiene 8 bits y contiene la paridad de entrelazado de todos los bytes transmitidos desde el último BIP de la ONU en cuestión, excluidos los bytes de preámbulo y delimitador. El receptor de la OLT calcula la paridad de entrelazado de bits de cada ráfaga de la ONU, y compara su resultado con el campo BIP recibido a fin de medir el número de errores del enlace.

8.2.2.2 Campo ONU-ID

El campo ONU-ID tiene 8 bits y contiene el ONU-ID específico de la ONU que está transmitiendo. El ONU-ID se asigna a la ONU durante el proceso de determinación de distancia. Antes de asignar el ONU-ID, la ONU pone en este campo el valor de ONU-ID no asignado (255). La OLT puede verificar este campo comparándolo con los registros de atribución de que dispone a fin de confirmar que en cada instante está transmitiendo la ONU correcta.

8.2.2.3 Campo Ind (Indicación)

El campo indicación proporciona a la OLT información de estado de la ONU en tiempo real. El formato del campo Ind es el que se indica a continuación.

Posición del bit	Función
7 (MSB)	PLOAMu urgente en espera (1= PLOAM en espera, 0 = no existe PLOAMs en espera)
6	Estado de FEC (1 = FEC ACTIVADO, 0 = FEC DESACTIVADO)
5	Estado de RDI (1 = Defectuoso, 0 = OK)
4	Tráfico en espera en las T-CONT de tipo 2
3	Tráfico en espera en las T-CONT de tipo 3
2	Tráfico en espera en las T-CONT de tipo 4
1	Tráfico en espera en las T-CONT de tipo 5
0 (LSB)	Reservado

Nótese que cuando la ONU ha indicado que una PLOAM urgente está en espera, la OLT debe transmitir una atribución ascendente que permita que la ONU transmita dicho mensaje PLOAM en el instante adecuado. El tiempo de respuesta debe ser inferior a 5 ms en funcionamiento normal.

Obsérvese asimismo que la ONU confirma el bit de PLOAMu en espera siempre que exista una o más células PLOAM en espera. El algoritmo de programación de la OLT debe tener en cuenta este hecho a la hora de determinar el momento en que debe transmitir las atribuciones PLOAMu.

La definición de las indicaciones de 'tráfico en espera' se dan en 8.4.

8.2.3 PLOAM ascendente (PLOAMu)

El campo PLOAMu tiene 13 bytes y contiene el mensaje PLOAM tal como se define en la cláusula 9. Este campo se transmite cuando lo indique el campo banderas de la estructura de atribución.

8.2.4 Secuencia de nivelación de potencia ascendente (PLSu)

El campo PLSu tiene 120 bytes y se utiliza para que la ONU realice medidas de control de potencia. Esta función sirve para ajustar los niveles de potencia de la ONU a fin de reducir el margen dinámico óptico recibido en la OLT. El contenido de este campo se fija localmente en la ONU, en función de su propio diseño. Este campo se transmite cuando lo indique el campo banderas de la estructura de atribución.

El mecanismo de control de potencia es útil en dos situaciones. Para determinar la potencia inicial y para modificar el modo de potencia del transmisor de la ONU. La primera sólo ocurre durante los procedimientos de activación de la ONU, mientras que la segunda tiene lugar durante el funcionamiento y durante la activación. Por lo tanto, el PLSu puede solicitarse en cualquier momento.

En numerosas ocasiones durante el proceso de activación, la OLT puede fijar el bit PLSu para la difusión de atribuciones destinadas a que las ONU configuren sus transmisores. Si la ONU no necesita utilizar el campo PLSu, en esos periodos desactiva su transmisor. Con ello se reducen las posibilidades de colisión.

En el caso de transmisión de PLSu durante el funcionamiento normal, la ONU debe, en general, transmitir según indique el campo PLSu. Por lo tanto, durante el funcionamiento normal la ONU debe transmitir el campo PLSu siempre que ello sea requerido, con independencia de la necesidad de realizar un ajuste del transmisor.

8.2.5 Informe de anchura de banda dinámica ascendente (DBRu)

La estructura de DBRu contiene información vinculada con la entidad T-CONT, no con la ONU. Este campo se transmite cuando lo indique el campo banderas de la estructura de atribución.

8.2.5.1 Campo asignación dinámica de anchura de banda (DBA)

El campo DBA contiene el estado del tráfico de la T-CONT en cuestión. A tal fin se reserva un campo de 8, 16, ó 32 bits. La codificación de los requisitos de anchura de banda de este campo (es decir, la correspondencia entre células/tramas en espera y números) se describe en 8.4. Obsérvese que la ONU debe transmitir el campo DBA con la longitud adecuada, aunque no se soporte el modo DBA, a fin de mantener la alineación de los elementos de la estructura.

8.2.5.2 Campo CRC

La estructura DBRu se protege utilizando un CRC-8, con el mismo polinomio que el indicado en la Rec. UIT-T I.432.1 ($g(x) = x^8 + x^2 + x + 1$). Sin embargo, a diferencia de la Rec. UIT-T I.432.1, no se realiza el OR exclusivo de la misma con 0x55. El receptor del campo DBRu implementa las funciones de detección y corrección de errores de CRC-8. Si el CRC-8 detecta la presencia de un error no corregible, se descarta la información de la DBRu.

8.2.6 Sección de cabida útil ascendente

Inmediatamente después del último campo de tara ascendente se encuentra la cabida útil ascendente GTC, que puede utilizarse para transportar células ATM, tramas GEM alineadas, o informes de DBA.

8.2.6.1 Cabida útil ATM ascendente

La cabida útil ascendente ATM contiene células ATM de 53 bytes. La longitud de esta cabida útil viene dada por la duración de la atribución menos el tamaño de las taras necesarias. La OLT debe intentar que los punteros se sitúen de tal forma que la cabida útil ATM sea siempre un entero múltiplo de 53 bytes. Si la cabida útil no contiene un número entero de células, la parte fraccional última está formada por bytes de relleno. En todo caso, las células están siempre alineadas con el inicio de la cabida útil (véase la figura 8-11).

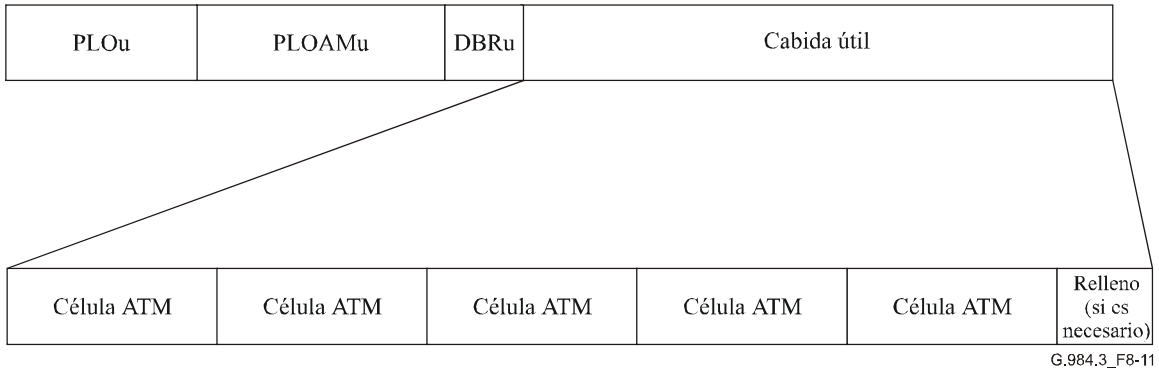


Figura 8-11/G.984.3 – Células ATM en sentido ascendente

8.2.6.2 Cabida útil GEM ascendente

La cabida útil GEM contiene cualquier número de tramas en modo trama GEM alineadas (figura 8-12). La longitud de esta cabida útil viene dada por la duración de la atribución menos el tamaño de las taras necesarias. La OLT debe mantener varios ejemplares de la máquina de estado de alineación GEM, y almacenar temporalmente las tramas fragmentadas hasta que se completen. El funcionamiento de la alineación de trama en GEM se describe en la 8.3.

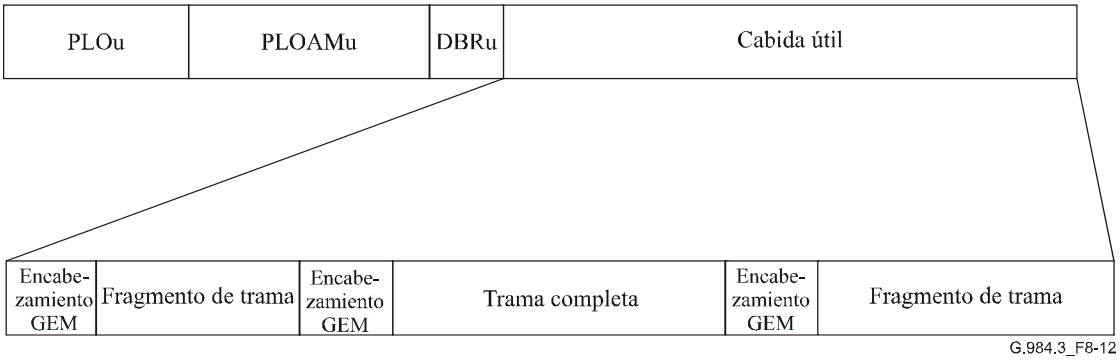


Figura 8-12/G.984.3 – Tramas GEM en sentido ascendente

8.2.6.3 Cabida útil DBA ascendente

La cabida útil DBA contiene un conjunto de informes de atribución dinámica de anchura de banda de la ONU en cuestión (figura 8-13). El primer informe DBA siempre está alineado de tal forma que su primer byte se encuentra al comienzo de la atribución. Todos los informes son contiguos. Si la longitud de la atribución no concuerda con la longitud total del informe, la ONU trunca el final

del último informe, o añade relleno de todos cero al final del último informe para compensar. La configuración, formato y utilización de estos informes se describe en 8.4. Obsérvese que la ONU debe responder a la atribución de cabida útil con DBA, aunque no se soporte el modo de DBA, a fin de mantener la alineación.

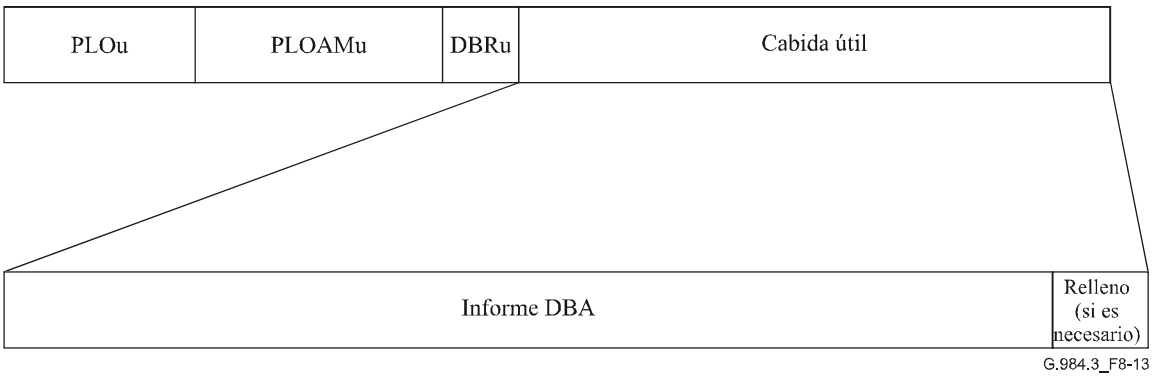


Figura 8-13/G.984.3 – Informe DBA en sentido ascendente

8.3 Correspondencia del tráfico en las cabidas útiles GTC

En la cabida útil GTC pueden transportarse diversos tipos de datos de usuario. Los protocolos portadores primarios son ATM y GEM. En cada uno de dichos protocolos portadores pueden transportarse varios servicios de usuario.

8.3.1 Correspondencia de células ATM en la cabida útil GTC

El tráfico ATM se transporta en el protocolo GTC de forma transparente. En sentido descendente, las células se transmiten desde la OLT a las ONU utilizando la partición de cabida útil ATM. La OLT puede atribuir en sentido descendente el tiempo que sea necesario para que todas las células se incluyan en la trama descendente. La subcapa de entramado ONU filtra las células entrantes en función del VPI, y entrega las células pertinentes al cliente ATM de la ONU.

En el sentido ascendente, las células se transmiten desde la ONU a la OLT utilizando el tiempo de atribución ATM configurado. La ONU almacena las células ATM conforme le llegan y las transmite en ráfagas de conformidad con la atribución de tiempo realizado por la OLT. La OLT recibe las células y las multiplexa con ráfagas de otras ONU, pasándolas a su cliente ATM.

8.3.1.1 Correspondencia de los servicios de usuario en ATM

Existen muchas Recomendaciones que describen la correspondencia de los servicios de usuario, tales como voz, servicios PDH, servicios Ethernet y otros, en un circuito virtual portador ATM.

8.3.2 Correspondencia de tramas GEM en la cabida útil GTC

El tráfico GEM se transporta mediante el protocolo GTC de forma transparente. En sentido descendente, las tramas se transmiten desde la OLT a las ONU utilizando la partición de la cabida útil GEM. En sentido ascendente, las tramas se transmiten desde la ONU a la OLT de acuerdo con el esquema de atribución de tiempo para GEM.

El protocolo GEM tiene dos funciones: proporcionar la alineación de las tramas de datos de usuario, y proporcionar la identificación de puerto y la multiplexación. Obsérvese que el término 'tramas de datos de usuario' denota tramas que se envían o se reciben de un usuario. Para ello se utiliza el encabezamiento GEM, tal como se muestra en la figura 8-14. El encabezamiento GEM contiene el indicador de longitud de cabida útil (PLI, *payload length indicator*), el ID de puerto (*Port ID*), el indicador de tipo de cabida útil (PTI, *payload type indicator*) y un campo de 13 bits de control de errores en el encabezamiento (HEC, *header error control*).

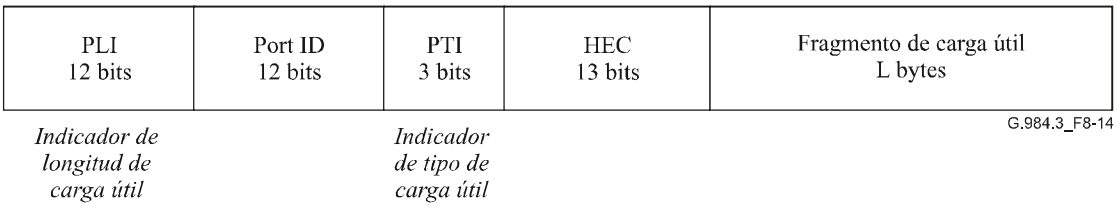


Figura 8-14/G.984.3 – Encabezamiento y estructura de trama GEM

El PLI indica la longitud en bytes, L, del fragmento de cabida útil que va a continuación de dicha cabecera. El PLI se utiliza para encontrar el siguiente encabezamiento en el flujo de datos y conseguir así la alineación. El tamaño de 12 bits de este campo permite que los fragmentos puedan ser de hasta 4095 bytes. Si las tramas de datos de usuario son más grandes, deberán descomponerse en fragmentos de menos de 4095 bytes.

El Port ID se utiliza para proporcionar 4096 identificadores de tráfico en la PON y realizar así la multiplexación del tráfico.

El campo PTI se utiliza para indicar el tipo de contenido del fragmento de cabida útil y su tratamiento más adecuado. La codificación de este campo de tres bits es similar a la utilizada en el encabezamiento ATM. Nótese que puesto que el transporte GEM sólo tiene lugar sobre el segmento G-PON, no es necesaria una indicación OAM extremo-a-extremo. Esto podría cambiar en el futuro, estando reservado el punto de código que permite esta función. La codificación es la que se muestra en el cuadro siguiente.

Código PTI	Significado
000	Fragmento de datos de usuario, no ha habido congestión, no es final de trama
001	Fragmento de datos de usuario, no ha habido congestión, es final de trama
010	Fragmento de datos de usuario, ha habido congestión, no es final de trama
011	Fragmento de datos de usuario, ha habido congestión, es final de trama
100	OAM GEM
101	Reservado
110	Reservado
111	Reservado

La información de congestión mediante los puntos de código 2 y 3 requiere estudios adicionales.

Para el punto de código 4, GEM reutiliza el formato de célula OAM especificado en la Rec. UIT-T I.610, es decir, soporta el fragmente de cabida útil de 48 bytes cuyo formato es el mismo que el descrito para las funciones OAM ATM.

Finalmente, el HEC proporciona funciones de detección y corrección de errores para el encabezamiento. El HEC que se utiliza es una combinación del código BCH(39, 12, 2) y un único bit de paridad. El polinomio generador para dicho código es $x^{12}+x^{10}+x^8+x^5+x^4+x^3+1$. El código BCH se calcula de tal forma que la división módulo 2 de los primeros 39 bits del encabezamiento (interpretado como un número de 39 bits, del que se transmite en primer lugar el bit más significativo) por el polinomio generador será cero en ausencia de errores. Si la división se implementa mediante un registro de desplazamiento, el valor de inicialización del mismo es todo ceros. El bit de paridad se fija en un valor tal que el número total de unos en todo el encabezamiento (40 bits) sea un número par. El proceso de decodificación del HEC de 13 bits se describe con más detalle en el apéndice III.

Una vez que el encabezamiento se ha ensamblado, el transmisor realiza el OR exclusivo del mismo con el patrón fijo: 0x0xB6AB31E055, y transmite el resultado. El receptor realiza el OR exclusivo de los bits recibidos con el mismo patrón fijo de bits a fin de recuperar el encabezamiento. Con ello se asegura que un conjunto de tramas sin servicio o de relleno tendrán el contenido suficiente como para permitir una alineación correcta.

El proceso de alineación que se realiza en G-PON requiere que exista un encabezamiento GEM al comienzo de cada partición GEM descendente y de cada cabida útil GEM ascendente. Así se garantiza que el receptor pueda encontrar el primer encabezamiento y encabezamientos ulteriores utilizando el PLI como puntero. En otras palabras, el receptor pasa inmediatamente al estado 'sync' (sincronismo) al comienzo de cada partición y cabida útil. Sin embargo, en el caso de que existan errores no corregibles en el encabezamiento, el proceso de alineación puede perder la sincronización con el flujo de datos. El receptor intentará volver a sincronizarse aplicando la máquina de estados que se muestra en la figura 8-15. En el estado captura, el receptor busca un HEC de encabezamiento GEM en todas las alineaciones (de bit y de byte). Cuando encuentra uno, pasa el estado pre-sync (presincronismo), en el que busca el HEC en el lugar indicado en el encabezamiento anteriormente detectado. Si existe concordancia con dicho HEC, pasa al estado Sync. Si no es así, pasa al estado captura. Obsérvese que las implementaciones específicas pueden opcionalmente tener varios ejemplares de estado Pre-sync, de forma que las discordancias de HEC no impidan que pueda detectarse el delimitador correcto. Asimismo, el proceso de recepción puede almacenar en una memoria intermedia los datos recibidos estando en el estado Pre-sync, y si finalmente el paso al estado sync es exitoso, puede asumirse que los datos almacenados constituyen un fragmento GEM válido.

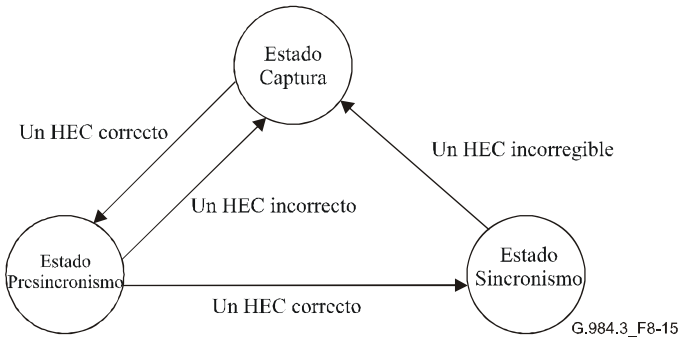


Figura 8-15/G.984.3 – Máquina de estados de alineación GEM

Para permitir el desacoplamiento de velocidad, se define una trama GEM sin servicio. Si no hay tramas de usuario para ser transmitidas, el proceso de transmisión genera dichas tramas sin servicio para rellenar los tiempos vacíos. El receptor las utiliza para mantener la sincronización y, por supuesto, no contienen datos que deban ser pasados al cliente GEM. El encabezamiento de trama GEM sin servicio se define como todo a ceros. Ello implica que el patrón realmente transmitido es 0xB6AB31E055, debido a la operación OR exclusivo (XOR) anterior a la transmisión.

Debido a la longitud aleatoria de las tramas de datos de usuario, el protocolo GEM debe soportar la fragmentación de las tramas de datos de usuario para permitir la inserción del encabezamiento GEM al comienzo de cada partición o cabida útil. Nótese que la fragmentación puede producirse en ambos sentidos, ascendente y descendente. Para este fin se utiliza el bit menos significativo del campo PTI del encabezamiento GEM. Cada trama de datos de usuario puede dividirse en un

conjunto de fragmentos. A cada fragmento se le antepone un encabezamiento, indicando el campo PTI el fragmento que contiene el final de la trama de datos de usuario. En la figura 8-16 se ilustran algunos casos de utilización del PTI.

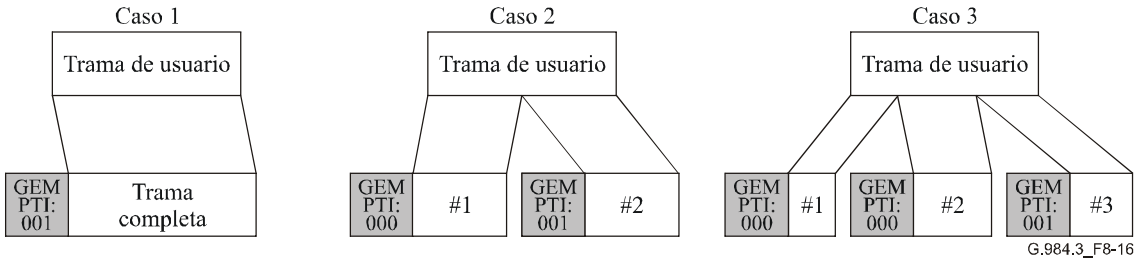


Figura 8-16/G.984.3 – Casos de utilización del campo fragmento

Es importante señalar que cada fragmento se transmite íntegramente en bloque. Es decir, un fragmento no puede superar los límites de una trama. Ello es una consecuencia natural del requisito de que cada partición o cabida útil GEM debe iniciarse con un encabezamiento. Por lo tanto, el proceso de fragmentación debe conocer la cantidad de tiempo que resta a la partición o cabida útil en curso de modo que fragmente adecuadamente sus tramas de datos de usuario. Otra implicación de ello es la transmisión de tramas sin servicio. En algunos casos, completar una trama de usuario previa puede dejar pendientes cuatro o menos bytes en la partición o cabida útil GTC, que es un tamaño inferior al tamaño mínimo de una trama GEM. En este caso, el proceso de transmisión envía un patrón de encabezamiento GEM de naturaleza descartable. El proceso de recepción reconoce que dicho encabezamiento es descartable y no lo tiene en cuenta. En cualquier caso, el alineamiento GEM se restaura correctamente al comienzo de la siguiente partición o cabida útil.

El proceso de fragmentación inherente de GEM puede utilizarse en el sistema GTC para dos fines. El primero ya se ha mencionado, es decir, para insertar un encabezamiento al principio de cada partición o cabida útil. Adicionalmente, la fragmentación permite que datos sensibles al tiempo, como por ejemplo el tráfico de voz, puedan descartar la transmisión de tráfico no sensible. En general, ambas utilizaciones de la fragmentación pueden implementarse en dos etapas de procesamiento diferentes, la primera para insertar el tráfico de carácter urgente, y la segunda para incluir encabezamientos que permitan acoplar a los mismos la partición/cabida útil GTC. Sin embargo, un método más sencillo es realizar un única etapa de fragmentación para ambas funciones. En esta situación, los fragmentos GEM de datos urgentes se envían siempre al comienzo de cada partición o cabida útil. Debido a que la trama GTC tiene una periodicidad de 125 µs, ello debería proporcionar una latencia suficientemente baja para los datos urgentes. En la figura 8-17 se ilustra esta configuración.

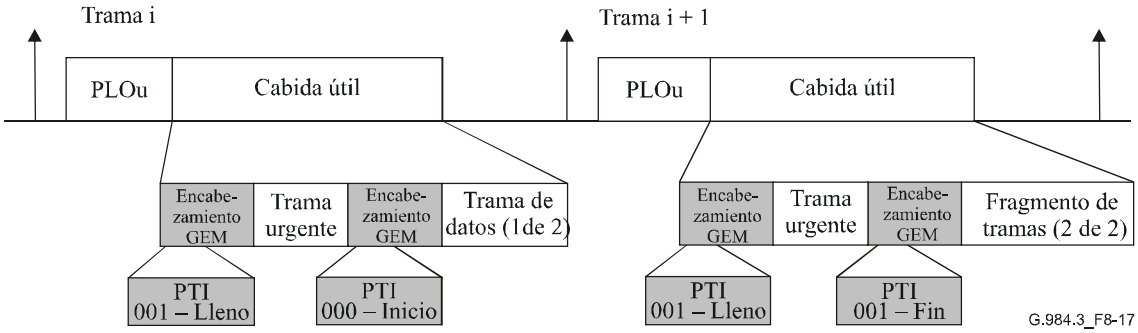


Figura 8-17/G.984.3 – Relación entre el entramado GEM y el entramado GTC

8.3.2.1 Correspondencia de señales de usuario en GEM

En el apéndice I se describe como se realiza la correspondencia de señales de usuario en el GEM.

8.4 Señalización y configuración de la atribución dinámica de anchura de banda

El sistema G-PON soporta la atribución dinámica de anchura de banda mediante el proceso de información de estado y de supervisión de tráfico de la OLT (es decir, sin información de estado). Todas las OLT proporcionan DBA de supervisión de tráfico, de forma que las ONU que no informan de estado dispongan de alguna funcionalidad DBA básica. En la DBA sin información, no son necesarias características de protocolo específicas y todo el mecanismo DBA está incluido en la OLT. Como tal, la DBA sin información de estado no se describe más en esta Recomendación; sin embargo, ello no le resta importancia. En caso de DBA con información de estado, existen tres mecanismos para la señalización de informes de DBA de la G-PON: las indicaciones de estado en el PLOu, los informes anexos o informes adosados a la DBRu y los informes ONU en la cabida útil de DBA. Estos mecanismos se describen a continuación.

Las indicaciones de estado proporcionan una indicación rápida pero sencilla del tráfico en espera en la ONU. La indicación se transporta en el campo Ind de PLOu. Existen cuatro informes de un único bit, uno para cada tipo de T-CONT. Con ello se pretende dar a la OLT una alerta rápida sobre la necesidad de supervisión DBA en dicha ONU, pero no se identifican las T-CONT específicas ni se proporciona información detallada, como por ejemplo, la anchura de banda.

Los informes adosados actualizan continuamente el estado del tráfico de un T-CONT específico. Este informe se transporta en el DBRu asociado a dicho T-CONT. Existen tres formatos para este tipo de informe (tipos 0, 1 y 2). El formato de informe de tipo 0 es el método soportado por defecto, siendo opcionales los demás métodos.

El informe de la ONU permite que ésta pueda transmitir un informe DBA en cualquiera de sus T-CONT, o en todos ellos, en una única transmisión. Ésta se transporta en una partición de cabida útil DBA dedicada en sentido ascendente atribuida por la OLT. Es opcional soportar este método.

Debido a que algunas de las funciones de información de DBA son opcionales, la OLT y la ONU deben realizar en el momento inicial un procedimiento de toma de contacto para negociar el tipo de informes DBA que serán utilizados. A tal fin, se utiliza el canal OMCI G-PON. Hasta que no finalice la toma de contacto no debe hacerse uso de las prestaciones que ofrece la DBA. No obstante, se consigue que el sistema de transporte sea resistente a fallos estableciendo el requisito de que la ONU siempre genere el formato correcto del informe solicitado por la OLT, con independencia de las posibilidades que ofrezca su DBA. A continuación se describen con detalle las opciones, su gestión y las condiciones de fallo.

8.4.1 DBA de indicación de estado

8.4.1.1 Definición del mensaje

El informe DBA de indicación de estado consta de cuatro bits en el campo Ind de PLOu. Se transmite en todas las transmisiones ascendentes de la ONU. Cada bit corresponde a un tipo diferente de T-CONT. Si el bit se pone a uno para el tipo X de T-CONT, la OLT asume que existen datos en espera en al menos una de las memorias intermedias de T-CONT de tipo X. Si la ONU tiene más de un T-CONT de dicho tipo, el bit es el resultado de aplicar la función lógica OR del estado de todas las memorias intermedias. En tal caso, la OLT no conocerá cuál es el T-CONT que tiene datos en espera, y necesitará tomar acciones adicionales.

Para los tipos 2 a 4 de T-CONT, el contrato no incluye una componente de anchura de banda fija. Por lo tanto, si en dichos T-CONT hay datos en espera, el bit correspondiente se pone a uno. Sin embargo, el tipo 5 de T-CONT es especial en el sentido que su memoria intermedia puede contener datos que pertenezcan a la parte de anchura de banda fija de su contrato. Los datos de anchura de banda fija no deben hacer producir una indicación de estado, ya que ello haría que la indicación

estuviera siempre puesta a uno. Por lo tanto, para los T-CONT de tipo 5, sólo la presencia de datos de anchura de banda no fija hace que el bit de indicación se ponga a uno.

Estas indicaciones de estado están destinadas a proporcionar a la OLT un aviso rápido de que existen datos en espera. Sin embargo, el algoritmo DBA de la OLT no necesita dichas indicaciones para conceder anchura de banda a las ONU, pues dicho requisito podría añadir retardos a la provisión de anchura de banda inicial a las ONU.

8.4.1.2 Opciones de la ONU y la OLT

Las ONU y las OLT pueden soportar o no esta forma de información de la DBA. Si la ONU no soporta este modo de información, debe tener siempre los bits puestos a cero. Nótese que si una ONU no soporta un tipo determinado de T-CONT, el bit puede estar siempre puesto a cero. El diseño de la OLT debe tener en cuenta el hecho de que algunas implementaciones de la ONU pueden tener todos sus indicaciones de estado puestas a cero durante todo el tiempo. Si la OLT no soporta este modo, se ignoran los bits de estado.

8.4.1.3 Tratamiento de casos excepcionales

Debido a que este modo de información utiliza bits en posiciones fijas de una estructura existente, los desacuerdos en relación con el soporte de este modo no dan lugar a errores de alineación. El algoritmo de la OLT debe diseñarse de forma que pueda tratar ambos tipos de ONU.

8.4.2 Informes DBA adosados del DBRu

8.4.2.1 Definición del mensaje

El informe DBA adosado consta de un mensaje de 1, 2 ó 4 bytes que especifica el volumen de datos en espera en la memoria intermedia del T-CONT correspondiente al Alloc-ID que ha generado la transmisión del DBRu. La OLT genera la transmisión del DBRu fijando el punto de código adecuado en el campo banderas de la estructura de atribución del mapa de anchura de banda. El CRC-8 del DBRu abarca el informe.

El mensaje informe utiliza como unidad básica el número de células ATM o de bloques GEM en espera en la memoria intermedia del T-CONT. Tal como se describe en el apéndice II/G.983.4, se permiten los tres formatos G.983.4 siguientes:

- Modo 0: con un único campo que informa de la cantidad total de datos en la memoria intermedia T-CONT.
- Modo 1: con dos campos, el primero informa de la cantidad de datos con "testigos PCR" (1 byte), y el segundo informa de la cantidad de datos con "testigos SCR" (1 byte) en la memoria intermedia T-CONT. Este tipo de informe es adecuado para los T-CONT de tipo 3 y 5.
- Modo 2: con cuatro campos, el primero contiene la codificación no lineal del número total de células de clase T-CONT#2 que tienen testigos PCR (anchura de banda garantizada) (1 byte). El segundo campo contiene la codificación no lineal del número total de células de clase T-CONT#3 que tienen testigos SCR (anchura de banda garantizada) (1 byte). El tercer campo contiene la codificación no lineal del número total de células de clase T-CONT#3 que tienen testigos PCR (anchura de banda no garantizada) (1 byte). El cuarto campo contiene la codificación no lineal del número total de células de clase T-CONT#4 que tienen testigos PCR (la anchura de banda posible, "*best effort*") (1 byte). Este tipo de informe utiliza cuatro bytes en total. Es adecuado para la información de T-CONT de tipo 5, o para que las ONU proporcionen información resumida de todos los T-CONT incluidos en un único mensaje.
- En los modos 1 y 2, "PCR" y "SCR" representan la anchura de banda máxima y la anchura de banda garantizada de las conexiones subyacentes, respectivamente. Éstas se especifican

en células para conexiones ATM o en bloques de información de longitud fija en el caso de conexiones GEM.

Todos los tipos de informes utilizan un campo común de un byte de longitud para transmitir el número de células o de bloques que se encuentran en la memoria intermedia. El campo información se configura en base a este campo en mini-intervalos tal como se especifica en la Rec. UIT-T G.983.4. Sin embargo, se especifica un código no válido en lugar de un código de reserva de la Rec. UIT-T G.983.4 de forma que la ONU pueda indicar que no puede informar del valor real. En el cuadro 8-1 se incluyen los puntos de código revisados.

Cuadro 8-1/G.984.3 – Puntos de código en los campos de información de DBA

Longitud de la cola	Entrada binaria (ONU)	Codificación del octeto	Salida binaria (OLT)
0-127	00000000abcdefg	0abcdefg	00000000abcdefg
128-255	00000001abcdefx	10abcdef	00000001abcdef1
256-511	0000001abcdexxx	110abcde	0000001abcde111
512-1023	000001abcdxxxxx	1110abcd	000001abcd11111
1024-2047	00001abcxxxxxxx	11110abc	00001abc1111111
2048-4095	0001abxxxxxxxxx	111110ab	0001ab111111111
4096-8191	001axxxxxxxxxxx	1111110a	001a11111111111
>8191	01xxxxxxxxxxxxx	11111110	011111111111111
No válido	N/A	11111111	N/A

La longitud de la cola del cuadro 8-1 refleja el número de células en el caso de ATM y el número de bloques de información, que por defecto es de 48, en el caso de GEM, que existen en la memoria intermedia T-CONT. Aunque la estructura de la cola depende de la implementación específica, el concepto de memoria intermedia T-CONT es el mismo que el indicado en 1.3/G.983.4.

NOTA – Información en GEM.

En el caso de GEM, la longitud del paquete se normaliza con respecto al número de bloques de información. El número de bloques de información de longitud B se obtiene mediante un proceso de redondeo al alza. En resumen, si en la memoria intermedia T-CONT se almacenan k paquetes de longitud L_i (i = 1,..., k), el valor del que se informa, R, se calcula de la forma siguiente.

$$R = \text{int}\left(0{,}99 + \frac{1}{B}\sum_{i=1}^{k} L_i\right)$$

donde int() es una función que devuelve la parte entera de su argumento.

8.4.2.2 Opciones disponibles en la ONU y la OLT

Es opcional que la ONU soporte la información de DBA adosada. Si no la soporta, debe soportar el formato de información modo 0. Opcionalmente puede soportar los modos 1 y 2, o ambos. La OLT debe soportar el modo 0 de DBA adosada y, opcionalmente, puede soportar los modos 1 y 2.

La OLT conoce las capacidades de la ONU a través del OMCI. En función de las capacidades de la ONU y de las suyas propias, la OLT puede fijar el modo de información de cada T-CONT. La ONU puede así responder de la forma normal a la atribución de DBRu (estando fijado el valor del bit bandera).

8.4.2.3 Tratamiento de casos excepcionales

La OLT no debe transmitir una atribución DBRu que solicite un formato incorrecto de DBRu. La OMCI controla el formato del DBRu. Sin embargo, debido a desconfiguraciones o transitorios de conmutación, la OLT puede solicitar un DBRu de un tipo que la ONU no espera o que no soporta. En ese caso, la ONU debe responder con el formato del DBRu solicitado en la atribución, pero debe rellenar todos los campos en el formato erróneamente solicitado con el código no válido. La OLT interpreta entonces que se trata de un error e ignora el DBRu. Es importante señalar que la OLT debe mantener la alineación de la ráfaga, ya que la longitud del DBRu transmitido por la ONU siempre concuerda con el valor esperado por la OLT.

8.4.3 DBA con informe de ONU completa

8.4.3.1 Definición del mensaje

El informe de DBA de ONU completa permite a la ONU transmitir informes de DBA para cualquiera de sus T-CONT. A diferencia del método adosado, el método de ONU completa da a la ONU libertad para seleccionar los T-CONT de los que desea informar. En general, esto permite que la OLT prepare una cabida útil DBA considerablemente más pequeña que la necesaria para informar de todos los T-CONT de la ONU. Los T-CONT puede disputarse entonces el tiempo de información, pudiendo la ONU tomar las decisiones de planificación más adecuadas.

Los formatos de los informes son similares a los utilizados en el DBRu, añadiéndose a los informes dos bytes que transportan el Alloc-ID correspondiente al informe T-CONT, y dos copias de la indicación del modo DBRu (utilizando los mismos puntos de código definidos para el campo bandera del Alloc-ID), tal como se muestra en la figura 8-18. Puesto que la OLT no conoce el formato del informe, debe haber una tolerancia adicional frente a errores en la indicación del modo del DBRu. En el formato que se muestra en la figura 8-18, esta información se expresa tres veces. Existen dos copias explícitas en las indicaciones del modo DBRu, y una copia implícita en el Alloc-ID, ya que cada Alloc-ID tiene un modo asociado. Por tanto, la OLT puede comparar las tres indicaciones de formato y tomar una decisión por voto mayoritario para determinar la longitud del informe. Este resultado puede ser confirmado por la presencia del CRC-8 en la ubicación predicha. Si la OLT pierde la alineación, ya sea por una decisión de formato DBRu incompleto o por un error no corregible por el CRC, en general, la OLT descarta el resto del informe de DBA. Nótese que para ello es necesario que se produzcan dos bits erróneos.

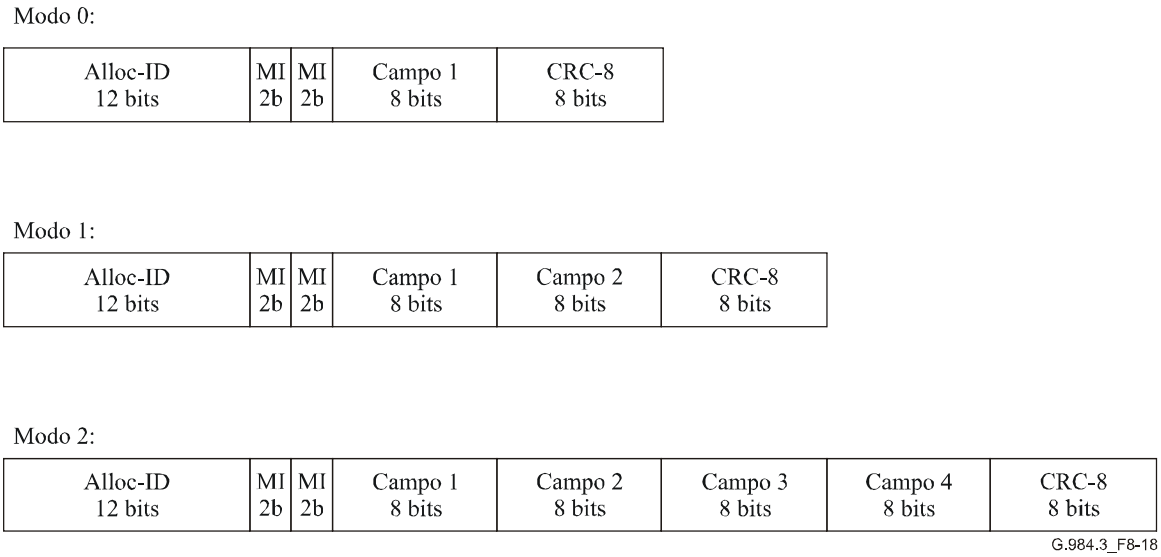


Figura 8-18/G.984.3 – Formatos de los tres informes para la función DBA de ONU completa

Las estructuras del informe de DBA de ONU completa se protegen con un CRC-8 que utiliza el mismo polinomio que el indicado en la Rec. UIT-T I.432.1 ($g(x) = x^8 + x^2 + x + 1$). Sin embargo, a diferencia de la Rec. UIT-T I.432.1, no se realiza el OR exclusivo del polinomio CRC con 0x55. La OLT implementa las funciones de detección y corrección de errores del CRC-8. Si el CRC-8 indica que ha ocurrido un error no corregible, se descarta la información de la estructura.

8.4.3.2 Opciones disponibles en la ONU y la OLT

La capacidad de información de ONU completa es opcional para la ONU y la OLT. La OLT detecta las capacidades de la ONU a través del OMCI. Conocidas éstas, la OLT puede asignar un nuevo Alloc-ID y configurarlo para la información de DBA de ONU completa. La ONU debe ser capaz de responder al Alloc-ID de una forma normal.

8.4.3.3 Tratamiento de casos excepcionales

La OLT no debería intentar configurar un Alloc-ID para la información de DBA completa si la ONU no soporta dicha función. No obstante, si lo hace, la ONU responde a la atribución, pero rellena la cabida útil con todos cero, tal como haría si no tuviera informes que transmitir. La OLT recibe esta transmisión sin incidentes y la descarta.

9 Mensajes GTC

Esta cláusula se centra en los mensajes de OAM de la capa física.

Existen tres métodos para transportar información entre la estación de gestión de red, la OLT y las ONU:

Canales OAM integrados. Se definen varios campos en las estructuras de trama en sentido descendente y ascendente. Estos campos transportan información en tiempo real tal como intercambio de seguridad, DBA y supervisión de la BER del enlace. Se describen en la cláusula 8.

Mensajes PLOAM. La OLT puede mandar a las ONU un mensaje dedicado de 13 bytes en sentido descendente, y las ONU enviar otro en sentido ascendente a la OLT con las funciones OAM de que disponen. Se describen en esta cláusula.

Información OAM con OMCI transportada en un canal GEM dedicado o en un VPI/VCI ATM dedicado. El método exacto de transporte se describe en la cláusula 14. La sintaxis del OMCI se describe en la Recomendación relativa a la OMCI de G-PON.

9.1 Formato del mensaje PLOAM

Las alarmas de OAM o alertas producidas por haberse superado determinados umbrales, se transportan en mensajes incluidos en el campo PLOAM de 13 bytes. Asimismo, todos los mensajes sobre las activaciones se mapean en el campo mensaje del campo PLOAM.

La estructura del mensaje GTC se muestra en la figura 9-1, y se define sobre la base de las definiciones siguientes.