

# Chapter 2

## Legacy Digital Networks

### 2.1 Introduction to Digital Networks

The aim of this Chapter is to survey the first digital networks, which were suitable for transporting data (or, in general, multimedia) traffic [1]. In particular, we will consider the data network based on the X.25 standard [2]. Then, we will focus on the ISDN network and on its special evolution for data transfer, based on the Frame Relay protocol [3–5]. Finally, we will consider the B-ISDN network and the related ATM protocol [6–8]. This Chapter has a preparatory value, providing basic concepts, which will also be applied to the Internet, as shown in Chap. 3 (e.g., key concepts are flow control, traffic shaping, buffer management, etc.).

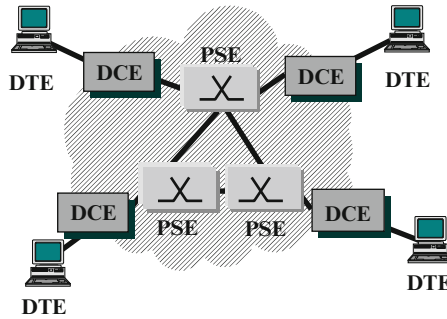
#### 2.1.1 X.25-Based Networks

X.25 is an ITU-T Recommendation defined in 1976 and subsequently refined [1]. This specification defines the protocols for synchronous transmissions between a user terminal (here named Data Terminal Equipment, DTE<sup>1</sup>) and a first network equipment (here named Data Circuit-terminating Equipment, DCE). The packet data network connecting all the DCEs is based on Packet-Switching Exchange (PSE) elements. The network architecture is shown in Fig. 2.1. No details are given on the protocols employed in the network interconnecting DCEs. However, the X.75 protocol by ITU-T (specifying the protocols for the communication between two packet-switched data networks) can be used in this network [9]. Even if X.25

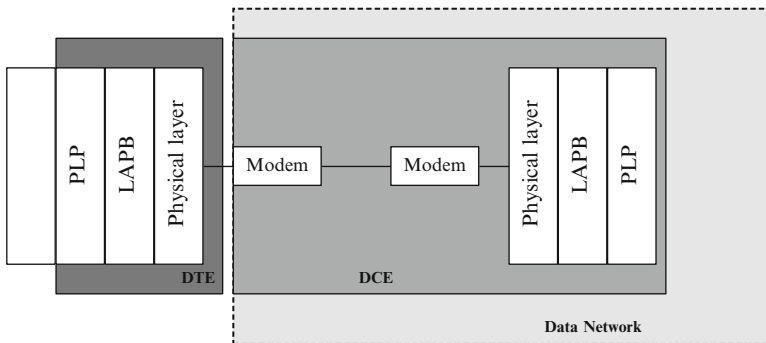
---

The online version of this chapter (doi:[10.1007/978-1-4614-4084-0\\_2](https://doi.org/10.1007/978-1-4614-4084-0_2)) contains supplementary material, which is available to authorized users.

<sup>1</sup> DTE is the part of a data-processing machine, which can transmit data over a communication circuit. A DTE is generally attached to a DCE (network side) in order to send and receive data over the communication facility.



**Fig. 2.1** X.25 network architecture



**Fig. 2.2** DTE on the user side and DCE on the network side. Note that the protocol architecture at the DTE is mirrored with respect to that on the DCE

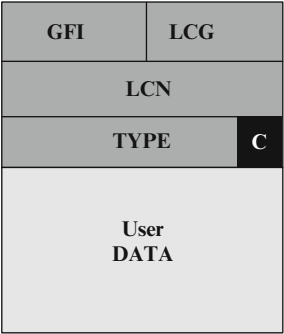
defines the protocol stack at the user interface, it is common to use the term “X.25 network” to denote the whole network with DCEs and PSEs. X.25 addresses are defined in the ITU-T X.121 Recommendation.

Typical applications of X.25 included automatic teller machine networks and credit card verification networks.

The subdivision of X.25 network protocols into layers was at the basis of the OSI model. In particular, X.25 is a connection-oriented protocol, which defines the first three layers of the OSI architecture, that is physical, data, and network layers, called in this standard as *physical*, *frame*, and *packet* layers, respectively. These layers are described below (see Fig. 2.2).

1. *Physical layer*: It is based on the X.21 protocol, which is similar to the serial transmissions of the RS-232 standard (ITU V.24). X.21 is an ITU recommendation for the operation of digital circuits [10]. The X.21 interface uses eight interchange circuits (i.e., signal ground, DTE common return, transmit, receive, control, indication, signal element timing and byte timing); their functions are defined in Recommendation X.24 [11] and their electrical characteristics are described in Recommendation X.27 [12].

**GFI** = General  
Format Identifier  
**LCG** = Logical  
Channel Group  
number  
**LCN** = Logical  
Channel Number  
**TYPE** = packet Type  
identifier  
**C** = Control bit  
(equal to 1)



**Fig. 2.3** Format of a control packet (layer 3). A data packet has a similar format, except for the field “type” (where different fields are used for the flow control scheme: send and receive sequence numbers and indication of a packet being part of a sequence) and the control bit equal to 0

- 2. *Data link layer*: It employs the Link Access Protocol-Balanced (LAP-B), a subset of the High Level Data Link Control (HDLC) protocol in its balanced version, meaning that both parts can start a new transmission without needing the authorization of the other part.
- 3. *Network layer*: The Packet Layer Procedure (PLP) is adopted. The transfer of information between two DTE devices attached to a packet switched network depends on PLP. The PLP layer communicates between DTE devices by means of units, called packets.

Note that information and control messages share the same protocol layers in X.25; this is what is called “in-band signaling”.

The data PDU generated by the end-user reaches the network layer where a header is added for addressing purposes (logical channel identifier). The X.25 packets (layer 3) have different lengths. A packet begins with a 3-byte header (see Fig. 2.3); the first two bytes contain Group and Channel fields, forming together a 12-bit virtual circuit number. Then, the packet is received at layer 2: LAPB encapsulates the data PDU coming from network layer by including a header and a trailer for error correction. Then, this information is managed by the physical layer. The transmission capacity for a DTE typically ranges from 75 to 192 kbit/s; however, there are also examples where the access speed reaches 2 Mbit/s. In Italy, the X.25 network was named ITAPAC. Other X.25 networks were available in the World since early 1980s.

In the X.25 protocol stack, layer 2 provides error control. Moreover, both layers 2 and 3 implement two independently operated flow control techniques. Flow control is needed to avoid overwhelming the receiver with too much data. Error control is adopted to verify whether the data have been received correctly; in the presence of errors, a retransmission is requested. Due to error and flow controls, we may understand that X.25 entails a heavy overhead.

Each frame sent over a particular link is saved in a buffer until its information has been checked and the frame has been approved by the receiving node.

LAPB is a bit-oriented protocol, which ensures that frames are correctly ordered and error-free. LAPB adopts an ARQ scheme to recover the erroneous frames on each link (in the LAPB frame there are two bytes -Frame Check Sequence field-used for error detection). Both Go-Back-N and Selective Repeat schemes can be adopted to manage retransmissions. A sliding window technique is integrated with the ARQ scheme to operate flow control: assuming a maximum window size of  $n$  frames, the sender can send up to  $n$  frames before stopping transmissions, waiting for an acknowledgment (which allows sliding the window).

There are three types of LAPB frames: information, supervisory, and unnumbered.

- The information frame (I-frame) carries upper-layer information and some control information. I-frame functions include sequencing, flow control, error detection, and recovery.
- The supervisory frame (S-frame) carries control information. S-frame functions include requesting and suspending transmissions, reporting on status, and acknowledging the receipt of I-frames.
- The unnumbered frame (U-frame) carries control information. U-frame functions include link setup and disconnection, as well as error reporting. U frames do not have sequence numbers.

The layer 3 protocol (PLP) supports a flow control task to ensure that a source DTE does not overwhelm the destination DTE, and to maintain timely and efficient delivery of packets. Flow control is operated for each virtual circuit, differently from LAPB, which provides flow control independently of virtual circuits (it does not know what is a virtual circuit; LAPB just controls all the traffic on a link). The destination DTE has to send an acknowledgment for each packet received. PLP adopts a sliding window flow control mechanism like that used by LAPB [1]; the PLP max window size is either 8 or 128 packets.

The DCE sends the received packets to the local PSE, which inspects the destination address contained in the packet. Each PSE contains a routing directory specifying the outgoing links to be used for each network address.

Each node stores the packets in a buffer before processing and transmitting them on the appropriate output link at the highest bit-rate available. This method is referred to as *store and forward*. The packet management procedure at the nodes consists primarily in checking the packet format, selecting an outgoing path, checking for errors, and waiting for available capacity on the outgoing link.

The PLP protocol is connection-oriented with two possible services: Switched Virtual Circuit (SVC) and Permanent Virtual Circuit (PVC). In the first case, the exchange of data between source and destination requires the setup of a path, which connects these network end-points; a release procedure must be performed when the call ends.

PLP operates in five distinct modes: call setup, data transfer, idle, call clearing, and restarting.

- *Call setup mode* is used to establish SVCs between DTEs. PLP uses the X.121 addressing scheme to set up the virtual circuits [13]. The call setup mode is executed on a per-virtual-circuit basis. This mode is only used for SVCs, but not for PVCs.
- *Data transfer mode* is adopted to transfer data between two DTEs across a virtual circuit. In this mode, PLP handles segmentation and reassembly, bit padding, error and flow control. This mode is executed on a per-virtual-circuit basis for both PVCs and SVCs.
- *Idle mode* is used when a virtual circuit is established, but there is no data transfer. It is executed on a per-virtual-circuit basis and is used only for SVCs.
- *Call clearing mode* is needed to terminate communication sessions between DTEs. This mode is executed on a per-virtual-circuit basis and is used only for SVCs.
- *Restarting mode* is used to synchronize the transmission between a DTE device and a locally connected DCE device. This mode is not executed on a per-virtual-circuit basis. It affects all the established virtual circuits.

A Logical Channel Group (LGC) of 4 bits and a Logical Channel Number (LCN) identifier of 8 bits are assigned to each SVC and PVC. LGC and LCN together form a virtual circuit number; a DTE may have up to 4,095 ( $=2^{12}-1$ ) virtual circuits at a time. Packets of different virtual circuits share the same physical resources on the links.

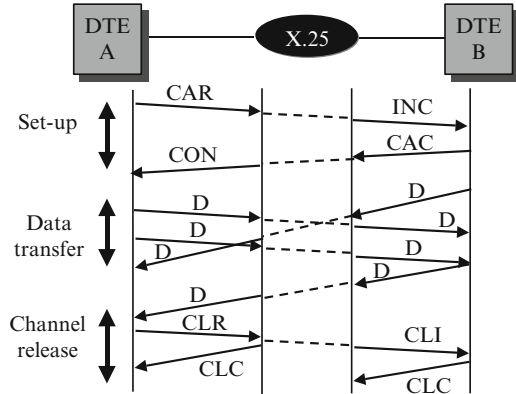
X.75 is a signaling system used to interconnect packet-switched network elements (such as X.25) on international circuits [9]. It permits the transfer of call control and network control information as well as of user traffic. On layer 2, X.75 uses LAPB in the same way as X.25. On layer 3, X.75 is almost identical to X.25.

Asynchronous terminals can also be connected to X.25 networks. These devices (e.g., a character-mode terminal) are too simple to implement the full X.25 functionality. Hence, a Packet Assembler & Disassembler (PAD) must be interposed between DTE and DCE. PAD performs three primary functions: buffering (storing data until a device is ready to process them), packet assembly, and packet disassembly. PAD buffers data to be sent to or to be received from the DTE device. It also assembles outgoing data into packets and forwards them to the DCE. PAD provides protocol conversion, and transparent service for DTEs. X.3, X.28, and X.29 protocols are used as interface between asynchronous terminals and packet networks [14–16].

The procedure to set up a layer 3 connection (SVC) and for the exchange of data is described in Fig. 2.4. The following signaling messages are involved: CAR (call request), CAC (call accepted), INC (incoming call), CON (call connected), CLI (clear indication), CLR (clear request), and CLC (clear confirmation). Symbol D denotes the transfer of a layer 3 data packet.

As a final consideration, we can state that X.25 was born in mid 1970s, with the support of telecom carriers in response to the ARPANET datagram technology. X.25 (as well as Frame Relay described in Sect. 2.1.3) can be used to carry IP datagrams; thus, X.25 is seen as a link layer protocol by the IP layer. Along the path,

**Fig. 2.4** Procedures for the exchange of data (SVC)

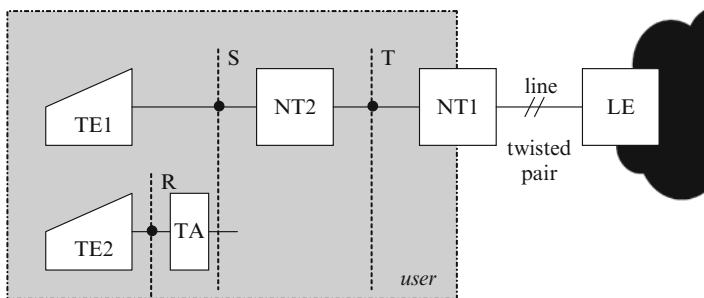


LAPB error control (with retransmissions) on each hops, and hop-by-hop flow control entail a heavy protocol overhead. Putting “intelligence into the network” made sense in mid 1970s, when very simple terminals were available. Today, the adoption of a quasi-error-free transmission medium (like optical fibers) favors pushing “intelligence to the edges”. This is the reason why the X.25 technology quickly disappeared.

### 2.1.2 ISDN

A fundamental step in the evolution of telephone networks is the conversion started at the beginning of 1960s from analog technology to a packet-based, digital switching system. In these networks, the distribution (access) network is still analog, whereas the backbone network connecting the switching units is numeric. Hence, the Public Switched Telephone Network (PSTN) needs a digital-to-analog conversion (modem) if a data stream has to be transmitted. Moreover, another conversion has to be carried out in the network when the analog voice signal reaches the digital core part of the network. This is a very inefficient approach, especially with the increasing number of telecommunication services that a user may need to access. In order to solve this problem, a numeric access even from user premises is needed, thus allowing a unified system to support voice and different types of data transitions. A computer can thus be connected to the network with a baseband link, without using a modem. This technology is provided by the Integrated Services Digital Network (ISDN) [3–5], which has been standardized by ITU-T in 1980s according to the following areas:

- Protocols of family “E” deal with telephone network standards for ISDN. For example, E.164 describes international addressing for ISDN.
- Protocols beginning with “I” deal with concepts, terminology, and general methods. The I.100 series includes general ISDN concepts and the structure of



**Fig. 2.5** User access architecture to the ISDN network (basic rate access case)

other I-series Recommendations; I.200 deals with service aspects of ISDN; I.300 describes network aspects; I.400 describes the User-Network Interface (UNI); I.500 deals with network internal interfaces; I.600 focuses on network management principles.

- Protocols beginning with “Q” address switching and signaling. Q.921 describes ISDN layer 2 functions; Q.931 specifies layer 3 functions.

The ISDN network still employs the twisted pair medium (of PSTN) for the access of users; moreover, ISDN substitutes the common channel Signaling System No. 7 (SS#7) with an enriched signaling set.

ISDN supports both circuit-switching and packet-switching, an essential characteristic to manage different service types with related digital traffic flows.

### 2.1.2.1 The User Access Architecture

The end-user will be connected to the ISDN network (i.e., the Local Exchange, LE) by means of a twisted pair, which arrives at a Network Termination 1 (NT1). Moreover, the Terminal Equipment (TE) uses a Network Termination 2 (NT2) to connect to NT1. A non-ISDN terminal equipment can also be connected by means of a Terminal Adaptor (TA). See Fig. 2.5.

NT1 supports all the functions of a network termination. In particular, it operates at OSI layer 1 (termination of the transmission line, management of the clock, channel multiplexing on the line).

NT2 has the functionalities of layers 1, 2, and 3. For instance, NT2 can be an ISDN Private Automatic Branch eXchange (PABX). NT2 functionalities cannot be divided between TE and NT1.

TE has all the seven layers of the OSI protocol stack. TE is equivalent to DTE in X.25 networks; the only difference is that a TE in the ISDN network is not simply a data terminal, but may generate multimedia traffic. Two different types of TEs are possible: TE1 with ISDN interface and TE2 without ISDN interface. In the TE2 case, we consider the possibility to connect to the network an old non-ISDN terminal, which needs an adaptor (sometimes incorrectly called “ISDN Modem”).

There are some important reference points between the different blocks in Fig. 2.5: that is, R, S, and T. Suitable interfaces correspond to these different reference points. Some blocks can be combined in implementations, so that there is the need to identify the functions at each reference point. Interfaces S and T must be equal, so that it is possible to connect directly TE1 with NT1 without using NT2 (e.g., without interposing a PABX). Many T lines can be connected to the NT1; analogously, many S lines can be connected to the NT2. The number of S lines and the number of T lines can be different. Since most homes do not have any NT2 equipment, S and T reference points are usually coincident and are identified as S/T.

In Europe and Japan, the operators own the NT1 and provide the S/T interface to customers. Instead, in North America, largely due to the U.S government's unwillingness to allow telephone companies to own customer premises equipment (such as NT1), the U interface (i.e., the interface between NT1 and LE) is provided to the customer, who owns the NT1. Hence, there are actually two incompatible variants of ISDN; some manufacturers have attempted to remedy by implementing devices, which contain both S/T and U jacks. Of course, if NT1 is property of the telecommunication network, T is the border point between users' responsibilities and network ones.

### 2.1.2.2 ISDN Access Structures

The flux of bits on the line connecting the user to the network (reference points S and T) is composed of different time-multiplexed channels. The different types of channels and their combinations (i.e., access structures) are defined in the ITU-T I.412 Recommendation [17]. There are basically two different channel types in ISDN:

- Channel B at 64 kbit/s. It transparently transports the flux of bits from one end to another in the network according to circuit-switching. Hence, only the physical layer is needed for B-channels in the switches within the network.
- Channel D at 16 or 64 kbit/s. This channel is packet- (message-) switched. Hence, at each node of the network, all the first three OSI layers (i.e., 1, 2, and 3) are needed to manage the flux coming from a D-channel. Such channel is used to send both signaling messages and user packet data.

There are two basic types of ISDN access structures:

- Basic Rate Interface (BRI) [18], which consists of two 64 kbit/s B-channels and one 16 kbit/s D-channel for a total bit-rate of 144 kbit/s:  $2B + D$ . This basic service is intended to meet the needs of most individual users.
- Primary Rate Interface (PRI) [19] for users requiring a higher capacity. This channel structure has 23 B-channels in USA and 30 B-channels in Europe plus one 64 kbit/s D-channel (totally, 1,536 kbit/s in USA and 1,984 kbit/s in Europe):  $23B + D$  and  $30B + D$ , respectively.



To access the BRI service, it is necessary to subscribe to an ISDN phone line. A customer must be within about 5.5 km of the telephone company central office; beyond that distance, expensive repeaters are needed or ISDN BRI services may not be available at all.

Finally, there are other access possibilities, denoted by letter H, where different combinations of B-channels are allowed:

- H0 = 384 kbit/s (6 B-channels)
- H10 = 1,472 kbit/s (23 B-channels)
- H11 = 1,536 kbit/s (24 B-channels)
- H12 = 1,920 kbit/s (30 B-channels)—International (E1) only

The network is typically unable to switch H-channels so that they require a permanent connection.

### 2.1.2.3 Services

ITU-T I.210 Recommendation describes the basic concepts on ISDN services [20]. There are three different types of services: bearer services, teleservices, and supplementary services.

#### Bearer Services

A bearer service has the task to transfer digital information between end-points (S or T) across the network. Bearer services are described in Recommendations from I.230 to I.233. Bearer services entail protocols for OSI layers 1, 2, and 3. The network acts as a relay system operating at layers 1, 2, or 3, depending on the cases described below.

- Circuit services (the network is a physical relay system) can be detailed as:
  - Transparent 64 kbit/s digital circuit.
  - 64 kbit/s non-transparent circuit for voice traffic. In this case, the network may employ some analog parts, thus requiring a digital-to-analog and an analog-to-digital conversion along the path to reach the destination in numeric format.
  - Transparent  $2 \times 64$  kbit/s digital circuit. This is the service where the network manages independently two connections at 64 kbit/s, which will be combined at the destination for re-obtaining the original flux at 128 kbit/s. Such service is well suited to video-telephony.
  - Transparent digital circuit at 384 kbit/s or 1,920 kbit/s. Practically this service is unused.

- **Frame mode service:** the network operates as a relay at layer 2. This name is due to the fact that packet data units are also named frames at layer 2. Two different sub-cases are possible:
  - *Frame switching*, where the network has a complete layer 2 protocol.
  - *Frame relaying*, where only part of layer 2 (i.e., the lower part) is implemented inside the network. Hence, the following functionalities are not supported within the network, but only end-to-end: acknowledgment of packets, recovery of erroneous packets, flow control.
- **Packet mode service:** the network operates a relay at layer 3, i.e., a packet-switched network. Three different services should be supported, such as virtual circuit, connectionless transfer, and signaling. Practically, only the virtual circuit service has been implemented, employing the corresponding protocol of X.25 at layer 3 (i.e., PLP).

## Teleservices

A teleservice entails an end-to-end communication accessed at S or T reference points. Teleservices involve OSI protocols from layer 1 to layer 7. Teleservices rely on bearer services for the transport of information from one end to another end of the network. Typical examples of teleservices are (ITU-T I.240 and I.241 Recommendations): telephony, videotelephony, facsimile. Practically, the ISDN network provides the bearer service, whereas TE1 implements the protocol layers of the teleservice.

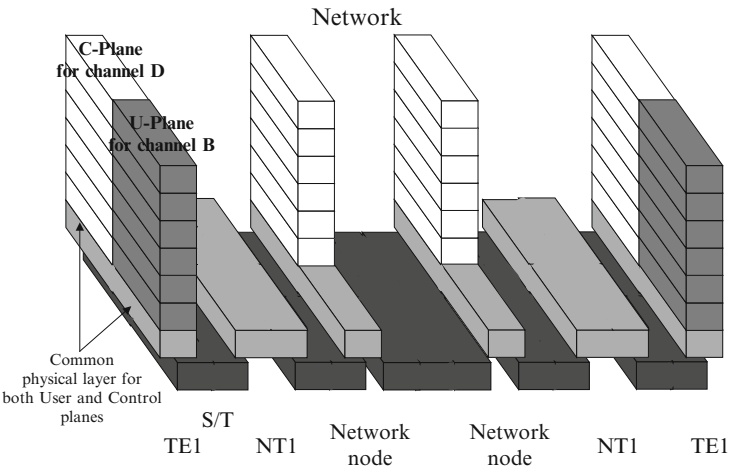
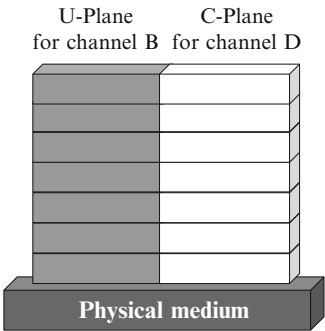
## Supplementary Services

Supplementary services are provided together with a bearer service or a teleservice in order to improve it. In particular, many supplementary services are defined to support bearer services of the circuit type (ITU-T Recommendations from I.251 to I.257), such as calling number notification, group calls, etc.

### 2.1.2.4 ISDN Protocol Stack

ITU-T I.320 Recommendation defines the protocol stack for reference points S and T [21]. The OSI reference model was mainly related to X.25, where signaling is managed by the same protocol stack of the information traffic (“in-band” signaling). Hence, the X.25 approach is incompatible with circuit-switching, where once a circuit is established, information is transparently conveyed by the network that, in this case, acts as a relay system at level 1. To overcome these limitations of the X.25 approach, the ISDN protocol stack has been conceived with two parallel stacks: one for information traffic (also called User Plane) and the other for

**Fig. 2.6** ISDN protocol stack architecture



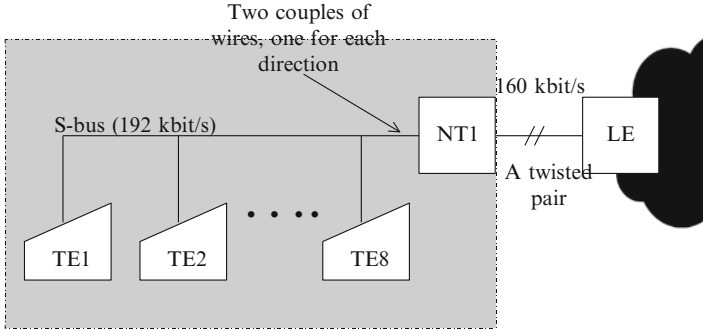
**Fig. 2.7** Example of protocol stacks at different interfaces for a circuit-switched ISDN connection

signaling traffic (also called Control Plane). At each layer, we have two protocols, one for the user plane and the other for the control plane. ISDN adopts an “out-of-band” signaling approach. See Fig. 2.6.

In a circuit-switched connection (ITU-T I.320 Recommendation), we have both user and control planes at each node. However, the user plane stack related to channel B is reduced to only the physical layer (physical relay), whereas the control plane of channel D has a complete stack, where, practically, only layers 1, 2, and 3 are used (for instance, Q.931 is a layer 3 protocol for channel D, also including higher layer functions). See Fig. 2.7.

**2.1.2.5 Layer 1 Protocol**

In the definition of the physical layer, there is no distinction between channels D and B.



**Fig. 2.8** BRI multi-point access architecture with a passive bus: up to 8 TEs can be connected

According to Recommendation I.431 [19], PRI and accesses of the H type use the same layer 1 of the 2 Mbit/s E1 numeric transmission {ITU-T G.703 and ITU-T G.704 Recommendations, respectively on electric interface and frame structure [22, 23]}. PRI is characterized by a point-to-point configuration (i.e., a single terminal directly connected to the network).

Instead, the physical layer of BRI has required an ad hoc solution, detailed in the ITU-T I.430 Recommendation [18]. The most general BRI access structure is based on a *passive bus* where many TEs can be connected; this is the so-called *multi-point* access architecture, as shown in Fig. 2.8.

In general, an NT1 can operate both in point-to-point configuration and in multi-point configuration. The point-to-point case can be considered as a special case of the multi-point one. In a multi-point configuration, the maximum distance is 200 m (short bus) or 500 m (extended bus); instead, in a point-to-point configuration the maximum distance is 1,000 m. In the multi-point configuration, TEs cannot communicate directly with each other; they can only communicate with the NT1. As many as eight distinct devices (telephones, computers, fax machines, etc.) can be connected to the bus, each of them, having as many separate telephone numbers as needed.

At the U point (between NT1 and the local exchange), there is a full-duplex transmission at 144 kbit/s (2B + D) with a gross bit-rate of 160 kbit/s. 2-Binary-1-Quaternary (2B1Q) line coding is adopted; the signal has a DC component with this coding. Two approaches are available for supporting bidirectional transmissions on a two-wire link: Echo Cancellation (ECM) and Time Compression (TCM), according to ITU-T G.961 Recommendation.

At the customer site, the 2-wire U interface is converted into a 4-wire S/T interface by the NT1 (from 160 to 192 kbit/s). A normal ISDN device plugs into the S/T interface an RJ 45 (8 pin) jack, carrying two pairs of wires. One pair carries the signal from TE to NT, the other pair carries the signal from NT to TE. The signals transmitted over the two pairs are at a gross rate of 192 kbit/s, using an

Alternate Mark Inversion (AMI) line coding to avoid the DC component in the signal.<sup>2</sup> A frame of 48 bits is transmitted every 250  $\mu$ s. A very similar (but not identical) frame format is used on the two pairs, with the TE to NT signal synchronized with the NT to TE signal, delayed of two bit times. The beginning of each frame is marked by an F (framing) bit, followed by an L (balancing) bit, both with reversed polarity. In both directions, each frame contains two 8-bit B1 channel slots and two 8-bit B2 channel slots ( $8 \text{ bits/slot} \times 2 \text{ slots/frame} \times 4,000 \text{ frames/s} = 64 \text{ kbit/s}$ , conveyed on each channel B). Each frame also contains 4 bits of the D-channel ( $4 \text{ bits} \times 4,000 \text{ frames/s} = 16 \text{ kbit/s}$ , shared among the TEs in a multi-point configuration). In the direction from NT to TE, four E (echo) bits copy back the D bits from the other direction and provide collision detection for multiple devices competing for channel D.

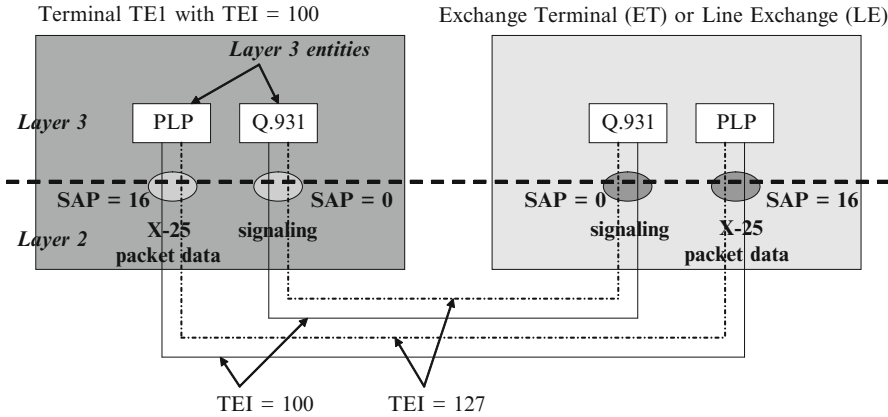
### 2.1.2.6 Layer 2 Protocol

The ISDN protocols specified by the recommendations for layers 2 and 3 are valid only for D-channels. As for layer 2, ITU-T Q.920 and Q.921 Recommendations are considered [24, 25].

The layer 2 protocol is based on HDLC and its frame structure. In particular, the protocol is named Link Access Procedure on the D-channel (LAPD) and has the specific task of allowing the communication between peer layer 3 entities. A layer 3 entity is identified by a Service Access Point (SAP). There are different types of SAPs, each denoted by a suitable SAP Identifier (SAPI): SAPI = 0 is related to signaling (e.g., Q.931 signaling); SAPI = 16 is used for X.25 packet data traffic; SAPIs from 32 to 62 denote frame relay data; SAPIs different from 16 to 32–62 are used for call control messages; finally, SAPI = 63 is adopted for management messages. In order to distinguish different TEs in a multi-point connection, a suitable Terminal Endpoint Identifier (TEI) is defined. Each layer 2 connection is therefore identified by SAPI + TEI, which together form the Data Link Connection Identifier (DLCI), the address field of a LAPD frame. In the LAPD header, the SAPI field has 6 bits (numbers from 0 to 63) and TEI has 7 bits (numbers from 0 to 127). TEI numbers can be preassigned (TEIs 0–63), or dynamically assigned (TEIs 64–126) for terminals supporting automatic TEI allocation. TEI 0 is commonly associated with ISDN PRI circuits. TEI values from 64 to 126 are used for dynamic TEI assignment for ISDN BRI circuits. TEI 127 is used for group broadcast: a frame transmitted by the network with TEI = 127 is received by all the terminals, which are connected to the related network termination. Most TEIs are dynamically assigned by means of the TEI management protocol. The user broadcasts an

---

<sup>2</sup> A DC component in the signal is problematic due to different aspects: (1) saturation or change in amplifiers operating point; (2) a DC bias does not pass through a transformer (AC coupling, *bandpass filtering*), but gives rise to the “DC-wander” phenomenon, which entails a significant distortion of the pulse. Some line codes remove the DC component and are identified as DC-balanced. The AMI code is DC-balanced; instead, 2B1Q is not DC-balanced.



**Fig. 2.9** Example of ISDN layer 2 LAPD addressing for sending data and signaling from a line exchange to a TE1

identity request and the network responds with an identity assigned, containing the TEI value. Functions are also provided to verify and release TEI assignments. A terminal can have assigned more TEIs; for instance TEI = 127 and one or more TEIs for data or signaling traffic. See the example in Fig. 2.9. Note that typically TEI = 0 in a PRI interface, because PRI does not support multi-point connections.

Layer 3 does not use the TEI value, but employs an association between the layer 2 TEI with the SAPI to univocally identify the connection.

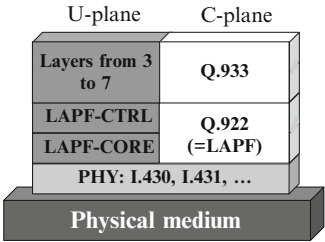
### 2.1.2.7 Layer 3 Protocol

Layer 3 is specified in ITU-T Q.930, Q.931, and Q.932 Recommendations for signaling traffic on channel D [26]. These protocols have to manage the exchange of end-to-end signaling for channel B. When a call arrives at user premises using multi-point connections, all the terminals (e.g., different ISDN phones) must be alerted. As soon as the first terminal is activated, the other terminals are released. In the case of data packet traffic on channel D, the X.25 layer 3 protocol (i.e., PLP) is used, as shown in Fig. 2.9.

## 2.1.3 Frame Relay-Based Networks

This is a new network technology for the transfer of data on geographical areas. It is based on a layer 2 protocol, named Frame Relay, which can be considered as a variant of the LAPD protocol used in ISDN. Frame relay was one of the “fast packet-switching” technologies introduced in the early Nineties. Frame relay became a new network type, independent of ISDN (it is not just a service provided by ISDN).

**Fig. 2.10** Frame relay protocol stack of an end system (both user and control planes)



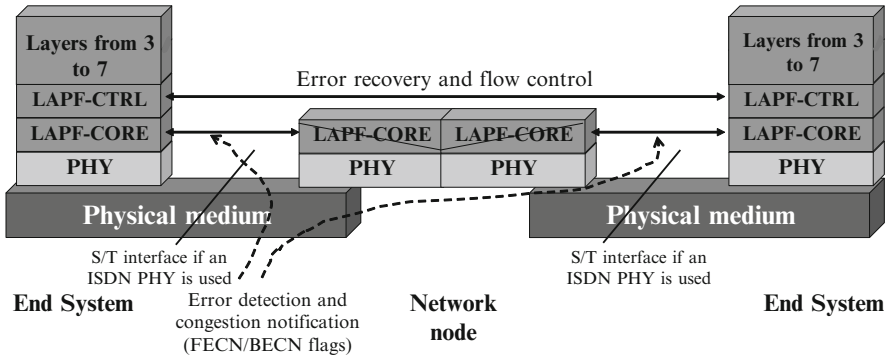
Frame relay entails lower overhead and achieves higher performance than previous protocols. Digital networks employing frame relay at layer 2 are called frame relay networks and this is the subject of this Section. Frame relay is used in both private and public networks.

Two standards organizations actively involved in the development of frame relay are ANSI and ITU-T. The initial frame relay standard was approved by ANSI in 1990 and included standards T1.606 [27], T1.617 [28], and T1.618 [29]. The ITU-T Recommendations are published as I.233 [30], Q.922 Annex A [31], and Q.933 [32]. Full interoperability between ANSI and ITU-T standards are obtained if the address is in the two-byte format in the frame header (see the description below). The Frame Relay Forum (FRF) is a nonprofit organization dedicated to promoting the acceptance and the implementation of frame relay, based on national and international standards [33, 34].

The fundamental characteristic of frame relay is to allow data to be transferred performing minimal control in the network: there is no error correction and no flow control in the network links; both tasks are end-to-end performed. This is a quite different approach with respect to X.25 networks, where error control was performed on each link. X.25 networks were based on unreliable physical medium (with considerable bit error rates from  $10^{-3}$  to  $10^{-5}$ ), transmission techniques were analog (i.e., use of modems), nodes had low processing and storage capabilities. With the adoption of optical fibers the error rates are drastically reduced (bit error rates from  $10^{-6}$  to  $10^{-9}$ ), thus making useless to perform error recovery on each link. This is the reason why frame relay performs end-to-end error control (no local error control). Such simplification allows improving the data throughput performance of the network.

Frame relay is a connection-oriented protocol with virtual circuits: an end-to-end connection must be established before data can be transferred. Switching is performed at layer 2, differently from X.25 networks, where switching is performed at layer 3. The protocol stack employs a user plane (data, information flow) and a control plane (signaling). Hence, signaling is out-of-band as in ISDN and differently from X.25. The frame relay protocol stack is shown in Fig. 2.10 and is described below:

- *Physical layer:* It is common for user and control planes. It is based on ISDN physical resources (one B-channel, one ISDN BRI access according to I.430 [18], one ISDN PRI according to I.431 [19], etc.).



**Fig. 2.11** Frame relay service: user plane protocols in internal network nodes and at end systems. Note that error recovery and flow control are performed end-to-end

- *Layer 2*: User and control planes typically adopt different protocols both related to ITU-T Q.922 Recommendation. In particular, the control plane employs the LAPF protocol defined in Q.922, whereas the user plane adopts LAPF at end nodes and a subset of LAPF, named LAPF-core {i.e., the lower part of the full LAPF protocol, which is defined in Annex A of Recommendation Q.922 [31]}, at intermediate nodes. The typical functions of LAPF-core are: framing, multiplexing/demultiplexing of virtual circuits, error detection, address, and management of congestion events. Note that the upper part of the LAPF protocol, named LAPF-control, is used to operate end-to-end error recovery (ARQ protocol) and flow control. At intermediate nodes in the network, the user plane only terminates the LAPF-core; this is the classical *frame relay service*, as shown in Fig. 2.11. However, it is also possible that the network adopts both LAPF-core and LAPF-control (i.e., a full LAPF protocol) in the user plane, as in the control plane; in this case, the network provides a *frame switching service*.
- *Layer 3*: On the control plane the Q.933 protocol [32] is adopted, derived from the Q.931 protocol of ISDN networks. This protocol is responsible for the management of virtual circuits. On the user plane, only end systems have a full layer 3 protocol.

User and control planes convey data organized in layer 2 messages called *frames*. They are “routed” through virtual circuits by means of the address field, named Data Link Connection Identifier (DLCI). The DLCI field has only a local meaning; it can be changed at each node according to the path defined during the setup phase. The frames on the control plane have the same format of the LAP-F frames on the user plane. The different fields of the frame header are described below, referring to Fig. 2.12. The frame header can have different formats with 2, 3, and 4 bytes. It includes the following subfields:

- DLCI of different length, depending on three different formats (10, 16, and 23 bits, respectively). DLCI has a different definition with respect to ISDN. There are two extreme cases: (1) the DLCI field with all bits equal to 0 (i.e.,  $\text{DLCI} = 0$ ) is reserved





**Fig. 2.12** Default LAPF frame header (2-byte long). The Upper DLCI field contains 6 bits; the Lower DLCI field contains 4 bits

- for a channel conveying signaling for all the virtual connections on the same link;
- (2) the DLCI field with all bits equal to 1 (e.g., DLCI = 1,023 in the 10 bit DLCI case) is used for a channel transporting management information for the link.
- Command/Response (C/R), not used by the standard frame relay protocol (it is used by higher layer protocols).
  - Address Extension (EA): There is one EA bit at the end of each byte in the address field. EA = 0 except for the last byte of the address field where EA = 1.
  - Forward Explicit Congestion Notification (FECN) bit: If it is set to 1 by an internal node of the frame relay network, it denotes a congestion situation on the related link on the path towards the destination of the frame.
  - Backward Explicit Congestion Notification (BECN) bit: If it is set to 1 by an internal node of the frame relay network, it denotes a congestion situation on the link where the frame is sent, but in the opposite direction.
  - Discard Eligibility (DE) bit: If it is set to 1 by an access node of the frame relay network, it authorizes to discard the related frame with priority (with respect to those with DE = 0) in internal nodes when they are congested. The setting of the DE bit requires a traffic policing function implemented at the entrance nodes of the frame relay network. The discard of packets marked with DE = 1 requires a buffer management function at intermediate nodes.
  - DLCI/DL-core indication (D/C) bit: It is used in the address field format of 3 or 4 bytes; if set to 1, a field destined to DLCI is used for control information of the LAPF-core protocol.

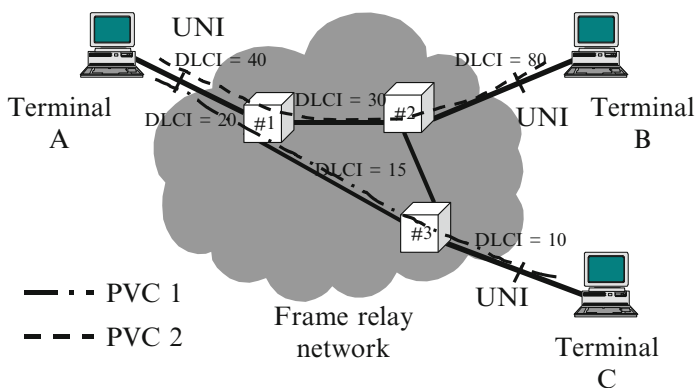
Frames are produced by a source with FECN = 0, BECN = 0, DE = 0. The DE bit can be modified at the first (access) node of the frame relay network. FECN and BECN bits can be modified at any internal node of the frame relay network.

At the LAPF-control level, the frame header also includes a control field of 1–2 bytes (at the LAPF-core level, the header does not contain such control field).

The packet payload has a variable length with a maximum value of 4,096 bytes. However, the frame relay forum developed an implementation agreement setting the maximum payload size at 1,600 bytes for interoperability reasons (this frame size can easily support the largest Ethernet frame for LANs). Packet sizes have to be reduced for voice real-time services.

Finally, there is a 2-byte Frame Check Sequence (FCS) trailer field, which is used to detect errors in the transmitted frame (cyclic redundancy check).

Referring to Fig. 2.13, the interface between an end-user and the network is named User to Network Interface (UNI). End-users are interconnected using Virtual Circuits, which can be either PVC or SVC. A PVC is a permanent connection between two end-points that is set up by the operator. This connection always



**Fig. 2.13** Characterization of virtual channels and use of DLCI in frame relay networks

exists, meaning that there is a circuit used for this PVC at each node along the path in the network, whereas an SVC is a temporary connection between two end-points, which is set up upon request of one of the parties. This connection can be released when it is not needed, similarly to a phone call.

Frame relay supports the statistical multiplexing of the traffic flows of the different virtual paths sharing the same link.

Still referring to the frame relay network example in Fig. 2.13, we can note that one path (i.e., one end-to-end virtual channel) is characterized by the DLCI values of the links crossed at the different nodes. For instance, PVC 2 connecting Terminal A to Terminal B is characterized by the following associations at each node along the path:

$$(\text{Terminal A, DLCI} = 40) \cup (\text{Node\#1, DLCI} = 30) \cup (\text{Node\#2, DLCI} = 80).$$

PCVs can be used when there is a stable traffic between end points (e.g., interconnections of different locations belonging to the same organization); otherwise, SVC connections are more efficient since they are set up on demand, thus allowing a better multiplexing of resources among competing traffic flows. SVCs are typically used for public access. The Q.933 layer 3 protocol of the control plane is in charge of supporting the setup of a virtual path, its maintenance/control, and its release when the call ends. Q.933 messages are a subset of those defined for the corresponding Q.931 protocol of the ISDN control plane. Differently from the user plane, all the intermediate nodes of the frame relay network use the layer 3 Q.933 protocol on top of a complete LAPF protocol on the control plane.

The Q.933 protocol defines the characteristics of the access to a frame relay network by means of an ISDN interface. In particular, there are two different cases depending on the location of the first node of the frame relay network.

- *Circuit-switched access:* There is an ISDN circuit towards a remote access node of the frame relay network, named Remote Frame Handler (RFH); hence, RFH and the Local Exchange (LE) of the ISDN network where the user line arrives are not co-located. The ISDN circuit between the user terminal and RFH can be

semipermanent or set up on demand on B or H channels. In case of access path established on demand, the setup procedure is carried out on a D-channel via the Q.931 protocol (LAPD). When the B (or H) channel is activated, it supports the Q.922 (LAPF) protocol between the terminal and the RFH. Then, the Q.933 protocol messages are used to establish the connection between the terminal and a remote host through the frame relay network. Such procedure employs DLCI = 0 for all the messages exchanged in the network. Once such procedure is completed, the exchange of end-to-end data can start by means of the LAPF-core protocol.

- *Packet-switched access*: The LE of the ISDN network and the access node of the frame relay network (Frame Handler, FH) are co-located. The setup of a path is according to the following procedure. Q.933 control messages are exchanged on channel D by means of LAPD between the user terminal and the LE + FH in order to establish a logic connection on either a B- (H-) channel or a D-channel. When this connection is set up, LAPF core is used to exchange data.

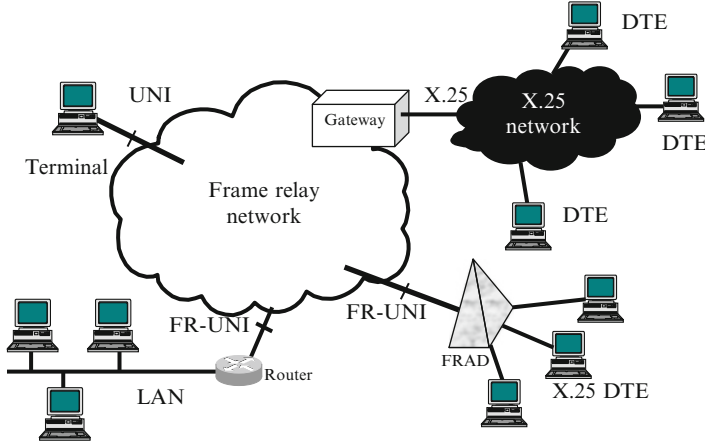
### 2.1.3.1 Network Infrastructure

Frame relay is used in different topologies in both public and private data networks. The five most common topologies are point-to-network, point-to-point, star, full-mesh, and partial mesh. The point-to-network topology is a single link to the network. The point-to-point configuration consists of two UNIs connected together. The star or hub topology consists of distributed sites communicating with each other through a central location. In the full-mesh topology, each node is connected to all other nodes. The mesh topology has the advantage that if there is a failure at a node or on a link it is very easy to find alternative paths. The disadvantage of this topology is that it is very expensive:  $N(N-1)/2$  bidirectional links are needed for an  $N$ -node full-mesh network. Finally, in the partial mesh topology, only the core of the network is interconnected according to a full-mesh topology.

The access to a frame relay network is allowed both to terminals (hosts) and to network equipment (e.g., routers), provided that they support the frame relay protocol stack described in Figs. 2.10 and 2.11. In this case, a Frame Relay Access Device (FRAD) is interposed between the host and the network, thus having the new interface named FR-UNI. It is also possible that X.25 terminals and networks be interconnected to a frame relay network. In this case, a gateway is interposed: it receives X.25 frames according to the LAPB protocol, obtains the PLP packets, which are then managed by the LAPF-core protocol in the frame relay network (Fig. 2.14).

### 2.1.3.2 Traffic Regulation (Policing)

We are considering here the case where a variable bit-rate traffic source has an access line to the frame relay network with a capacity denoted by Access bit-Rate (AR), which is typically much higher than the maximum traffic load generated by



**Fig. 2.14** Interworking with frame relay

the source. During the connection establishment phase, the following flow control parameters are defined to monitor and regulate the input traffic flow:

- *Measurement interval*,  $T_c$ , i.e., the time interval on which we measure the source traffic to determine whether it is conformant to specifications.  $T_c$  is the time periodicity according to which the input traffic is controlled.
- *Committed burst size*,  $B_c$ , denoting the maximum number of bits that the network is able to accept and convey in a time  $T_c$  from a given source.
- *Excess burst size*,  $B_e$ , representing the maximum number of excess bits in  $T_c$  (with respect to the  $B_c$  value) that the network will try to convey to destination without any special guarantee.

On the basis of the above parameters, the capacity that the frame relay network assures to a terminal traffic flow is denoted as Committed Information Rate (CIR) and can be expressed as:

$$\text{CIR} = \frac{B_c}{T_c} \quad \left[ \frac{\text{bit}}{s} \right] \quad (2.1)$$

The extra capacity that the network can provide, denoted as Excess Information Rate (EIR), is expressed as:

$$\text{EIR} = \frac{B_e}{T_c} \quad \left[ \frac{\text{bit}}{s} \right] \quad (2.2)$$

The frames sent in a  $T_c$  interval and requiring the extra capacity (of the  $B_e$  bits in  $T_c$ ) are *marked* with  $\text{DE} = 1$ , so that they can be discarded at an intermediate node if it experiences buffer congestion.

Of course the access capacity AR must fulfill the condition below:

$$\text{CIR} + \text{EIR} \leq \text{AR} \left\lceil \frac{\text{bit}}{s} \right\rceil \quad (2.3)$$

Higher values of  $T_c$  are preferable for users since they allow sending bursts of data. From the network standpoint, lower  $T_c$  values are preferable since they permit both a better control on the traffic injected into the network and a better statistical multiplexing of traffic flows.

To summarize, the frames generated by a source are monitored on a  $T_c$  time interval basis. As long as the number of bits generated in  $T_c$  is lower than or equal to  $B_c$ , frames are accepted in the network with  $\text{DE} = 0$ ; if the bits generated in  $T_c$  exceeds  $B_c$ , but are lower than or equal to  $B_c + B_e$ , frames are accepted in the network with  $\text{DE} = 1$ ; if the bits generated in  $T_c$  exceeds  $B_c + B_e$ , frames are *discarded*. Then, the measurement process of the bits generated by the source restarts in the next  $T_c$  interval and so on. This situation is depicted in Fig. 2.15, where  $B_t$  denotes the maximum number of bits that the access line can convey in  $T_c$  (i.e.,  $B_t = \text{AR} \times T_c$ ).

### 2.1.3.3 Congestion and Flow Control

In the frame relay network, flow control is end-to-end operated in order to limit the traffic load injected into the network. The traffic generated by a source is controlled at the entrance of the network according to the previously described traffic regulator.

Congestion control is a crucial part in telecommunication networks, since the occurrence of congestion leads to buffer overflows and the consequent loss of frames (an end-to-end ARQ scheme is needed), unpredictable delays, and the reduction of network throughput. Congestion control is end-to-end operated. In fact, the network is in charge of monitoring congestion at transit nodes and reporting it to the end-terminals, which have the responsibility to react accordingly. Mainly, two techniques are available to manage buffer congestion [35]:

- Each node controls the occupancy of its buffers; when a threshold value is exceeded for the buffer of a given link, a procedure is started to notify congestion to all virtual channels using this link. Hence, FECN is set to 1 for all the frames sent by this node through the bottleneck link; moreover, BECN is set to 1 for all the frames received by this node through the bottleneck link. Let us refer to Fig. 2.16, referring to the virtual circuit from terminal A to terminal B. Let us assume that node #4 reveals congestion on the link towards node #2. Hence, FECN is set to 1 at node #4 for all the frames that from node A are sent to node B; moreover, BECN is set to 1 at node #4 for all the frames that from node B are sent back to node A. BECN notifies the sender that there is congestion in the network and that a bit-rate reduction is needed. FECN can be used by the

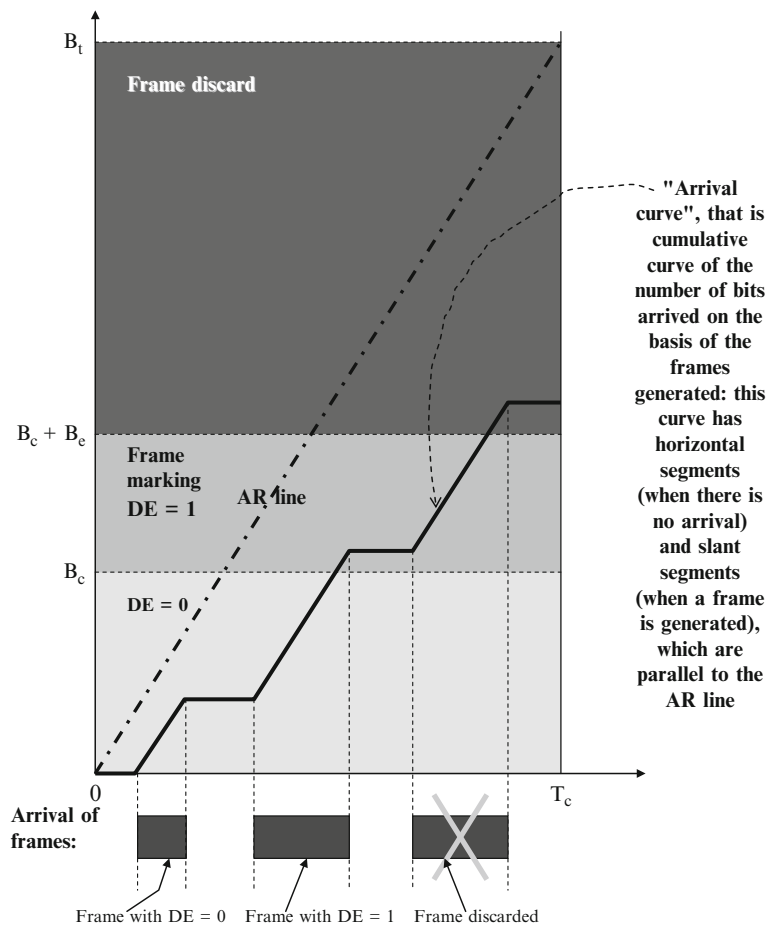


Fig. 2.15 Management of source traffic entering a frame relay network

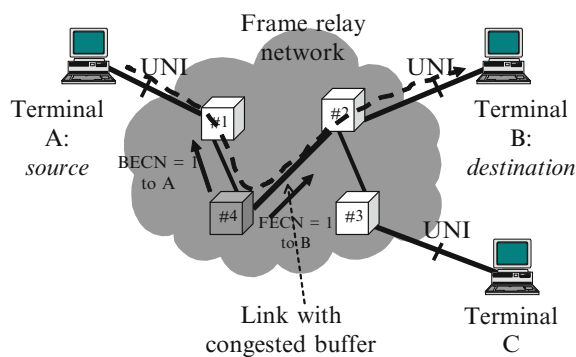


Fig. 2.16 Use of BECN and FECN in the presence of congestion on a bottleneck link

destination device in the case that its upper layer protocols can control the traffic injected by the source through an end-to-end procedure. This is the typical case of the TCP protocol, as described in Sect. 3.8.1.

- If a link is congested (i.e., the related transmission buffer is full) the related node can discard frames starting from those having  $DE = 1$  for which the network does not guarantee correct delivery.

## 2.2 B-ISDN and ATM Technology

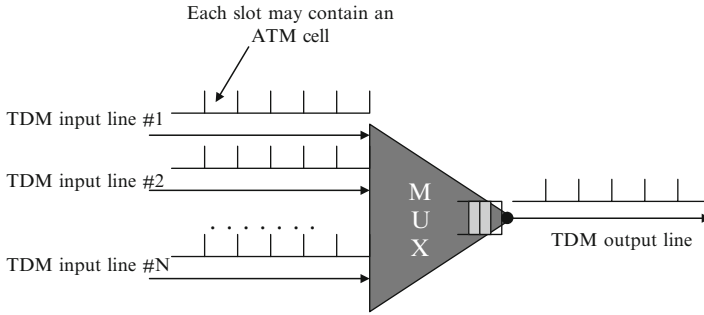
The broadband evolution of ISDN (i.e., Broadband ISDN, B-ISDN) was defined in 1990 in a draft ITU-T document, subsequently consolidated in the ITU-T I.150 Recommendation [36]. Asynchronous Transfer Mode (ATM) denotes a technology for the transmission of multimedia traffic on B-ISDN [6–8]. ATM specifications are the result of a very long standardization process. In practice, ATM denotes the name of a layer 2 protocol, but it provides such a strong characterization of the network that we can also use the term “ATM network”. The following list summarizes the main characteristics of an ATM network:

- The basic transmission unit is a packet of fixed length, called *cell*. It is formed of a payload of 48 bytes and a header of 5 bytes, which contains all the information to support the ATM protocol.
- The transmission on the links is based on asynchronous time division multiplexing, an innovative solution with respect to previous network technologies.<sup>3</sup>
- An ATM network is connection-oriented, where switching is performed at layer 2.
- The payload of an ATM packet (cell) is transparently managed by the network: there is no error control<sup>4</sup> and no flow control at intermediate nodes, but only end-to-end.
- Multimedia traffic classes can be managed by the ATM network. They correspond to different applications (i.e., services). Each traffic class is described in terms of the bit-rate behavior and has guaranteed some Quality of Service (QoS) requirements (maximum delay, delay jitter, etc.). Even connectionless traffic can be supported.

---

<sup>3</sup>In Asynchronous Time Division Multiple Access (A-TDMA), we have different packet data traffic sources sharing the slots of the TDMA frame without a fixed, predetermined allocation (this would be the case of Synchronous-TDMA, S-TDMA). A traffic source can have assigned different slots and a different number of slots from frame to frame to adapt to varying traffic load conditions. A-TDMA improves the utilization of the transmission line resources and entails lower delays than S-TDMA by exploiting the multiplexing effect.

<sup>4</sup>Typically a quite reliable transmission medium is used (i.e., optical fiber). Hence, bit-error rates are on the order of  $10^{-10}$  (and lower). In such circumstances, it is not efficient to check the correctness of the cell payload at each hop, but only end-to-end.



**Fig. 2.17** ATM network element: multiplexer. The different input lines send packets to one common output buffer. The A-TDMA principle is implemented

Due to the connection-oriented nature of an ATM network, before a sender and a receiver can exchange data, an end-to-end path must be established by means of a setup procedure. During this setup phase, not only a path is established, but it is also verified that resources on the involved links are enough to support the new traffic, guaranteeing for it (and for the already-active connections) the contractual QoS levels. If that verification is successful, the new connection is activated, otherwise it is refused. Such procedure is called Connection Admission Control (CAC), a crucial part of ATM networks that, differently from previous network technologies, can support QoS requirements for different traffic classes.

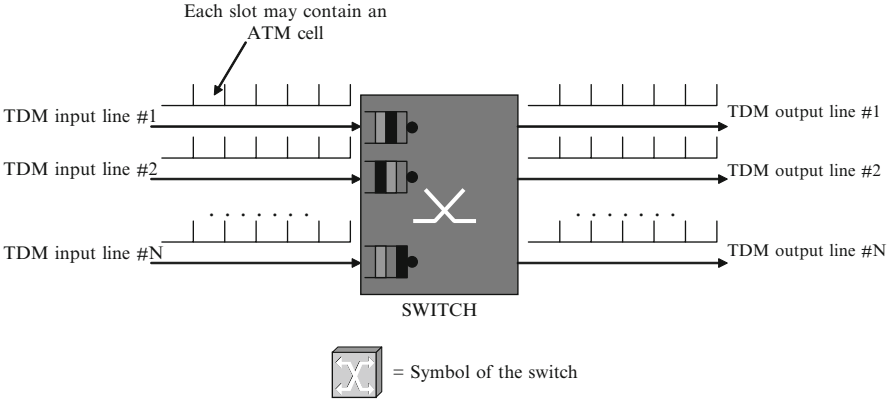
ATM networks manage both switched virtual paths (formed upon request) and semipermanent virtual paths (i.e., paths configured by the operator and that are active for a long time in order to provide a fixed end-to-end connectivity). The end-to-end established path is not physically switched, but is logically formed and identified by some form of “labels”, denoting the links between the different network elements. This is the reason why paths are “virtual” in ATM networks.

An ATM network is typically composed of two different network elements:

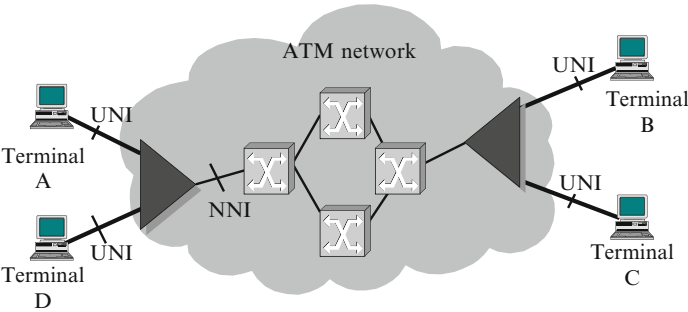
- Multiplexers/demultiplexers (see Fig. 2.17)
- Switches (see Fig. 2.18)

Let us refer to the typical ATM network architecture shown in Fig. 2.19. A multiplexer receives the packet data traffic from different input TDM lines and queues data to be sent on a single TDM output link according to the asynchronous-TDMA scheme (i.e., no rigid slot assignment to input lines in the TDM frame). A multiplexer typically allows passing from low utilization input lines to high utilization output lines, i.e., a traffic concentrator, exploiting the statistical multiplexing of (bursty) traffic sources. A de-multiplexer performs the opposite operation. We may expect that multiplexers and demultiplexers are close to the end systems just to concentrate or to split the traffic. A switch connects TDM input lines to TDM output lines. Each packet of each input line must be analyzed by the switch processor. The virtual path descriptor in the cell header permits to forward the packet on the appropriate output link of the switch. Different switch technologies





**Fig. 2.18** ATM network element: switch. Each input line has a buffer (otherwise we could have that each output line has a buffer). A switching technology is used to interconnect input and output lines

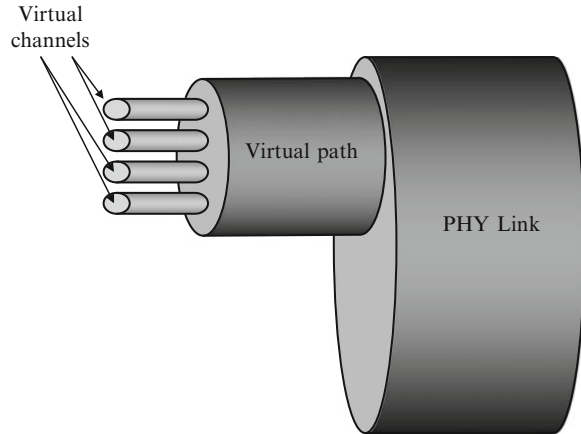


**Fig. 2.19** Example of ATM network architecture

are available. In general, internally to the switch, there are buffers at input lines or at output lines. In the first case, buffers are used to store cells waiting to be switched; in the second case, buffers are needed to store cells waiting to be transmitted on the selected output link. A more detailed description of the switches and their internal architectures is provided in the following Sects. 2.2.5 and 2.2.6.

The cell header contains the description of the virtual circuit, characterized by two fields: Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). During the virtual path setup phase (or during the circuit configuration process in the case of permanent paths) each switch is suitably instructed so that it can forward an incoming cell having a certain VPI + VCI to an output link corresponding to a new VPI + VCI couple, which is updated in the cell header. A virtual circuit is formed of a VPI and a VCI on each link: the virtual circuit in the cell header is updated at each switch. The resources of a link are shared among some virtual paths (VPIs); moreover, a path “multiplexes” several virtual channels (VCIs), as shown in Fig. 2.20.

**Fig. 2.20** Graphical representation of virtual paths and virtual channels for a given link. Each couple (virtual path, virtual channel) is mapped to a physical resource



The physical links used by ATM are typically based on optical fibers. More details on the ATM physical layer and physical medium are provided in the following Sect. 2.2.8.

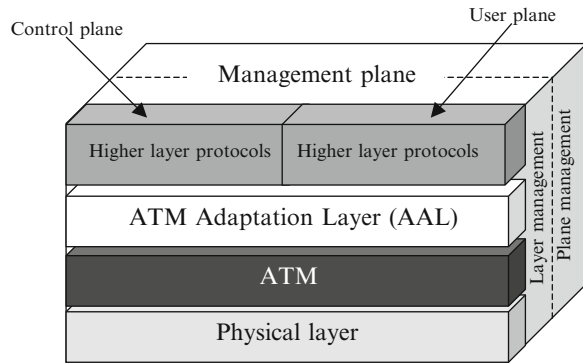
The ATM technology is quite expensive and is not widely adopted. However, ATM can still be a viable option for the access part of the network, but not for the backbone. For instance, in the high bit-rate Internet access with the twisted-pair medium of the telephone network, Asynchronous Digital Subscriber Line (ADSL) is used at the physical layer and the ATM protocol is adopted at layer 2.

### 2.2.1 ATM Protocol Stack

ITU-T I.321 Recommendation characterizes the ATM protocol stack (for B-ISDN networks) as a significant evolution of the ISO/OSI reference model. As shown in Fig. 2.21, the ATM protocol stack is three-dimensional, with three planes:

- *User plane*, for the end-to-end transfer of information traffic.
- *Control plane*, supporting signaling traffic for virtual path setup, for CAC of a new connection, for the maintenance of a connection, and, finally, for the release of a connection.
- *Management plane*, for operation and maintenance functions and for the coordination of the different planes.

Both user and control planes are characterized by two (stacked) layer 2 protocols (i.e., ATM Adaptation Layer, AAL, and ATM layer) and the physical layer. End systems have a complete protocol stack from physical layer to layer 7. Instead, intermediate nodes (i.e., multiplexers and switches) have only the lower layers (i.e., ATM and PHY).

**Fig. 2.21** ATM protocol stack

### 2.2.2 Cell Format

In previous data networks (i.e., X.25 and frame relay), the switched unit was a packet (or frame) of a variable length, whereas in the ATM case a fixed-length packet, called “cell”, has been defined as a result of a complex standardization process that took different aspects into account, such as the following ones:

- Efficient utilization of transmission resources
- Delay to cross a node
- End-to-end delay to transfer a cell
- Routing/switching complexity

The ATM cell is formed of a 5-byte header and a 48-byte payload. The header reduces the transmission efficiency, since header bits do not carry information, but are necessary for the management of the information. In general, let us denote with  $H$  the number of bytes of the packet header; let us denote with  $P$  the number of bytes of the packet payload. The efficiency of the protocol,  $\eta$ , can be expressed as:

$$\eta = \frac{P}{P + H} \quad (2.4)$$

Conversely, the percentage of wasted resources due to the header is  $100 \times H/(P + H)$ . In the ATM case, such percentage is about equal to 9.43 %. Hence, on an ATM link having (for instance) a physical layer capacity of 155 Mbit/s, about 14.6 Mbit/s are lost due to cell header transmissions; this is a considerable capacity that is needed to support the ATM protocol.

Let us make some considerations for the comparison between fixed-length packets and variable-length ones. Typically, a PDU received from higher layer protocols is fragmented into many ATM cells; it may happen that the last cell is only partly utilized and this is another cause of inefficiency. The use of a variable-length packet would avoid this problem even if some bits in the header would be needed to determine the packet length. However, the adoption of a fixed-length packet allows an easier management of buffers whose capacity is designed

according to multiples of the packet length. Finally and most importantly, the use of a fixed-length packet allows us to reduce the delays encountered at the transmission queue of a link. Let us provide a formal proof of this property on the basis of the results shown in Chap. 6. In particular, we compare two queue cases with the same mean packet transmission time,  $E[X]$ :

1. *Case #1*: Deterministic packet transmission time (i.e.,  $X = \text{const.}$ ), as for fixed-length packets. In this case,  $E[X^2] = \{E[X]\}^2$ .
2. *Case #2*: Exponentially distributed packet transmission time. In this case,  $E[X^2] = 2 \times \{E[X]\}^2$ . For the characterization of the exponential distribution, please refer to Chap. 4 (Sect. 4.2.5.4).

In both cases, we consider packets arriving at the transmission buffer (i.e., queue) according to a Poisson process. The mean packet delay  $T$  is determined by the Pollaczek-Khinchin formula (6.18) in Chap. 6, as follows:

$$T = E[X] + \frac{\lambda E[X^2]}{2[1 - \lambda E[X]]} = \begin{cases} E[X] + \frac{\lambda \{E[X]\}^2}{2[1 - \lambda E[X]]}, & \text{for case \#1} \\ E[X] + \frac{2\lambda \{E[X]\}^2}{2[1 - \lambda E[X]]}, & \text{for case \#2} \end{cases} \quad (2.5)$$

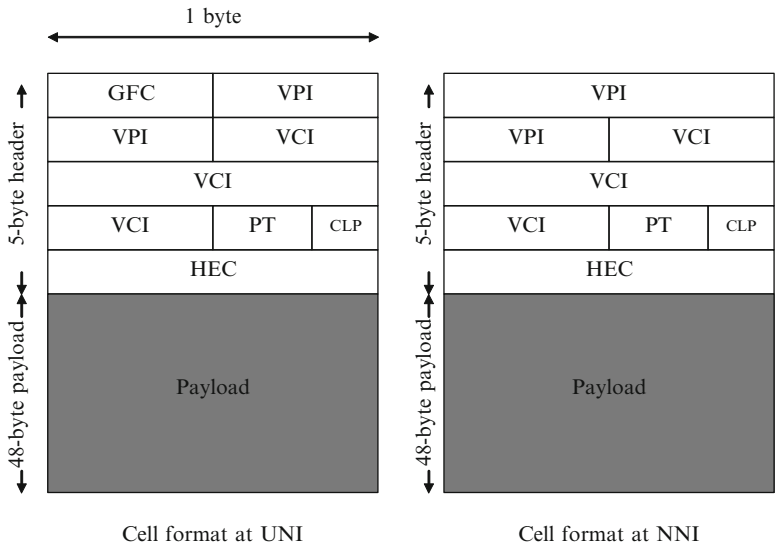
Analyzing the  $T$  expressions in (2.5), we notice that in both cases they are the sum of the mean packet transmission time  $E[X]$  and a second term; this queuing term is double in case #2 with respect to case #1. Hence, the use of fixed-length packets allows us to reduce queuing delays.

The final decision for the ATM cell length of 53 bytes with a payload of 48 bytes was the result of a compromise between telecommunication and information technology groups (more or less corresponding to European and American groups, respectively): the first liked small cells (32-byte payload) for small delays; the second preferred larger cells (64-byte payload) for high throughput. The final decision was exactly to take the mean value for the payload length, that is 48 bytes.

The structure of an ATM cell is represented in Fig. 2.22 by distinguishing the format at the User-to-Network Interface (UNI) and that at the Network-to-Network Interface (NNI). In the first case, we have the interface for the user access to the network; in the second case, we refer to the interface between two internal network elements. The cell structure definition is contained in ITU-T I.361 Recommendation.

Let us describe the different fields of an ATM cell referring to Fig. 2.22 (starting from the top):

- GFC (Generic Flow Control) is present in the UNI case, but not present in the NNI one. GFC is used to support a flow control scheme for the input traffic of the user towards the network (not in the opposite direction).
- VPI is a field of 8 bits for the UNI cell or of 12 bits for the NNI cell. It identifies a virtual path between two nodes.



**Fig. 2.22** Cell format (each row corresponds to one byte) for both UNI and NNI interfaces

**Table 2.1** Description of the PTI field of the ATM cell header

PTI value	Cell type	Congestion notification	AUU
000	Information data without congestion	No	0
001	Information data without congestion (last cell of a train)	No	1
010	Information data with congestion	Yes	0
011	Information data with congestion (last cell of a train)	Yes	1
100	OAM cell	–	–
101	OAM cell	–	–
110	RM cell	–	–
111	Reserved	–	–

- VCI is a field of 16 bits (both UNI and NNI cell format), which is used to identify the virtual channels of a given virtual path.
- Payload Type Identifier (PTI) is field of 3 bits used to describe the cell type and to transport some control information. PTI permits to describe the content of the cell payload, among the following three cases: information data, Operation, Administration, and Maintenance (OAM), Resource Management (RM) signaling. All the details about the PTI filed are given in Table 2.1. The most significant bit discriminates between information data (bit equal to 0) and all the other cases (bit equal to 1). Moreover, in case of a data cell, the second bit set to 1 in the PTI field is used to notify that the cell crossed a node with congestion along the path towards destination. This is the Explicit Forward Congestion Indication (EFCI). Finally, the last bit of the PTI field in the case

of information data is the AUU bit (ATM-User-to-ATM-user), which is used by the AAL5 protocol to denote the last cell ( $AUU = 1$ ) of a cell train deriving from the segmentation of the same higher layer packet. ATM switches set the EFCI bit in the headers of forwarded data cells to denote the occurrence of congestion (see also the next Sect. 2.2.7). When the destination receives an ATM cell with the EFCI bit set, it marks the congestion indication in RM cells (having  $PTI = 110$ ) sent in the opposite direction to notify the source. This mechanism is exploited only by the ABR traffic class to inform the source to reduce the traffic injection according to a reactive control scheme.

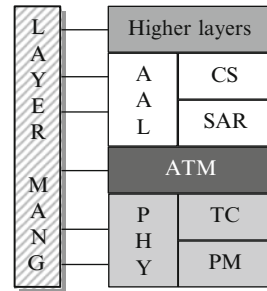
- Cell Loss Priority (CLP) bit to denote whether the cell has low ( $CLP = 1$ ) or high ( $CLP = 0$ ) priority. Different priority levels can be assigned to cells, so that only low priority cells can be dropped in case of congestion in the queues of ATM nodes. Hence, even in the presence of congestion, high priority cells are delivered to destination with high probability. The CLP bit can be set either by the sender to differentiate the priority among cells or by the access node if the connection violates its traffic contract with the network.
- Header Error Control (HEC) is a field of one byte for the parity check of the cell header at each hop. This code allows revealing errors and correcting single errors in the header. Due to the high reliability of the transmission medium (typically, optical fiber), it is not convenient to check the integrity of the entire cell (this task will be performed only end-to-end). Instead, only the header is verified: if the cell header is correct (or with a single error that is corrected) the cell is further forwarded (the network is sure to forward the cell on the intended path), otherwise the cell is discarded (higher layer protocols at end systems will be in charge of recovering this loss). The HEC code is also used to find the appropriate cell synchronism in a received ATM stream of cells. In fact, the ATM physical layer generates the last 8 parity bits of the cell header on the basis of the initial part (32 bits) of the header. This correlation due to the parity check bits is almost unique in the cell; it is unlikely that the same correlation on 40 bits is verified in another position of the cell. Such characteristic is important when the ATM traffic stream has to be extracted from complex physical layer multiplexed streams as in SDH (see the following Sect. 2.2.8). VPI and VCI are updated at each node according to the virtual circuit-switching approach. Hence, even the parity check (HEC) field has to be recomputed at each hop.

As for the payload, different formats are possible depending on the AAL protocol (see Sect. 2.2.4 of this Chapter).

### 2.2.3 *ATM Protocol Stack*

The ATM protocol stack (lower layers) is detailed in Fig. 2.23. In particular, we have:

**Fig. 2.23** ATM protocol stack



- The physical layer divided into two sublayers: Physical Medium (PM) and Transmission Convergence (TC). PM is in charge of physical layer-related functions such as the electro-optic conversion of bits and bit timing. TC, among other tasks, generates the HEC field of the cell.
- The ATM layer performs the following tasks:
  - It operates flow control at UNI by means of GFC.
  - It generates the first 4 bytes of the ATM cell header and adds them to the payload (transmission phase at the traffic source) or removes them from the cell (reception phase at the traffic destination).
  - It translates the VPI & VCI fields from input to output of a switch.
  - It performs the multiplexing (and demultiplexing) of the cells of different VPIs and VCIs on the same shared physical resources.
- The AAL layer has the following tasks: end-to-end transfer of messages of various lengths with cells of fixed length; management of erroneous cells and lost cells; flow control and congestion control; timing of the transported flow; multiplexing of different traffic flows on the same ATM connection. AAL is only end-to-end operated, that is by the end-nodes and not at the intermediate ones. The AAL layer is subdivided into two different sublayers: Segmentation And Reassembly (SAR) and Convergence Sublayer (CS).

SAR functions are as follows:

- In transmission, SAR divides the PDUs received from the CS sublayer into smaller units (SAR-SDUs) that, with some added control, form the SAR-PDUs fitting with the cell payload length (segmentation); in reception, SAR re-obtains the PDU for the CS sublayer.
- SAR performs a Cyclic Redundancy Check (CRC) on information bits.
- SAR introduces bits in the payload of each cell, which, depending on the AAL type, have a different function. For instance, cell numbering, PDU length in cells, Begin Of Message (BOM), Continuation Of the Message (COM), End Of Message (EOM) or message consisting of a single segment (Single Segment Message, SSM).

The CS function is to manage the higher layer PDUs for the different supported services, thus providing to SAR a CS PDU, including header and trailer control bits.

ITU-T I.363 Classes			
Class A	Class B	Class C	Class D
Real-time traffic		Non-real-time traffic	
Constant bit-rate traffic	Variable bit-rate traffic		
Connection-oriented services			Connectionless services
Mapping to ATM service categories and ALLs			
CBR	rt-VBR	nrt-VBR, ABR, UBR	
AAL1	AAL2	AAL3, 4, and 5	

**Fig. 2.24** Mapping between ITU-T traffic classes, ATM service classes, and ALLs (see Sect. 2.2.7)

**2.2.4 Traffic Classes and ALL Layer Protocols**

The different traffic classes are differentiated on the basis of time-criticality, bit-rate behavior, and type of connection. The ITU-T Recommendations of the I.363.x series describe AALs (i.e., CS and SAR sublayers) in relation to for the ITU-T traffic classes A, B, C, and D, as shown in Fig. 2.24.

AAL1 is used for Class A; its typical application is the support of services with circuit emulation (the network provides a dedicated end-to-end circuit). AAL1 is used for Constant Bit-Rate (CBR) real-time traffic for audio, video and, in general, isochronous applications. AAL1 does not allow the multiplexing of different ATM connections.

The AAL2 protocol is adopted for class B, referring to real-time Variable Bit-Rate (rt-VBR) connection-oriented traffic. AAL2 can be used for voice and video packet services. AAL2 allows the multiplexing of different AAL2 flows on the same ATM connection with given VPI and VCI fields by means of suitable flow identifiers. In the AAL2 case, there is not the SAR sublayer, but the CS one is more complex.

AAL3 and AAL4 have practically the same characteristics. They can be used for both Class C and Class D, that is non-real-time Variable Bit-Rate (nrt-VBR) traffic for connection-oriented (e.g., frame relay) or connectionless services. The AAL3/AAL4 protocol allows the multiplexing of different flows on the same connection by means of suitable flow identifiers.

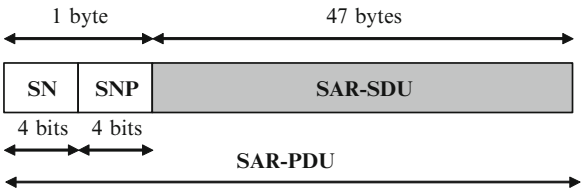
Finally, AAL5 is the simplest and most efficient adaptation protocol, able to support services of different classes (B, C, and D). It is either connectionless or connection-oriented. It is well suited to local area network emulation (Available Bit-Rate, ABR, class), nrt-VBR, and IP-ATM interworking (ABR and Unspecified Bit-Rate, UBR, classes). AAL5 does not support the multiplexing of different AAL flows on the same ATM connection.

More details on CBR, rt-VBR, nrt-VBR, ABR, and UBR services are provided in the following Sect. 2.2.7.

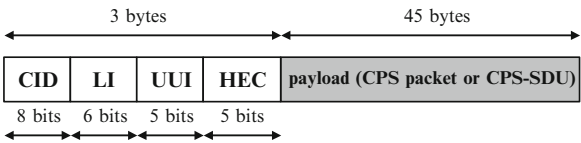
The different ALL types correspond to distinct cell payload formats, as described below.



**Fig. 2.25** AAL1 cell payload format (SAR-PDU)



**Fig. 2.26** AAL2 cell payload format (CPS PDU)



2.2.4.1 AAL Layer Protocols

The 48-byte cell payload format is described in Fig. 2.25 for AAL1. The overhead is of 1 byte, comprising the Sequence Number (SN) and the Sequence Number Protection (SNP), a code to protect the SN field. The SN permits to identify lost cells. The remaining 47 bytes of the cell payload represent the effective capacity of the AAL1 payload; this is the fragmentation unit operated by the SAR sublayer.

The AAL2 internal protocol architecture is slightly different with respect to the generic description given in Fig. 2.23. In particular, we have:

- Service Specific Conversion Sublayer (SSCS)
- Common Part Sublayer (CPS)

SSCS receives the higher layer PDU and formats a CPS packet to be included in the CPS PDU. Such PDU becomes the payload of the underlying ATM layer cell. Figure 2.26 shows the format of the CPS PDU with a 3-byte overhead. The Channel Identifier (CID) field is a logical identifier of the virtual connection to which this information unit belongs. The Length Indicator (LI) field denotes the length of the CPS packet; the default value considered here is 45 bytes (CPS packet), so that the corresponding CPS PDU represents the cell payload with AAL2 (if the CPS packet is longer than 45 bytes, segmentation is needed to generate more CPS PDUs). The User-to-User Indication (UUI) field is used to convey end-to-end user data or to support OAM operations. The Header Error Control (HEC) is a code to protect the first 19 bits of the CPS PDU.

The 48-byte cell payload formats for AAL3 and AAL4 are detailed in Fig. 2.27 and are characterized by a 4-byte overhead. The Segment Type (ST) field denotes if a cell is BOM, COM or EOM of a higher-layer PDU or if it represents a non-segmented unit (an SSM, i.e., a PDU segmented in a single payload unit). SN allows numbering subsequent data units. In the AAL3 case, the RES field is reserved for special applications. Instead, in the AAL4 case, the Multiplexing Identifier (MID) is used to multiplex different higher-layer messages on the same virtual connection. In the trailer, the Length Identifier (LI) field permits to specify

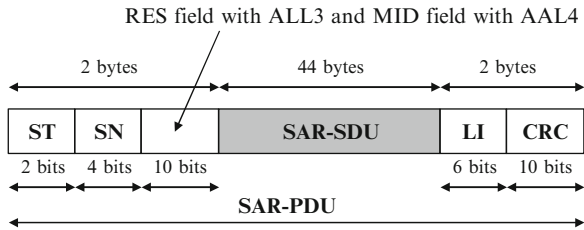


Fig. 2.27 AAL3 and ALL4 cell payload formats (SAR-PDU)

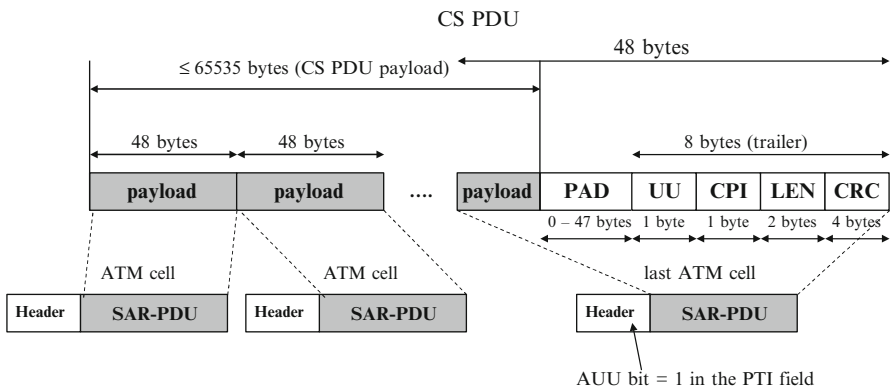
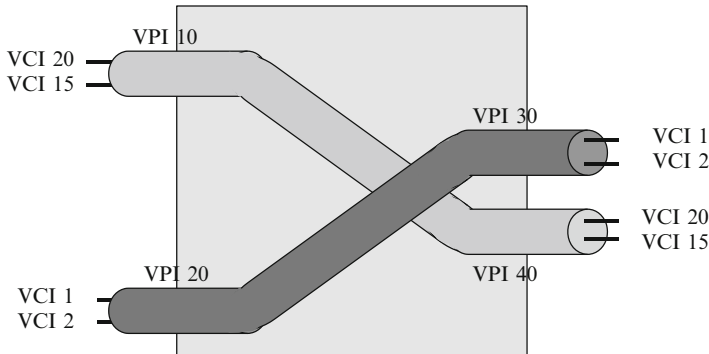


Fig. 2.28 AAL5: CS PDU segmentation for ATM cell generation

when the SAR-SDU (i.e., the information field) is shorter than 44 bytes. The Cyclic Redundancy Check (CRC) is a code to protect the entire SAR-PDU. In conclusion, we can state that the ATM cell payload capacity is strongly reduced because of the overhead bits of AAL3/AAL4. These AALs do not allow an efficient use of transmission resources.

The AAL5 protocol has been defined to achieve a better efficiency than AAL3/AAL4. This goal is obtained by reducing the control fields. In particular, AAL5 adopts a cumulative overhead at the CS PDU level: a 8-byte trailer is added. It is necessary to delimit the number of cells belonging to the same CS PDU; this is obtained by setting the AUU bit equal to 1 in the header (PTI field) of the last cell in the cell train produced by one CS PDU. The format of the AAL5 CS PDU is shown in Fig. 2.28. The CS PDU payload has a variable length up to 65,535 bytes; such length is coded by the Length (LEN) field in the trailer. A PAD field is used to have that the whole CS PDU has a length multiple of 48 bytes, so that the consequent generation of ATM cells is easier. The User-to-User (UU) field conveys transparent information from user to user. The Common Part Indicator (CPI) has the function to extend the trailer to a length of 8 bytes. Finally, a CRC field is used for revealing errors in the entire CS PDU.

Since AAL5 does not use flow identifiers, different AAL5 flows cannot be multiplexed onto the same ATM connection (VPI, VCI). This means that CS



**Fig. 2.29** ATM cross-connect switch

PDU belonging to different flows cannot be mixed on a connection, but must be sequentially transmitted.

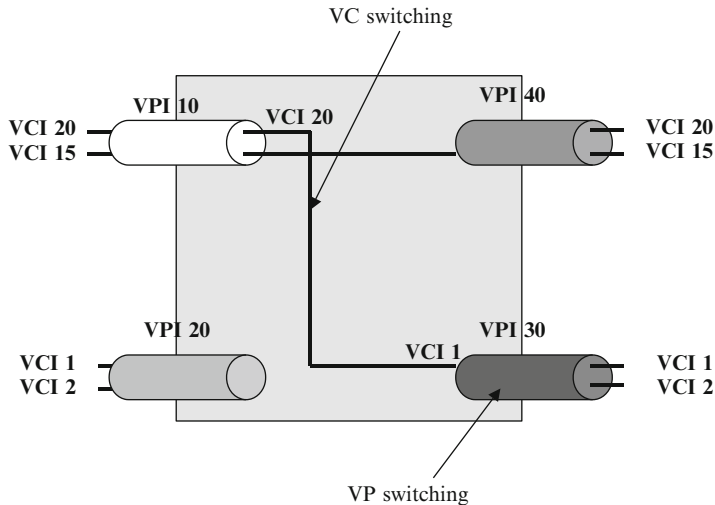
Even if AAL5 allows a CS PDU with maximum length of 65,536 bytes, RFC 1577 (and subsequent specifications) have defined a maximum length of 9,180 bytes in order to provide compatibility with the Switched Multi-megabit Data Service<sup>5</sup> (SMDS) [37].

### 2.2.5 ATM Switches

The switch is the crucial element of the ATM network architecture [38, 39]. It operates at layer 2 (ATM layer) and realizes the virtual circuit-switching by receiving a cell on an input port with a given VPI + VCI and by switching it (according to routing instructions defined in the path setup phase) to an output port with, in general, a new couple of values for VPI and VCI. However, there can be cases with only changes of VPI (see below) or even cases in which the pair VPI + VCI does not change. Two typical ATM switch architectures are detailed in Figs. 2.29 and 2.30. In the first case (also called ATM cross-connect), we have a switch where a cell only changes its VPI from input to output. Instead, in the second case (the most common case for ATM switches), a cell changes both VPI and VCI from input to output.

The ATM cross-connect switch can be considered as a first, simplified implementation of an ATM switch and can manage at most 4,096 ( $=2^{12}$ , as the VPI field contains 12 bits) input virtual circuits.

<sup>5</sup> SMDS was a public-switched broadband data service adopted in North America to interconnect local area networks and powerful computers across wide areas. It was based on the IEEE 802.6 standard.



**Fig. 2.30** ATM switch. We have highlighted that the input VCI = 20, VPI = 10 is switched to the output VCI = 1, VPI = 30

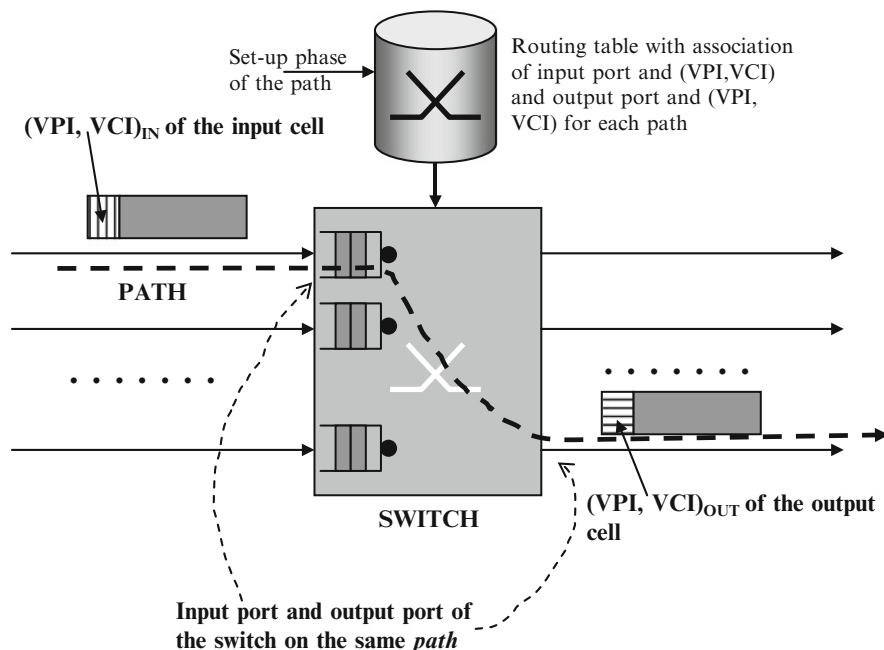
### 2.2.6 ATM Switch Architectures

The ATM network is connection-oriented: a virtual (i.e., logical) end-to-end path must be established before data transfer can take place. Switching is performed at the ATM layer: each switch along the path associates/translates the VPI/VCI of its input port with the appropriate VPI/VCI of the output port. This is possible because during the setup phase each switch updates its switching (routing) table with the association between the input port and the input VPI + VCI and the output port and the output VPI + VCI. Since the output cell has a new pair VPI + VCI with respect to the input one, the HEC field needs to be recomputed; see Fig. 2.31.

The switch typically connects one input to one output, but it may also support multicast (point-to-multipoint) connections, where it connects one input to many outputs. Three major factors have a large impact on the implementation (architecture) of an ATM switch:

- The high speed at which the switch has to operate (from 150 Mbit/s up to 2 Gbit/s).
- The statistical behavior of the ATM flows crossing the switch.
- Routing tables (mainly, these tables are pre-compiled for PVCs to minimize the complexity of the switch).

An ATM switch can be seen as a black box with  $N$  input lines and  $N$  output lines. A switch is composed of the following parts: (1) an input port block to interface input lines, (2) the switching fabric, (3) the output port block to interface output



**Fig. 2.31** Switching procedures at a node (switch); input and output ports are associated with (VPI, VCI) couples

lines. When a cell is received from a line, its header is processed by the input port to determine to which output port is destined on the basis of the routing table.

Within the node, it may occur that different cells simultaneously need to be addressed to the same output port, thus contenting for output resources (i.e., a conflict in the use of output resources). In such circumstances, only one cell must be selected at a time, while the other cells need to be buffered; this is the classical Head-Of-Line (HOL) problem. Buffers can be placed in either input ports (see Fig. 2.31) or output ones; a third solution adopts buffers at the switching fabric level (central buffering); a last approach uses buffers for both input and output.

A blocking phenomenon can also happen internally to the switching fabric when more cells should simultaneously use the same "internal links" between different switch stages (this problem is similar to that described in Sect. 1.6.2). Even in this case, buffering is needed either within the switch or at the input of the switch.

### 2.2.6.1 Input Buffering

Input buffering uses a dedicated buffer for each input port. Buffers manage cells in a First-Input First-Output (FIFO) basis. The solution with input buffers has the problem that a cell at the top of an input buffer may be blocked due to repeated conflicts on the output port. Such cell blocks all the other cells in the same input

buffer even if they could be delivered without conflicts to their output lines. This is the HOL problem, which causes a significant throughput reduction. In this case, the switching fabric works at the same speed of input ports (related to cell time).

### 2.2.6.2 Output Buffering

Output buffering uses a dedicated buffer for each output port. Cells destined to the same output port are stored in a FIFO buffer, waiting for transmission. The output port can only service one cell each time. Collisions happen when two cells are destined to the same output port. These collisions could be avoided if the switching fabric runs  $N$  ( $N$  = number of input ports) times faster than the speed of input ports. Output buffering is considered superior to input buffering in terms of throughput (theoretically, the maximum 100 % throughput is possible) and delay and avoids HOL problems. However, there can be scalability issues for large switches due to the speed increase that is needed to avoid collisions.

### 2.2.6.3 Internal Buffering (Shared-Memory Approach)

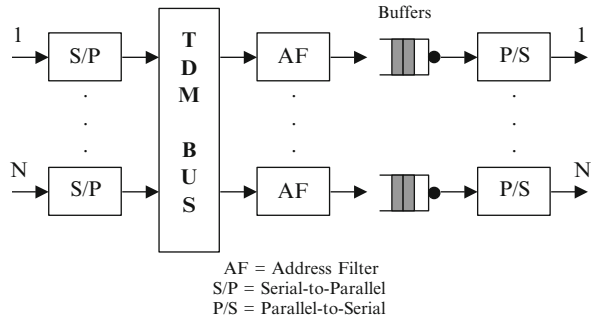
Central buffering uses a shared-memory inside the switch. Instead of having a one-to-one relation between queues and input or output ports, all the ports share the same queue. The use of a shared-memory has the advantage to support both queuing and switching: both functions can be implemented together, appropriately controlling reading and writing phases in the memory. This method does not suffer from HOL blocking and has the same speed requirements of the switching fabric with output buffering. Moreover, by modifying the memory read/write control circuits, the shared-memory switch can be flexible enough to support functions such as priority control and multicast.

### 2.2.6.4 Switching Techniques

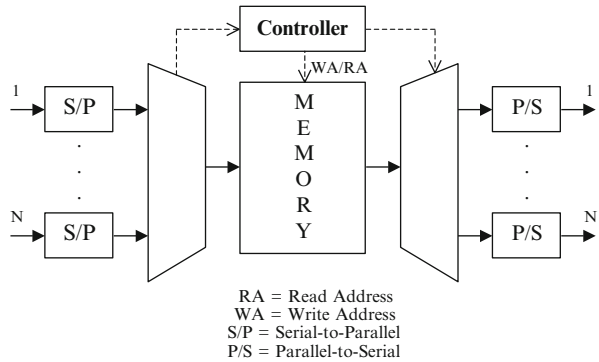
A critical requirement for ATM networks is to realize a fast packet-switching of virtual paths. Three basic techniques have been proposed for the switching function: shared-medium, shared-memory, and space-division [39].

A *shared-medium* switch puts all incoming cells on a common medium such as a bus, a ring or a dual bus. Time-division multiplexed (TDM) buses are a common example for this approach, as shown in Fig. 2.32. When a cell arrives at an input port, the outgoing link for that cell is identified with the related pair VPI + VCI. Then, the cell is tagged with the address of the output port and passed to the medium. Arriving cells are broadcast on the TDM bus. At each output, Address Filters (AFs) read the tag and decide whether to pass the cells to the related output buffer. The shared-medium speed must be at least equal to the sum of the speeds of all the  $N$  input lines of the switch. In this architecture, two cells cannot arrive

**Fig. 2.32** Shared-medium (i.e., TDM bus) switch architecture



**Fig. 2.33** Shared-memory switch architecture

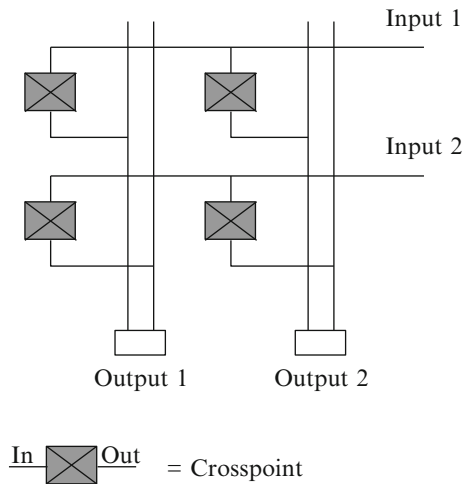


simultaneously at the same output port. They may, however, arrive at an output port faster than they can be served so that output buffers are needed to manage these situations.

An advantage of this shared-medium architecture is that it easily supports broadcast and multicast transmissions. As a result, many of these switches have been implemented by IBM, NEC, etc. However, because the address filters and output buffers must operate at the shared-medium speed, which is  $N$  times faster than the input port speed, there is a physical limitation to the scalability of this approach. Moreover, output buffers are not shared, thus requiring a greater amount of memory to guarantee the same cell loss rate. Finally, the shared-medium represents a single point of failure.

A *shared-memory* switch consists of a single dual-port memory shared by all input and output lines (see Fig. 2.33). Incoming cells are converted from serial to parallel form, and written in a Dual port Random Access Memory (DRAM). Inside the memory, cells are organized into separate queues, one for each output line. The shared-memory allows up to  $N$  concurrent write accesses by the  $N$  input ports and up to  $N$  concurrent read accesses by the  $N$  output ports. A memory controller generates an output stream of packets. Outgoing cells are converted from parallel to serial form to be transmitted on the output lines. This is an output queuing approach. There are two different ways to obtain a shared-memory switch:

**Fig. 2.34**  $2 \times 2$  crossbar switch architecture. Switches for  $N > 2$  can be obtained in a similar way by using multiple stages with  $2 \times 2$  crossbar switches



- *Full memory sharing*: All the output ports share the entire memory. Cells are dropped only if the entire memory is full. There can be unfairness issues when a burst of cells arrives at a particular output port. This may cause performance degradation for the flows related to the other ports.
- *Complete partitioning*: There is an upper limit to the number of cells in the queue for each output port. The disadvantage of this approach is that cells may be dropped (when the corresponding output queue buffering limit is reached) even if there is space available in the memory. This causes an inefficient utilization of the memory.

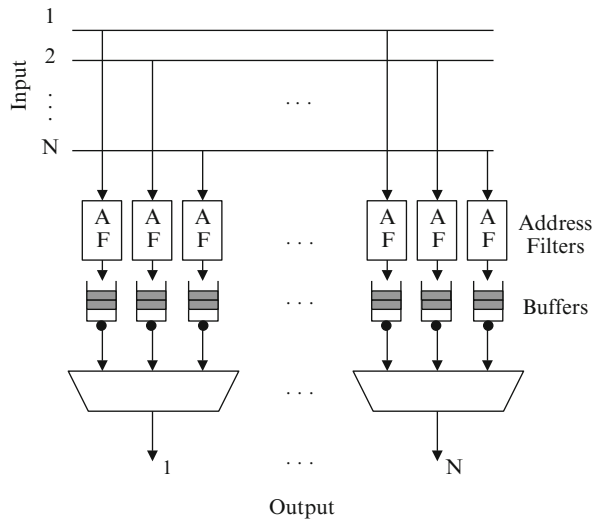
The shared-memory architecture has the same disadvantages of shared-medium, since the memory is a single point of failure. Moreover, there are scalability issues deriving from the memory access speed and the memory bandwidth, which must be at least the sum of the bandwidth of input and output lines.

Note that shared-medium and shared-memory switches are time-division architectures.

In *space-division architectures*, a physical path is established from one input to one output in order to form the switched path. The following alternatives are available for space-division switches:

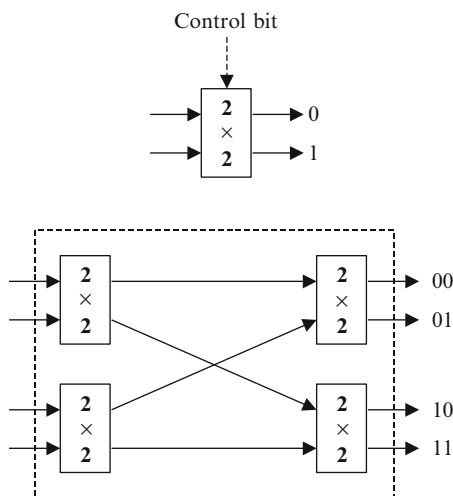
- *Basic crossbar switch*: Each input port has a connection point (i.e., a *crosspoint*) with each output port (see Fig. 2.34). A matrix-like space-division switching fabric is adopted, which physically interconnects any of the  $N$  inputs with any of the  $N$  outputs. When two cells from different input ports are destined to the same output port, one of the cells will be blocked and cleared. For obtaining an  $N \times N$  switch,  $N^2$  crosspoints are needed. Multi-stage switching fabrics can permit to construct a larger switch from more simple ones in order to reduce the number of crosspoints.



**Fig. 2.35** Knockout switch architecture

- *Knockout switch*: An improved version of the crossbar switch referred to as a Knockout switch has solved the blocking problem. Let us consider the switch architecture in Fig. 2.35. Each input has a separate broadcast bus. Each output has a block of Address Filters (AFs), one for each input bus. These filters select the appropriate cells for the output. Output FIFO buffering is needed, since packets from different inputs can arrive simultaneously at the same output. A scheduling mechanism, called arbiter/concentrator, is used to decide which cell to send from each output queue. This is a *fully interconnected switch*: since each input has a direct path to every output, no blocking occurs. The Knockout switch refers to the case where instead of using  $N$  different queues at the output, only  $L$  ( $<N$ ) queues are used. This technique is based on the observation that it is unlikely that more than  $L$  cells will arrive simultaneously at a given output.
- *Banyan and Delta-Banyan switches*: A Banyan architecture is a multi-stage switching fabric with a tree topology. Each input port is the root of a tree where output ports are the leaf nodes. A Banyan network is obtained as the interconnection of stages of elementary  $2 \times 2$  switching elements. The structure of a  $4 \times 4$  switching fabric (with the related  $2 \times 2$  elementary building blocks) is shown in Fig. 2.36. The  $2 \times 2$  elementary building block can route an incoming cell according to a control bit that corresponds to the output address. If the control bit is 0, the cell is routed to the upper port address, otherwise the cell is routed to the lower port address. As for the resulting  $4 \times 4$  switching fabric, the first bit of the output address denotes which switching element to route to, and then the last bit specifies the port. By extending the  $4 \times 4$  scheme, it is possible to build a  $8 \times 8$  switch fabric and so on. A switching fabric with multiple stages is said to be *self-routing* (or digit-controlled routing) when the output port address completely specifies the route through the switching network. Each input controller prefixes a routing tag (corresponding to the output address) onto every incoming cell using

**Fig. 2.36**  $4 \times 4$  Banyan switching fabric obtained from elementary  $2 \times 2$  switches



the same lookup table used for VPI/VCI translation. The Banyan switch enables self-routing and is popular, since the fabric is obtained by using simple elements, cells are routed in parallel, all elements operate at the same speed, and the architecture is scalable.

Delta networks are a subclass of Banyan networks. There are numerous types of delta networks, such as rectangular (where the switching elements have the same number of inputs and outputs), omega, flip, cube, shuffle-exchange, and baseline delta networks. The major advantage of these switches is their scalability. One disadvantage is that they suffer from internal blocking when two cells attempt to use the same internal link between two stages of the switching fabric. The solution to this problem is provided by the switching technique described below.

- *Batcher-Banyan switch*: In order to avoid internal blocking problems, a sort network (Batcher sort network) is added to arrange the cells before the Banyan network. In particular, cells are sorted in such a way that internal blocking is avoided. However, if cells are addressed to the same output port at the same time, the only solution to avoid cell blocking is buffering.

### 2.2.7 Management of Traffic

In ATM networks, flow control and error control are not operated at intermediate nodes, but only end-to-end. It is important to control not only the quality of the traffic but also its quantity in order not to congest some network nodes with the consequent increase in the delays experienced by all the related virtual circuits. Therefore, suitable techniques must be used to prevent congestion conditions.

In circuit-switched networks, congestion control is simply operated during the setup phase of the end-to-end link; in fact, it is necessary to check the availability of resources on all the links along the source-to-destination path (CAC technique). Such approach is not sufficient in ATM networks, since traffic sources may generate variable bit-rate: their loads are unpredictable. In addition to this, the adoption of packet-switching causes that links are shared by several paths and have a variable congestion level. The traffic management problem is complicated by the fact that there can be different types of traffic sources with different characteristics and QoS requirements. Hence, each traffic flow must have guaranteed a given bandwidth {we will expand later this concept in terms of *equivalent bandwidth* [40–44]} in the different links of the path in order to fulfill its QoS levels.

In ATM, the traffic can be with or without QoS guarantees. CBR and VBR belong to the first case; ABR and UBR belong to the second case. Referring to QoS-guaranteed traffic, two different types of techniques can be considered: *preventive control* (e.g., traffic load control) and *reactive control* (i.e., congestion control). Preventive control is used to decide whether a new connection can be admitted in the network (CAC technique), to smooth its traffic, and to monitor the input traffic on the connection to avoid unacceptable traffic peaks (Usage Parameter Control, UPC). Reactive control entails an action taken when a congestion event has occurred; the problem of this approach is that it implies an end-to-end delay before a repair action can start.

ATM networks can implement one or a combination of the following control functions to meet the QoS objectives of connections.

- Preventive control:
  - CAC
  - Resource reservation into the network
  - Traffic shaping
  - UPC, i.e., traffic policing
  - Traffic scheduling at nodes
- Reactive control:
  - Explicit Forward Congestion Indication (EFCI) together with end-to-end feedback signaling to notify the source to reduce the traffic rate.

Before starting the description of these control techniques, we need both to characterize the traffic sources in terms of traffic descriptors and to define their QoS parameters. On the basis of the taxonomy provided in Fig. 2.24, the following *services* have been defined in ATM networks for the support of the bit-rate generated by traffic sources:

- Constant Bit-Rate (CBR)
- Variable Bit-Rate (VBR)
  - Real-time VBR
  - Non-real-time VBR

**Table 2.2** Characterization of ATM services

	CBR	rt-VBR	nrt-VBR	ABR	UBR
Bandwidth guarantee	Yes	Equivalent	Equivalent	Minimum	No
Real-time traffic	Yes	Yes	No	No	No
Data bursty traffic	No	Yes	Yes	Yes	Yes
Congestion notification	No	No	No	Yes <sup>a</sup>	No

<sup>a</sup>ABR is the only traffic class, which foresees a congestion notification to invite the traffic source to reduce its traffic injection into the network (i.e., reducing the bit-rate)

- Available Bit-Rate (ABR)
- Unspecified Bit-Rate (UBR)
- Guaranteed Frame Rate (GFR)<sup>6</sup>

The characterization of these services is summarized in Table 2.2; we can better understand this table if it is considered together with Fig. 2.24. Note that a fixed bandwidth is reserved in the network for CBR sources, whereas an equivalent bandwidth must be available on all the links of the path to accept an rt-VBR or a nrt-VBR traffic source. A minimum end-to-end bandwidth is guaranteed for ABR sources, but even a greater bandwidth can be dynamically assigned to them, if available. Finally, there is no capacity guarantee for UBR traffic sources.

The equivalent bandwidth for a given traffic source,  $B_{eq}$ , is a complex parameter to be derived; it represents the bandwidth needed to guarantee some QoS levels for the generated traffic. Different equivalent bandwidth formulas are available, depending on the characteristics of the traffic source and the QoS requirements. There is a rich literature on the equivalent bandwidth. For more details, the interested reader could refer to [40–44]. For instance, the equivalent bandwidth of an rt-VBR traffic source can be determined assuming that this traffic arrives at a queue having a service rate of  $B_{eq}$  bit/s. Due to this service capability, the traffic experiences a delay, which is a random variable. Since rt-VBR is a real-time traffic, a QoS requirement is represented by a deadline, i.e., a maximum delay within which each cell has to be transmitted. The  $B_{eq}$  value can be determined by imposing a constraint on the probability that the service delay exceeds the deadline, thus causing packet dropping. Hence, we can refer to the following example of  $B_{eq}$  characterization:

$$B_{eq} : \text{Prob}\{\text{service delay}(B_{eq}) > \text{deadline}\} \leq 5\% \quad (2.6)$$

For an rt-VBR source, we can generally consider that  $\text{SRC} \leq B_{eq} \leq \text{PRC}$ .

Traffic descriptors detailed in Table 2.3 are used to characterize the traffic generated by a given source. Referring to this Table, PCR denotes the maximum

<sup>6</sup>This service is practically UBR with a guaranteed Minimum Cell Rate (MCR). The peculiarity of GFR is that it is used jointly with ALL5 and that if one cell of a higher layer message is dropped (due to congestion at a buffer), all the other cells of the same message are dropped. We will not provide further details on GFR in what follows.

**Table 2.3** Connection traffic descriptors

	Acronym	Definition
Peak Cell Rate	PCR	Maximum rate according to which cells will be sent in the network
Sustainable Cell Rate	SCR	Mean rate (long term value) according to which cells will be sent in the network
Minimum Cell Rate	MCR	Minimum acceptable rate of cells in the network
Maximum Burst Size	MBS	Maximum number of cells that can be sent together (in a burst) at the line rate (PCR)
Cell Delay Variation Tolerance	CDVT	Maximum acceptable difference in the delay of output cells at a node (related to queuing delays)

**Table 2.4** QoS parameters

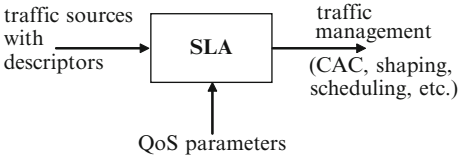
	Acronym	Definition
Cell Loss Ratio	CLR	Percentage of lost (or late) cells
Cell Transfer Delay	CTD	End-to-end delay for the transmission of a cell (maximum and mean value)
Cell Delay Variation	CDV	Variance of the end-to-end transmission delay of a cell
Cell Error Ratio	CER	Percentage of erroneous cells
Cell Misinsertion Rate	CMR	Percentage of erroneously delivered cells (routing error) among all the cells of a flow

bit-rate allowed to the source and SCR corresponds to the mean bit-rate. Hence, the source burstiness factor is  $\beta = \text{PCR}/\text{SCR}$ ; of course a CBR source has  $\beta = 1$ . The greater the traffic source burstiness, the higher the multiplexing gain by aggregating many sources of this type on the same link.

In ATM networks, there are many parameters to describe the QoS requested by a traffic source; some of them are detailed in Table 2.4. These parameters are measured at the receiver.

For traffic with QoS guarantees, the user and the network stipulate a *traffic contract*, also called Service Level Agreement (SLA). Such traffic contract specifies a traffic conformance algorithm and the expected QoS provided by the network under some traffic characteristics as defined by the descriptors (e.g., PCR, SCR, MBS, MCR, and CDVT). The guaranteed QoS level can be in terms of maxCTD, CDV, CLR, etc. Note that CDV is measured as follows:  $\text{CDV} = \text{maxCTD} - \text{minCTD}$ . The network agrees to meet or exceed (for some small percentage of time) the QoS negotiated as long as the traffic source complies with the contract [45]. UBR traffic does not require a traffic description, since it has no QoS guarantee. ABR traffic has guaranteed just the MCR. ABR and UBR traffic classes should have no impact on the QoS provided to guaranteed-QoS traffic classes. The QoS support approach envisaged in ATM networks is described in Fig. 2.37.

ATM layer functions (e.g., cell multiplexing) may alter the traffic characteristics of connections by introducing some Cell Delay Variation (CDV). When cells from two or more connections are multiplexed, the cells of a given connection may be delayed because of the presence of cells of other connections. Similar problems are



**Fig. 2.37** Conceptual scheme of the relation (depending on the SLA) between traffic source characteristics/classes, QoS parameters/requirements and traffic management

	ATM Layer Service Category					
Attribute	CBR	rt-VBR	nrt-VBR	UBR	ABR	GFR
Traffic parameters: (4)						
PCR and CDVT (5)	Specified			Specified (2)	Specified (3)	Specified
SCR, MBS, CDVT (5)	n/a	Specified		n/a		
MCR	n/a				Specified	n/a
MCR, MBS, MFS, CDVT (5)	n/a					Specified
QoS Parameters:						
Peak-to-peak CDV	Specified		Unspecified			
Max CTD	Specified		Unspecified			
CLR	Specified			Unspecified	(1)	

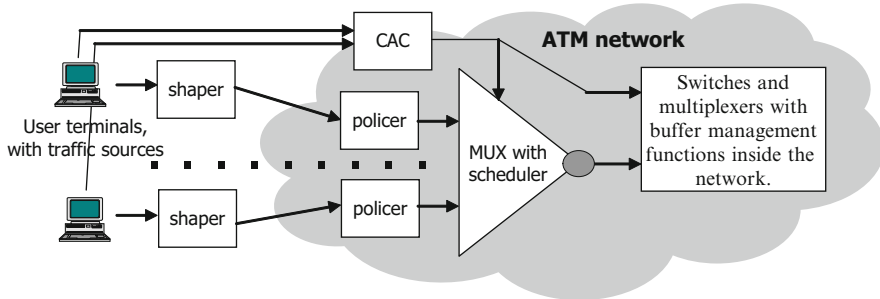
- Notes:
- 1. CLR is low for sources that adjust cell flow in response to control information. The CLR requirement is network-specific.
  - 2. Might not be subject to CAC and UPC procedures.
  - 3. Represents the maximum rate at which the ABR source may ever send. The actual rate is subject to the control information.
  - 4. These parameters are either explicitly or implicitly specified for virtual circuits.
  - 5. CDVT is not signaled. In general, CDVT has not a unique value for a connection. Different values may apply at each interface along the path of a connection.

**Fig. 2.38** ATM attributes of service categories

due to the insertion of OAM cells in a traffic flow. Consequently, with reference to the peak emission interval (i.e., the minimum interarrival time, obtained as the inverse of PCR), some randomness may affect the interarrival time between consecutive cells of a given connection, as monitored at the UNI. The upper bound to this delay variation is regulated by the delay tolerance parameter CDVT [46]: the CDVT allocated to a particular connection provides a limit to the delay differences among the cells belonging to the same traffic flow. Analogous considerations are valid if we refer to the sustained emission interval (i.e., the inverse of the contracted SCR).

Finally, Fig. 2.38 describes the attributes of the different service categories (i.e., CBR, VBR, etc.), as defined by the ATM Forum [46].

In a typical ATM access network, we have different traffic sources, each regulated by a traffic shaper, a CAC block, policers to monitor the traffic loads injected by the different sources, and a multiplex with scheduler to regulate the resource sharing on the access link. All these elements cooperate to support the QoS in ATM networks, according to the conceptual scheme shown in Fig. 2.39. These functions that are described in the following subsections (e.g., policing, shaping, scheduling) are also relevant to IP networks (see Chap. 3).



**Fig. 2.39** Conceptual scheme for traffic management with QoS support in ATM

### 2.2.7.1 Resource Reservation into the Network

At connection setup, an end-to-end path must be established between the source and the destination. This operation entails some form of reservation and management of the resources along the path (i.e., storage and transmission capacities).

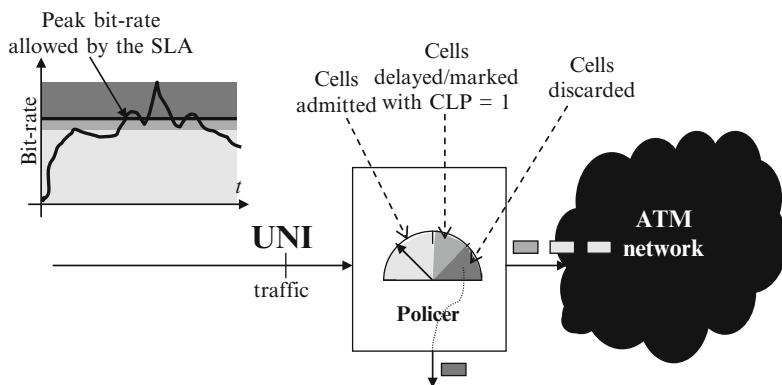
### 2.2.7.2 Connection Admission Control

CAC is a control operated by the network at the setup of a new connection to verify whether the QoS requirements can be fulfilled for both the new connection and the connections already in progress [46]. CAC procedures, based on traffic descriptors (see Table 2.3), permit to allocate resources and to derive parameter values for UPC operation. Several CAC techniques can be considered; they are generically categorized in two broad groups: (1) CAC based on bandwidth aspects; (2) CAC based on CLR considerations. In what follows, an example is provided about CAC dependent on bandwidth aspects.

Let us refer to VBR traffic sources (bursty traffic) on a shared access link to the ATM network. It would be highly inefficient to reserve the bandwidth corresponding to the PCR value for each VBR connection; hence, it is important to allocate the equivalent bandwidth for each VBR flow [40–44]. Let  $C$  denote the capacity of the link and let  $B_{eqi}$  the equivalent bandwidth of the  $i$ th VBR connection on the same link. A new VBR traffic source with equivalent bandwidth  $B_{eq}$  fulfills the CAC condition and, hence, is admitted if the following condition is fulfilled:

$$\sum_i B_{eqi} + B_{eq} \leq C \quad (2.7)$$

Otherwise, the new connection is rejected.



**Fig. 2.40** Traffic policer based on a UNI conformance test, which monitors input traffic and compares it with the traffic contract (SLA)

### 2.2.7.3 Usage Parameter Control

CAC operated in the setup phase is an important control to guarantee the QoS, but it cannot protect from the risk that an admitted traffic source overloads the network. Therefore, the main purpose of UPC is to protect network resources from malicious as well as unintentional misbehaviors, which can affect the QoS of already-established connections. UPC entails a monitoring action performed for each connection. UPC is based on ITU-T Recommendations I.356 [47] and I.371 [45].

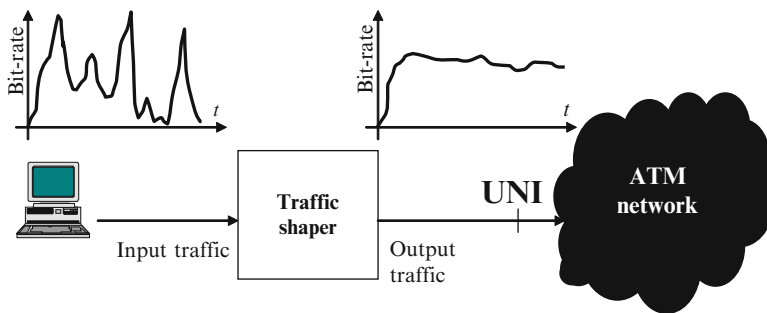
There can be both temporary traffic bursts produced by VBR sources or persistent traffic loads violating the contract stipulated with the network as verified in the CAC phase. In order to cope with these problems, UPC techniques are used on the network side of UNI. UPC is intended to ensure the conformance of a virtual connection with the negotiated traffic contract. The connection traffic descriptors contain the necessary information for *testing the conformance* of the cells generated. Conformance applies to cells as they pass UNI: cells are tested according to some algorithm so that the network may decide whether a connection is compliant or not. The UPC function is implemented in the *policer* on the network side of UNI [46]. Referring to Fig. 2.40, the policer shall be capable of

- Passing a cell that is conformant to connection traffic descriptors.
- Discarding a cell if it is not conformant to connection traffic descriptors; alternatively, if the tagging option is allowed for a connection, the policer shall be capable of converting CLP from 0 to 1 for a non-conformant cell, which is accepted into the network.

The action operated by a policer is quite similar to the flow control scheme adopted in frame relay networks (see Sect. 2.1.3.2).

ITU-T and ATM Forum have defined the Generic Control Rate Algorithm (GCRA) to be used for the conformance test. GCRA can be considered as a virtual





**Fig. 2.41** Traffic shaper

scheduling algorithm [46]. A GCRA test can be suitably defined for each ATM traffic class. GCRA can be used to control the peak cell rate, PCR. Otherwise, GCRA can be used to verify whether the cell rate is within some requested bounds on a given time window (i.e., SCR control). Moreover, different GCRA schemes can also be combined to obtain a more complex conformance test based on multiple parameters (e.g., PCR and SCR). GCRA algorithms (suitable not only for policing but also for traffic shaping) are of the following types:

1. PCR policing for CBR sources.
2. Combined SCR and MBS policing for VBR sources without limits on PCR.
3. Combined PCR, SCR and MBS (or CDVT) policing for VBR sources with PCR, SCR and burst (or delay, packet loss) limitations.

The effectiveness of CAC schemes depends on the fulfillment of the traffic contracts for the different traffic flows, as monitored by the policers.

#### 2.2.7.4 Traffic Shaping

Traffic shaping is a mechanism, which alters the traffic characteristics of a stream of cells to match its SLA. Traffic shaping allows us controlling the outgoing traffic, thereby eliminating bottlenecks because of data-rate mismatches. Each connection is subject to traffic shaping in an ATM network.

Let us refer to traffic shaping on the terminal side at UNI; it consists in filtering the input traffic of a source in order to reduce its burstiness. At the output of this regulator, the traffic offered to the network (UNI interface) is more regular, smoothed (almost constant). Avoiding burstiness is an important need for the networks, since sudden traffic peaks may cause congestion at node buffers and high delays. However, traffic may have a residual burstiness at the output of the shaper. This is important, because a shaper that completely smoothes the traffic may entail unacceptable delays in the delivery of the cells. The traffic shaper action on the input traffic is depicted in Fig. 2.41.

Policers and shapers usually have common structures. They identify traffic descriptors violations in identical ways. They are both based on a conformance test,<sup>7</sup> but differ in the way they respond to violations. In fact, a policer monitors input cells (does not regulate them) and drops or marks them if the conformance test fails (i.e., the traffic contract is exceeded). Instead, a shaper includes not only an algorithm for conformance test but also a queue: if cells exceed the traffic contract they are queued, not dropped.

Traffic shaper and policer should work in tandem. A good traffic shaping scheme should make it easier to detect misbehaving flows at the entrance of the network.

The determination of the parameters for the traffic shaping algorithms is a quite complex task due to the multiplexing of different traffic sources. In fact, the shaper can determine the conformance time for the transmission of each cell arriving on a link. However, there can be conflicts when multiple cells, from different connections, become eligible for transmission in the same time slot. As a result, the shaper can have a backlog of conformant cells, particularly when traffic arrives from multiple input links. These collisions can distort the shaped traffic flows and increase delays, even for conformant cells.

In what follows, we will examine two typical traffic shapers: the *leaky bucket* regulator and the *token bucket* regulator; with slight modifications they can also be used as policers. *Dual leaky bucket* and *dual token bucket* schemes will be shortly discussed as well.

Traffic shaping techniques have recently gained considerable importance in MPLS and in Integrated or Differentiated Services for QoS support in IP networks.

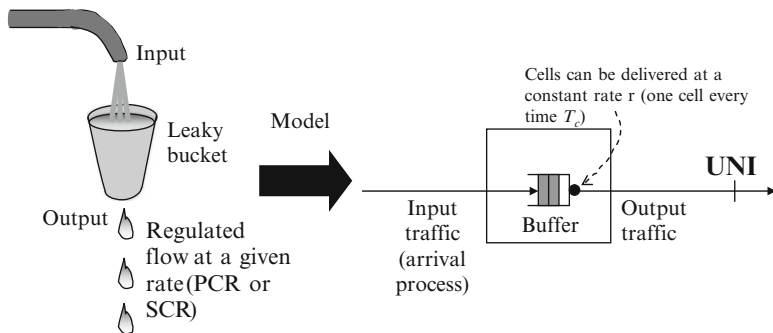
### Leaky Bucket Shaper

In this case, the traffic shaper is simply a buffer, which is able to deliver cells at a predetermined rate. The output cell rate is regulated at a given value at the expenses of increased delays experienced by the cells (the greater the input traffic burstiness, the higher the delays). A typical regulation could be based on PCR for type #1 GCRA or on SCR for type #2 GCRA, referring to the list of regulators at the end of Sect. 2.2.7.3. See Fig. 2.42. The buffer should have limited rooms if we want to constraint the delay caused by the shaper (i.e., the contribution to CTD). This constraint is fulfilled at the expenses of some losses for those cells arriving at a full leaky bucket buffer (overflowing cells are discarded).

The analytical model of a leaky bucket regulator is a G/D/1 queue (see Chap. 6), where “G” refers to a general input arrival process of cells, “D” is related to the deterministic time to deliver a cell (i.e., time  $T_c$ , according to Fig. 2.42), and “1” means that one cell is delivered to the network at a time. Actually, we should consider a queue of finite length.

---

<sup>7</sup> It is possible that the same type of test is used in both shaper and policer.

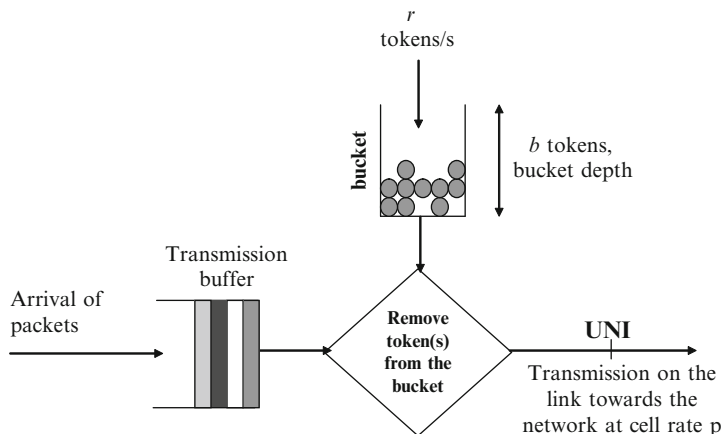


**Fig. 2.42** Leaky bucket traffic shaper: conceptual scheme and model based on queuing theory

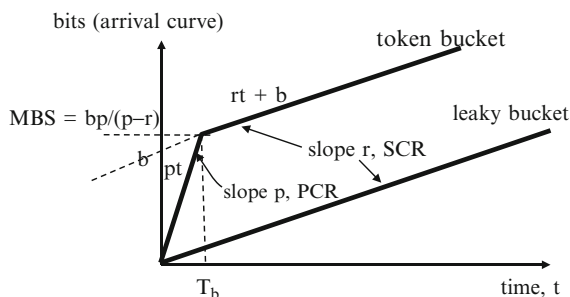
### Token Bucket Shaper

This traffic shaping scheme adopts both a token bucket and a data queue (it becomes a policer if there is no data queue). Tokens are put into the bucket at a certain rate. The bucket has a maximum capacity of tokens (i.e., bucket depth). If the bucket is full, newly arriving tokens are discarded. Each token represents the permission for the source to transmit a certain number of bits in the network. In order to send a cell, the regulator must remove from the bucket a number of tokens corresponding to the cell size. If the bucket does not contain a sufficient number of tokens to transmit a cell, the cell either waits until the bucket has enough tokens or the cell is discarded or the cell is marked and transmitted. If the bucket is already full of tokens, incoming tokens overflow and are not available for future cells. The token bucket regulator permits to maintain some traffic burstiness at the output; this is an advantage with respect to the leaky bucket shaper. The largest burst (i.e., MBS, the maximum length of a burst of data, which are transmitted at the maximum speed, PCR) a source can send into the network with the token bucket shaper is proportional to the bucket depth.

The model of the token bucket regulator is characterized by  $(r, b, p)$ , where  $r$  denotes the rate at which tokens are accumulated,  $b$  is the depth of the bucket, and  $p$  is the maximum transmission rate (PCR); see Fig. 2.43. For instance, let us simply consider that a token is the permission to transmit one cell. The token bucket regulates the output traffic, guaranteeing a regime cell rate of  $r$  cells/s, that is SCR. The bucket depth  $b$  allows the transmission of up to  $b$  cells at the maximum rate  $p$  ( $>r$ ), thus having some burstiness for the output traffic (MBS). The arrival curve of a traffic source denotes the cumulative number of bits generated as a function of time. The arrival curve of a token-bucket-regulated source is shown in Fig. 2.44 and the asymptotic burstiness index of the output flow (upper bound to traffic) is  $\beta = p/r$ . The token bucket regulator described here implements a GCRA algorithm of type #2, according to the categorization at the end of Sect. 2.2.7.3. Further details on the token bucket shaper will be provided in Sect. 3.5.1 in relation to the Guaranteed Service of IntServ.



**Fig. 2.43** Token bucket shaper according to the  $(r, b, p)$  model

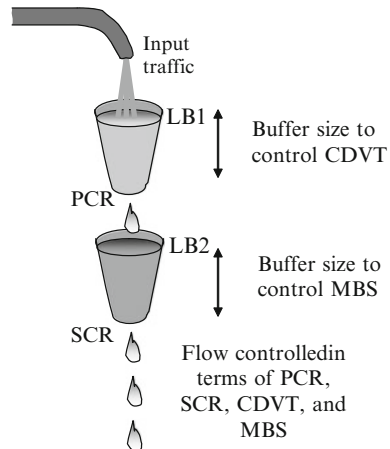


**Fig. 2.44** Arrival curve model of the output traffic for a token bucket shaper, characterized by PCR, SCR, and MBS; comparison with the arrival curve of the leaky bucket shaper

Another variant of the token bucket regulator is the dual token bucket, which adopts two cascade token buckets.<sup>8</sup> Two alternatives are possible: (1) the *single-rate token bucket* with SCR regulation and where the tokens overflowed from the first bucket are placed in a second bucket to transmit excess traffic peaks (GCRA algorithm of type #2); (2) the *dual-rate token bucket* with token rates corresponding to both PCR and SCR regulations (GCRA algorithm of type #3).

<sup>8</sup> Both classical token bucket and dual token bucket schemes can be described by means of the set of three values  $(r, b, p)$ .

**Fig. 2.45** Dual leaky bucket policer



### 2.2.7.5 Dual Leaky Bucket Policer

Dual Leaky Bucket (DLB) is a colloquial term to describe the a conformance algorithm to test a traffic flow. There are different variants of the DLB scheme; we consider here an example based on PCR, SCR, CDVT, MBS, and the time window  $T_w$  to control the average rate. DLB is described here as policer, but its algorithm could also be used in a shaper, where input cell buffering is allowed. The DLB policer determines whether the cells entering the network are conformant or not. Non-conformant cells are either dropped or marked, but not buffered. A DLB policer consists of two components, as shown in the conceptual scheme in Fig. 2.45:

- The first Leaky Bucket (LB1) controls that the cells are emitted up to a maximum speed, PCR. The bucket depth is set according to the CDVT value. When this buffer is empty, newly arriving cells (exceeding the PCR requirement) are lost; no cell marking is allowed in this case.
- The second Leaky Bucket (LB2) controls not to exceed the long-term mean cell rate SCR, measured on the interval  $T_w$ . Cells exceeding the SCR contract are marked with  $CLR = 1$ . MBS is controlled by the size of the second bucket.

DLB implements a GCRA algorithm of type #3, according to the characterization provided in Sect. 2.2.7.3. DLB and (dual) token bucket schemes are similar concepts and can have equivalent effects on the source traffic; sometimes these types of regulators are even confused.

### 2.2.7.6 Traffic Scheduling

Traffic scheduling is a fundamental function for ATM networks in order to share the physical transmission resources among competing flows with conflicting QoS requirements. Scheduling must guarantee to preserve some form of priority

among traffic classes. Typically, different transmission queues are needed to manage the different traffic classes at a multiplexer.

Different scheduling and priority schemes can be adopted [48]. For instance, a priority level and Weighted Fair Queuing (WFQ) can be used to define the service order of the queues and the service time for each of them. Note that the WFQ service discipline, known also as Packet-by-packet Generalized Processor Sharing (PGPS), is an approximation of the *ideal* Generalized Processor Sharing (GPS) scheme, where the available capacity is bit-by-bit divided among the active (fluid) flows of traffic, according to their different weights. Another interesting scheduling method is represented by the Earliest Deadline First (EDF) scheme; it is a form of a dynamic-priority scheduler, where the priority of each cell is assigned as it arrives. Specifically, a deadline is assigned to each cell on the basis of the delay guarantee associated with the flow to which the cell belongs. The EDF scheduler selects to service (i.e., to transmit on the link) the cell with the closest deadline.

### 2.2.7.7 Congestion Control by Means of Buffer Management

Buffer management is a type of preventive congestion control, which selects the cells to be discarded from a buffer in the attempt to prevent congestion. Overload situations are natural, since network operations are asynchronous: cells can compete for the same time slots on a link and therefore need to be buffered. Buffering on the other hand has to be limited, due to its cost and the impact on latency. A good ATM switch should achieve a certain trade-off between latency (buffer size) and cell loss rate. CAC and UPC cannot avoid congestion situations in the network. Hence, to manage overload situations, preventive control can be used to selectively discard cells from congested buffers. In particular, we consider the two following buffer management techniques, which protect high-priority cells ( $CLP = 0$ ) with respect to low-priority ones ( $CLP = 1$ ):

- In a *push-out mechanism*, all cells are allowed to enter the buffer if there are available resources. Let us now consider a cell arriving at a full buffer: if this cell has a low priority, it is discarded; instead, if this cell has a high priority, it is discarded only if there is no low-priority cell in the buffer, which can be discarded to make room for the new high-priority cell.
- The *threshold mechanism* allows all cells to enter the buffer as long as the number of waiting cells is lower than a given threshold. When the number of waiting cells exceeds such limit, newly arriving cells with low priority are discarded, instead high-priority cells are admitted as long as there is room available in the buffer.

Both schemes have similar performance. However, the threshold mechanism is preferred because it is simpler than the push-out one.

More refined schemes control the cells to be dropped rather than having them dropped at random. In situations where a higher-layer packet (ALL level) is segmented in cells, the drop of a single cell entails the need to resend the entire

higher-layer packet. In such circumstances, it is convenient to continue to drop the cells from the same packet in the presence of congestion. Two techniques can be considered:

- **Partial Packet Discard (PPD):** If a packet is damaged (due to the loss of a cell), the remaining cells from the same packet can be discarded.
- **Early Packet Discard (EPD):** If a BOM cell arrives and the buffer occupancy is above a certain threshold, all the cells of the same packet are discarded beforehand.

### 2.2.7.8 Reactive Schemes for Congestion Control

A reactive scheme can be used to manage congestion events: a congested network node may set the EFCI flag in the cell header so that this indication can be notified to the destination (forward congestion notification). Hence, the end system can use this indication for a protocol, which signals to the source to adaptively reduce the traffic injection into the network. This reactive scheme is supported only by the ABR traffic class in ATM.

It is also possible that the congestion notification be sent directly to the source by a congested intermediate node; this is a backward congestion notification scheme. Both forward and backward schemes suffer from network-wide delays in reacting to congestion events.

### 2.2.8 ATM Physical Layer

ITU, ANSI and ATM Forum have specified the ATM physical layer. Details are provided below, mainly referring to ITU and ANSI definitions. In particular, two different modalities are available for the transmission of cells on the physical medium, according to ITU-T I.432 Recommendation [49]. Referring to the User-to-Network Interface (UNI, either public or private), we have:

- *Sequence of cells:* The transmission of cells is carried out directly on the physical medium without using a specific frame structure. A continuous stream of cells is sent. Periodical insertion of OAM cells is needed. This solution may be adopted for private UNI.
- *SDH or SONET:* ATM traffic streams are multiplexed in complex transmission structures, where each stream is identified by a pointer. More details on these transmission structures are provided below.

ITU-T Recommendations I.432.1, I.432.2, I.432.3, I.432.4, I.432.5 specify the physical layer characteristics at ATM UNI interfaces, considering the following bit-rates [49]: 155.52 and 622.08 Mbit/s (I.432.2), 1.544 and 2.048 Mbit/s (I.432.3), 51.84 (I.432.4) and 25.6 Mbit/s (I.432.5).

**Table 2.5** ATM physical layer for public UNI

Frame format	Bit-rate (Mbit/s)	Media
DS1	1.544	Twisted pair
DS3	44.736	Coaxial pair
STS-3c, STM-1	155.520	Single-mode fiber
E1	2.048	Twisted pair
E3	34.368	Coaxial pair
J2	6.312	Coaxial pair
$N \times T1$	$N \times 1.544$	Twisted pair, coaxial pair

**Table 2.6** ATM physical layer for private UNI

Frame format	Bit-rate (Mbit/s)	Media
Cell stream	25.6	UTP-3 (phone wire) or STP
STS-1	51.84	UTP-3 (phone wire)
FDDI	100	Multimode fiber
STS-3c, STM-1	155.52	UTP-5 (data grade UTP)
STS-3c, STM-1	155.52	Single-mode fiber, multimode fiber, coaxial pair
Cell stream	155.52	Multimode fiber, STP
STS-3c, STM-1	155.52	UTP-3 (phone wire)
STS-12, STM-4	622.08	Single-mode fiber, multimode fiber

Different physical layers can be used for ATM networks. Correspondingly, different media are available, such as single-mode or multimode optical fiber, shielded or unshielded twisted-pair (STP, UTP), and coaxial cable. Details on the physical layers and media are provided in Tables 2.5 and 2.6, respectively for public and private UNI. For instance, the access capacity of 155.52 Mbit/s can be achieved by both the cell sequence approach (private UNI) and the SDH/SONET one (public and private UNI). The transmission bit-rates shown in Tables 2.5 and 2.6 are related to maximum distances, depending on the adopted medium.

Category 3 UTP (UTP-3, phone wire) is adopted for residential ATM access in order to take advantage of existing building wiring. 51.84 Mbit/s over UTP-3 cabling as well as 25.6 Mbit/s over UTP-3 or STP is possible for a maximum distance of approximately 100 m. In case of 155.52 and 622.08 Mbit/s transmissions, the maximum distance becomes approximately 2 km with an optical fiber and approximately 200 m with a coaxial cable.

### 2.2.8.1 SDH/SONET

In 1985, Bellcore began working on a standard, called Synchronous Optical Network (SONET) for long-distance optical fiber connections. Later, CCITT (now ITU-T) joined this effort. The main problem encountered was to find a compromise between American, European, and Japanese interests in order to guarantee the



interconnection of different systems. The result was the SONET standard published by the American National Standards Institute (ANSI) [50] and the Synchronous Digital Hierarchy (SDH) standard [51] defined in ITU-T G.707, G.708, and G.709 Recommendations [52–54]. SONET and SDH *transport technologies* are not directly related to ATM, but can be used to transport ATM cells. There are slight differences in the frame format between SONET and SDH. SDH is used in Europe and SONET is used in USA and Japan.

Synchronous Transfer Signal (STS) denotes the electrical specifications of the various levels of the SONET hierarchy. Synchronous Transfer Mode (STM) is the analogous term for the SDH hierarchy. In SDH/SONET, data transmission is organized in frames<sup>9</sup> of 125  $\mu$ s. The base signal for SONET is STS-1 and the base signal for SDH is STM-1.

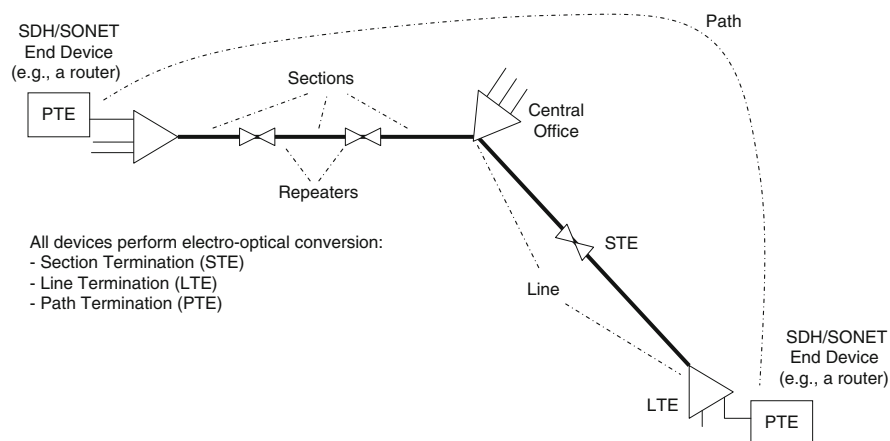
SDH and SONET allow direct synchronous multiplexing: several lower-bit-rate signals can be directly multiplexed onto a higher speed SDH or SONET signal without intermediate stages of multiplexing. A single multiplexed signal is called *tributary* or *container* respectively for SONET and SDH.

Before SDH and SONET, the digital transmission hierarchy was based on the PDH technology, as already introduced in Chap. 1. When a PDH multiplexer is trying to multiplex different signals onto one data stream, it has to consider that the clocks of all incoming tributaries are not perfectly synchronized: the rise and fall times of pulses are not coincident in the tributaries. A PDH multiplexer reads data from all the incoming streams at the maximum allowed speed according to a cyclic process. It may happen that when the multiplexer services a stream, the bit of this stream have not yet arrived, because this stream has a slower clock; then, the multiplexer stuffs the data stream with “dummy bits” (or “justification bits”). This process is known as “plesiochronous operation” (from the Greek, “almost synchronous”). The multiplexer has a means of notifying the receiving end that stuffing has taken place so that extra bits can be discarded when demultiplexing the flows. The problem with PDH multiplexing is that a lower-level data stream is extracted from a higher-order one only if the demultiplexer performs all the operations made by the multiplexer that created the higher-level flow. As a result, all the flows need to be demultiplexed. This operation is called Add/Drop; it is a complex task and the related equipment is quite expensive.

Differently from PDH, SDH/SONET transport networks are tightly synchronized: atomic clocks are used to synchronize the clocks of the networks. The reality is that a perfect synchronization is practically impossible in large-scale geographical networks: temperature variations and different cable lengths always cause a residual drift in the clocks of tributaries. This is the reason why SDH/SONET adopts a new approach for multiplexing tributary signals in a higher-order one: pointers are used to individuate tributaries in the payload. Hence, it is possible to manage tributaries not running at the same clock rate and/or not aligned with the clock of the multiplexer. In particular, SDH/SONET adopts a pointer, describing

---

<sup>9</sup> PDH, SDH, and SONET are all based on 64 kbit/s digital voice channels of the PCM type.



**Fig. 2.46** Optical link

the start of a tributary flow in the STS/STM frame payload. Hence, it is not necessary for the multiplexer to get the tributary signals in synchronism or to stuff the frame with bits. If a tributary signal clock slips over time with respect to the multiplexer clock, the SDH/SONET multiplexer simply recalculates the pointer for each new frame. Each byte of the tributary signal, and thus, the tributary signal itself, is visible in the frame. Hence, it is possible to extract a single tributary signal out of the main signal, not needing to demultiplex all the flows as with PDH.

The structure of optical links (distinguishing *section*, *line*, and *path*) is described in Fig. 2.46.

The STS-1 frame is composed of bytes according to a matrix with 9 rows and 90 columns (see Fig. 2.47); totally, there are 810 bytes in a frame. In this  $90 \times 9$ -byte structure, one byte transmitted every  $125 \mu\text{s}$  (frame duration) corresponds to a 64 kbit/s channel. Since there are  $90 \times 9$  bytes transmitted every  $125 \mu\text{s}$ , the corresponding bit-rate is 51.84 Mbit/s. The bytes of the matrix are sent from top row and moving from left to right. The first three columns are used by Section OverHead (SOH) and by Line OverHead (LOH); they both form the so-called Transport OverHead (TOH). The data payload uses the remaining 87 columns, where a column is used for Path OverHead (POH). A pointer in TOH identifies the beginning of the payload, called Synchronous Payload Envelope (SPE). SOH contains information required for section-to-section communication (i.e., repeater-to-repeater communication) and, in particular, framing, performance monitoring, and a voice channel for maintenance personnel. LOH contains information required for line termination equipment communication, such as an Add/Drop terminal; it also contains the payload pointer, OAM data, line performance monitoring, and a voice channel for maintenance personnel.

SPE contains the actual information being transmitted and POH supports end-to-end monitoring of the payload. SPE can have a phase shift with respect to the

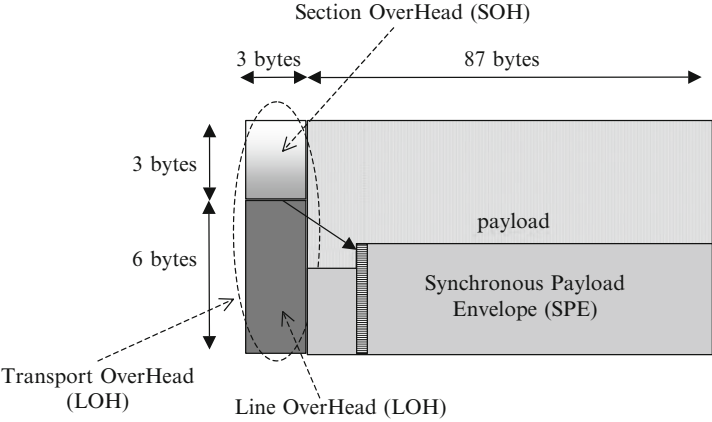


Fig. 2.47 STS-1 frame structure

Table 2.7 Hierarchy of the most common SDH/SONET data rates

Optical level	Electrical level	Line rate (Mbit/s)	Payload rate (Mbit/s)	Overhead rate (Mbit/s)	SDH equivalent
OC-1	STS-1	51.840	50.112	1.728	–
OC-3	STS-3	155.520	150.336	5.184	STM-1
OC-12	STS-12	622.080	601.344	20.736	STM-4
OC-48	STS-48	2,488.320	2,405.376	82.944	STM-16
OC-192	STS-192	9,953.280	9,621.504	331.776	STM-64
OC-768	STS-768	39,813.120	38,486.016	1,327.104	STM-256

beginning of the STS-1 frame. Moreover, SPE may float inside the STS-1 frame in case the clock used to generate the payload is not synchronized with the clock used to generate the frame. TOH is valid only on a link-by-link basis (no end-to-end significance). POH is processed only by the equipment terminating the SONET signal.

The hierarchy of the most common SDH/SONET transmissions is shown in Table 2.7 that also highlights the correspondences between SONET STS signals and SDH STM ones. For instance, STS-3 is equivalent to STM-1. Note that OC-*n* specifies the optical fiber transmissions corresponding to STS-*n* SONET.<sup>10</sup> Different OC-*n* signals can be multiplexed onto the same optical fiber by means of the Dense Wave Division Multiplexing (DWDM) technology.

<sup>10</sup> We refer to cases where the entire OC bandwidth is used for a single channel (instead of the cases where there are multiple channels in the OC bandwidth). Hence, in our study, we should add the letter “c” at the end of “OC-*n*” (i.e., OC-*nc*); such letter has been omitted here for the sake of simplicity.

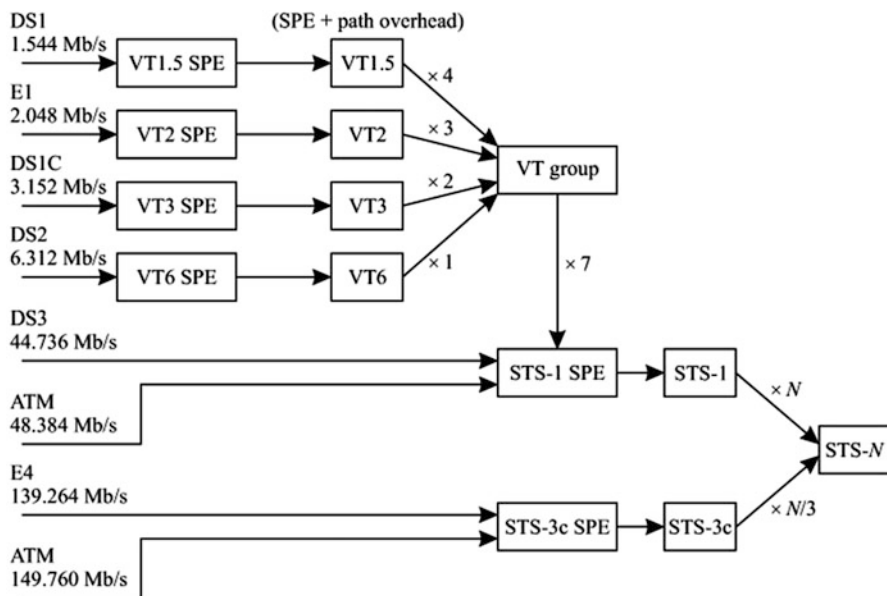


Fig. 2.48 Tributary hierarchy in SONET

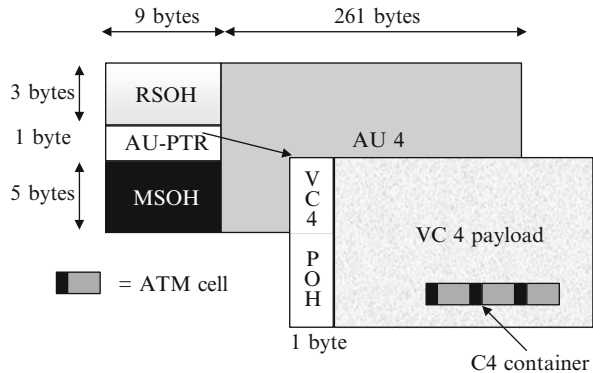
It should be noticed that the difference between the various STS- $n$  frames is due to the frame width. The frames are always composed of 9 rows, but the number of columns (the “width”) changes, depending on the  $n$  value (i.e.,  $n \times 90$  columns).

In SONET, different lower-bit-rate flows can be multiplexed into an STS- $n$  frame; they are called (virtual) tributaries. Multiplexing is carried out according to a hierarchy, as shown in Fig. 2.48. For instance, the North American DS1 rate of 1.544 Mb/s is transported by means of Virtual Tributary 1.5 (VT 1.5). A Virtual Tributary Group can carry 4 DS1 signals (i.e., 4 VT 1.5 s). Since an STS-1 can carry 7 Virtual Tributary Groups, it can support  $7 \times 4 = 28$  DS1 signals.

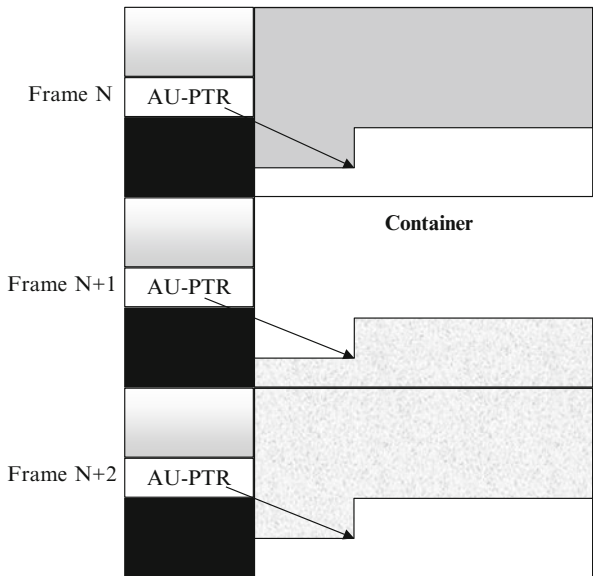
STM-1 operates at 155.520 Mbit/s, thus having the possibility to carry 3 interleaved STS-1 frames. The STM-1 frame has 9 rows and  $3 \times 90$  columns:  $3 \times 3$  columns are used by overhead (collectively named Section Overhead, SOH in the SDH case) and the other 261 columns belong to the payload (i.e., one Virtual Container-4, VC-4, or three VC-3s). The 9 SOH columns are distinguished in Regenerator Section Overhead (RSOH), AU-pointer (AU-PTR), and Multiplex Section Overhead (MSOH). RSOH and MSOH convey control information. In the STS-1 payload, one column is used for the Path Overhead (POH), so that we can consider that STM-1 is characterized by a total overhead of 10 columns (out of 270 columns). Thus, the actual useful information rate carried by the STM-1 payload is 149.76 Mbit/s.

The STM-1 payload (excluding the 9 bytes of POH) contains  $9 \times 260 = 2,340$  bytes. Since, the ATM cell length of 53 bytes is not a multiple of 2,340 bytes, ATM cells arriving at a fixed rate do not have a fixed position in the VC-4 container.

**Fig. 2.49** STM-1 internal structure with pointers and containers



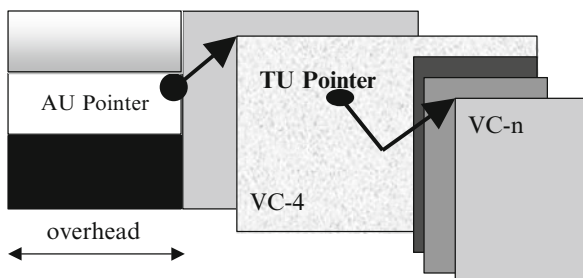
**Fig. 2.50** Use of the pointer in STM-1 for a container (e.g., the whole VC 4) not aligned with the payload. Note that different subsequent frames are stacked to highlight the shift of the position of the same container from one frame to another



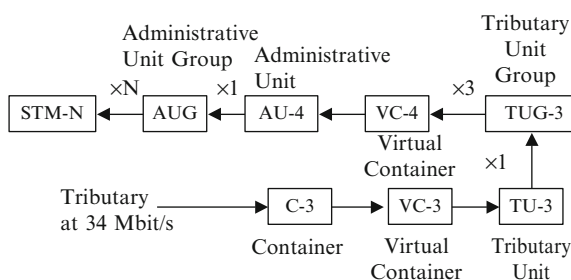
Moreover, VC-4 may fluctuate in the payload. Since the position of each octet in the STM has a number, the AU-PTR pointer (having a fixed position in SOH) specifies the number of the first VC-4 byte, that is the first byte of the associated POH. Cells are identified within VC-4 by means of the correlation present in the ATM cell header due to the HEC field. Figures 2.49 and 2.50 describe the use of the pointer. In particular, Fig. 2.50 shows the use of the pointer in a case where there is a phase shift of VC-4 with respect to the payload.

Referring to Fig. 2.51, the STM-1 payload may contain different layers of “information blocks”, called Virtual Containers (VCs), each of them addressed by a pointer and having a header, named POH. A lower-order VC plus the corresponding header form a Tributary Unit (TU); a higher-order VC plus its corresponding header form an Administrative Unit (AU). There is a complex

**Fig. 2.51** SDH:  
organization of multiplexed  
tributaries



**Fig. 2.52** Example of SDH  
multiplexing, starting from  
a low-bit-rate tributary at  
(about) 34 Mbit/s



organization according to which tributaries from the existing PDH hierarchy (e.g., from 1.544 to 2.048, and to 139.264 Mbit/s) can be multiplexed in the STM-1 payload. ITU-T G.709 Recommendation specifies the different combinations of virtual containers, which can be used to fill in the STM-1 payload. A detailed example of the SDH multiplexing hierarchy is provided in Fig. 2.52. By means of pointers used at two levels it is possible to compensate for phase or frequency differences between different VCs in the same STM, and between VC and STM.

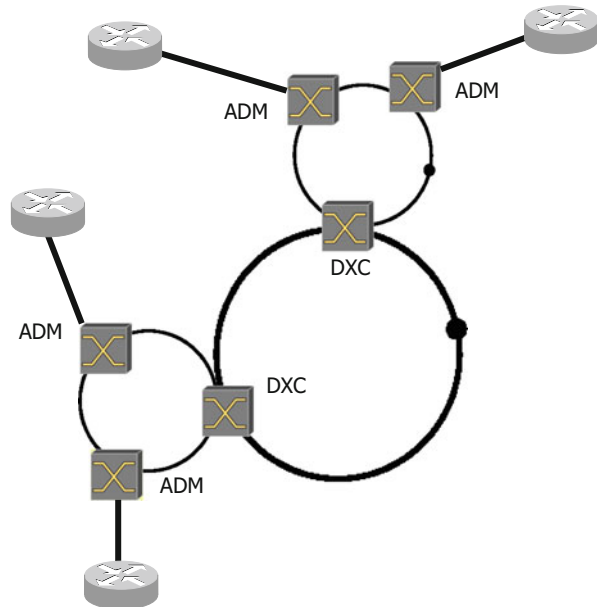
The SDH technologies most commonly used today are STM-1, STM-4, and STM-16.

There are three fundamental operations, which can be performed on an SDH/SONET signal: multiplexing, add/drop multiplexer, and cross-connect (see Fig. 2.53).

- An SDH/SONET multiplexer may manage a variety of input signals (T1, T3, etc.) and other signals and may combine them into a single higher-bit-rate output.
- An Add/Drop Multiplexer (ADM) has a high-bandwidth input and a high bandwidth output at the same bit-rate, and is able to extract (drop) some lower-rate channels out of the SDH/SONET stream and to add simultaneously some lower-rate channels into that stream.
- Perhaps the most powerful SDH/SONET device is the Digital Cross Connect (DXC). A DXC contains a number of input and output ports, which may operate at several bit-rates. The DXC is able to extract any of the input tributaries and to insert them into any of the high bit-rate output ports.

SDH transport networks have defined two lower layers (i.e., path layer and transmission media layer); more details are beyond the scope of this book.

**Fig. 2.53** Example of SDH/SONET ring network topology



### 2.2.8.2 ATM Signaling

ATM signaling protocols vary depending on the type of ATM link:

- ATM UNI signaling is used between an ATM end system and an ATM switch across an ATM UNI.
- ATM NNI signaling is used across NNI links.

Signaling messages are transmitted in a connectionless way, without any requirement for end-to-end synchronization (service class D). They are broken down into ATM cells via AAL 5 and sent by means of Signaling Virtual Channels (SVCs). All signaling is carried out by the connection with VPI = 0 and VCI = 5.

The ATM signaling at UNI (also defined by ATM Forum UNI specifications) is based on ITU-T Q.2931 Recommendation [55], which, in turn, is based upon the Q.931 signaling protocol of ISDN [26]. The ATM signaling protocols run on top of a Service Specific CONvergence Protocol (SSCOP), defined by ITU-T Q.2110 and Q.2130 Recommendations [56, 57]. This is a data link protocol, which guarantees a reliable delivery through the use of windows and retransmissions.

ATM signaling adopts the one-pass method for connection setup, a typical choice in connection-oriented networks. In particular, a connection request is propagated from the source end system through the network, setting up the connection as it goes, until it reaches the destination end system. The routing of the connection request (and hence of any subsequent data flow) is governed by ATM routing protocols. These protocols route the request on the basis of both the

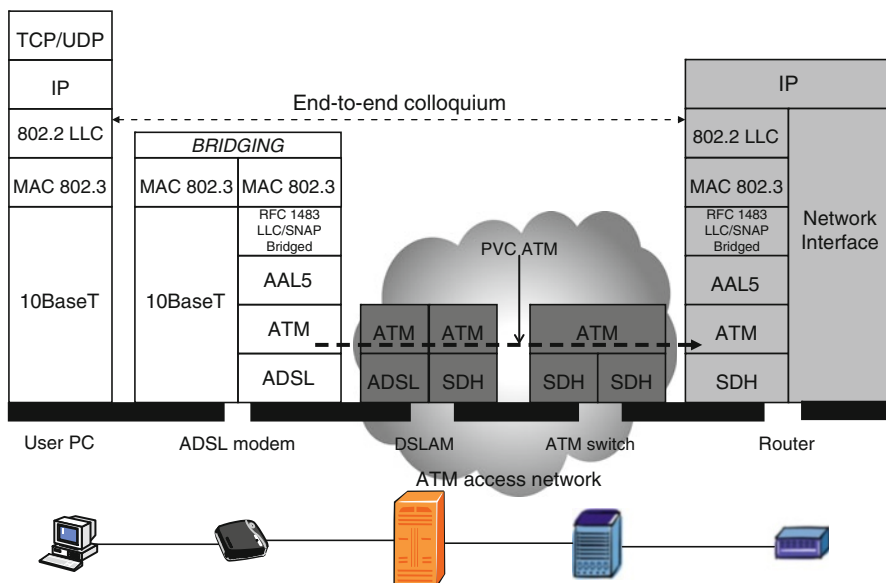


Fig. 2.54 ADSL access to the Internet

destination address and the QoS parameters requested by the source. The destination may choose to accept or reject the connection request.

There are three types of SVCs:

- Meta-Signaling Virtual Channels (MSVC)—one per interface—are bidirectional, 64 kbit/s, permanent signaling channels, which can be connected or disconnected as required.
- Point-to-point Signaling Virtual Channels (PSVC) are bidirectional and are used to connect, monitor, and then disconnect virtual user connections.
- Broadcast Signaling Virtual Channels (BSVC) are unidirectional from the network to the users.

### 2.2.9 Internet Access Through ATM Over ADSL

The ADSL transmissions described in Sect. 1.6.1 can be used to allow a high-speed access to the Internet. The user from his/her home adopts an appropriate modem to transmit the ADSL signal on the twisted pair to the local office; here, a DSL Access Multiplexer (DSLAM) terminates the DSL session and sends the traffic in the ATM network. Using permanent virtual circuits, the ATM network forwards the traffic up to the first router to access the Internet. The network topology and the protocol stack of the ADSL access to the Internet is described in Fig. 2.54.



## References

1. Stallings W (2003) Data and computer communications. Prentice Hall, Upper Saddle River, NJ
2. ITU-T. Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit. Recommendation X.25, October 1996
3. Helgert HJ (1991) Integrated services digital networks: architecture, protocols, standards. Addison-Wesley, New York
4. Stallings W (1992) Advances in ISDN and broadband ISDN. IEEE Computer Society Press, Los Alamitos, CA
5. Stallings W (1995) ISDN and broadband ISDN with frame relay and ATM. Prentice-Hall, Upper Saddle River, NJ
6. de Prycker M (1991) Asynchronous transfer mode: solution for broadband ISDN. Ellis Horwood, Chichester
7. Onvural RO (1994) Asynchronous transfer mode networks: performance issues. Artech House, Inc., Norwood, MA
8. Karim MR (1999) ATM technology and services delivery. Prentice-Hall, Upper Saddle River, NJ
9. ITU-T. Packet-switched signalling system between public networks providing data transmission services. Recommendation X.75, October 1996
10. ITU-T. Interface between data terminal equipment and data circuit-terminating equipment for synchronous operation on public data networks. Recommendation X.21, September 1992
11. ITU-T. List of definitions for interchange circuits between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) on public data networks. Recommendation X.24, November 1988
12. ITU-T. Electrical characteristics for balanced double-current interchange circuits operating at data signalling rates up to 10 Mbit/s. Recommendation X.27, October 1996
13. ITU-T. International numbering plan for public data networks. Recommendation X.121, October 2000
14. ITU-T. Packet assembly/disassembly facility (PAD) in a public data network. Recommendation X.3, November 1988
15. ITU-T. DTE/DCE interface for a start-stop mode data terminal equipment accessing the packet assembly/disassembly facility (PAD) in a public data network situated in the same country. Recommendation X.28, December 1997
16. ITU-T. Procedures for the exchange of control information and user data between a Packet Assembly/Disassembly (PAD) facility and a packet mode DTE or another PAD. Recommendation X.29, December 1997
17. ITU-T. ISDN user-network interfaces – interface structures and access capabilities. Recommendation I.412, November 1988
18. ITU-T. Basic user-network interface – layer 1 specification. Recommendation I.430, November 1995
19. ITU-T. Primary rate user-network interface – layer 1 specification. Recommendation I.431, March 1993
20. ITU-T. Principles of telecommunication services supported by an ISDN and the means to describe them. Recommendation I.210, November 1988
21. ITU-T. ISDN protocol reference model. Recommendation I.320, November 1993
22. ITU-T. Physical/electrical characteristics of hierarchical digital interfaces. Recommendation G.703, November 2001
23. ITU-T. Synchronous frame structures used at primary and secondary hierarchical levels. Recommendation G.704, October 1998
24. ITU-T. Digital subscriber Signalling System No.1 (DSS1) – ISDN user-network interface data link layer – General aspects. Recommendation Q.920, March 1993

25. ITU-T. ISDN user-network interface – data link layer specification. Recommendation Q.921, September 1997
26. ITU-T. Digital subscriber Signalling System No. 1 (DSS 1) – ISDN user-network interface layer 3 specification for basic call control. Recommendation Q.931, May 1998
27. ANSI. Frame relaying bearer service. Recommendation T1.606, 1991
28. ANSI. ISDN – signaling specification for digital subscriber signaling system number 1 (DSS1). Recommendation T1.617 [It is equivalent to ITU-T Q.933 Recommendation], 1991
29. ANSI. Core aspects of frame protocol for use with frame relay bearer service. Recommendation T1.618, 1991
30. ITU-T. Frame mode bearer services. Recommendation I.233 [It deals with Frame Relay and Frame Switching], October 1991
31. ITU-T. ISDN data link layer specification for frame mode bearer services. Recommendation Q.922 [This recommendation describes the LAPF protocol; Annex A is on frame relay], February 1992
32. ITU-T. ISDN Digital subscriber Signalling System No. 1 (DSS 1) – signalling specification for frame mode basic call control. Recommendation Q.933 [This recommendation deals with user-to-network signaling for Frame Relay services; it is based on Q.931, which deals with circuit/packet switched services], March 1993
33. Frame Relay Forum (1996) User to network implementations agreement. FRF.1.1
34. Frame Relay Forum (1995) Multiprotocol encapsulation implementation agreement. FRF.3.1
35. ITU-T. (1991) Congestion management for the ISDN framerelaying bearer service. Recommendation I.370
36. ITU-T. (1992) B-ISDN asynchronous transfer mode functional characteristics functional characteristics. Recommendation I.150
37. Hemrick C, Lang L (1990) Introduction to switched multi-megabit data service (SMDS), an early broadband service. Proceedings of the XIII international switching symposium (ISS 90), May 27–June 1, 1990
38. Pandya AS, Sen E (1998) ATM technology for broadband telecomm networks. CRC Press, Boca Raton, FL
39. Arpaci M, Copeland JA (2000) Buffer management for shared-memory ATM switches. IEEE Commun Surv Tutor 3(1):2–10
40. Guérin R, Ahmadi H, Naghshineh M (1991) Equivalent capacity and its application to bandwidth allocation in high-speed networks. IEEE J Sel Area Comm 9:968–981
41. Elwalid A, Mitra D (1993) Effective bandwidth of general Markovian traffic sources and admission control of high speed networks. IEEE/ACM T Network 1:329–343
42. Kesidis G (1994) Modeling to obtain the effective bandwidth of a traffic source in an ATM network. MASCOTS, Los Alamitos, CA, pp. 318–322
43. Chang C-S, Thomas J (1995) Effective bandwidth in high speed digital networks. IEEE J Sel Area Comm 13:1091–1100
44. Gibbens RJ, Hunt PJ (1991) Effective bandwidths for the multi-type UAS channel. Queueing Syst 9:17–28
45. ITU-T (1994) Traffic control and congestion control in B-ISDN. Recommendation I.371
46. ATM Forum (1999) Traffic management specification. Version 4.1. AF-TM-0121.000. <ftp://ftp.atmforum.com/pub/approved-specs/af-tm-0121.000.pdf>
47. ITU-T (1993) B-ISDN ATM layer cell transfer performance. Recommendation I.356
48. Guérin R, Peris V (1999) Quality-of-service in packet networks: basic mechanisms and directions. Comput Network 31:169–189
49. ITU-T (1993) B-ISDN user-network interface – physical layer specification. Recommendations of the I.432 series (I.432.1, I.432.2, I.432.3, I.432.4, I.432.5)
50. ANSI. SONET – basic description including multiplex structure, rates and formats. T1.105, 2001
51. The ATM Forum (1993/1994) ATM user-network interface specifications 3.0 and 3.1. Prentice-Hall, Upper Saddle River, NJ

52. ITU-T. Network node interface for the synchronous digital hierarchy (SDH). Recommendation G.707, January 2007
53. ITU-T. Sub STM-0 network node interface for the synchronous digital hierarchy (SDH). Recommendation G.708, April 1991
54. ITU-T. Interfaces for the optical transport network (OTN). Recommendation G.709, February 2012
55. ITU-T. B-ISDN DSS2 UNI Layer 3 Specification for basic call/connection control. Recommendation Q.2931, February 1995
56. ITU-T. B-ISDN AAL – service specific connection oriented protocol (SSCOP). Recommendation Q.2110, July 1994
57. ITU-T. B-ISDN signalling ATM adaptation layer – service specific coordination function for support of signalling at the user-network interface (SSCF at UNI). Recommendation Q.2130, July 1994

<http://www.springer.com/978-1-4614-4083-3>

Queuing Theory and Telecommunications  
Networks and Applications

Giambene, G.

2014, XXI, 516 p. 268 illus., 32 illus. in color., Hardcover

ISBN: 978-1-4614-4083-3