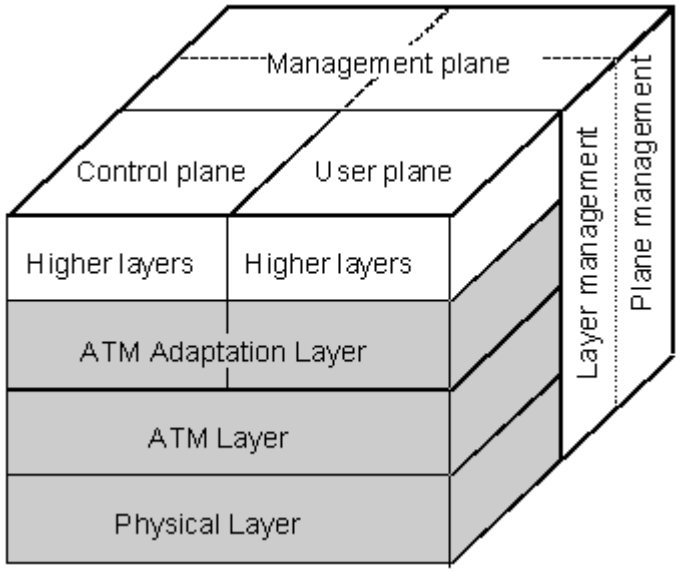
4.2.4 ATM = Asynchronous Transfer Mode

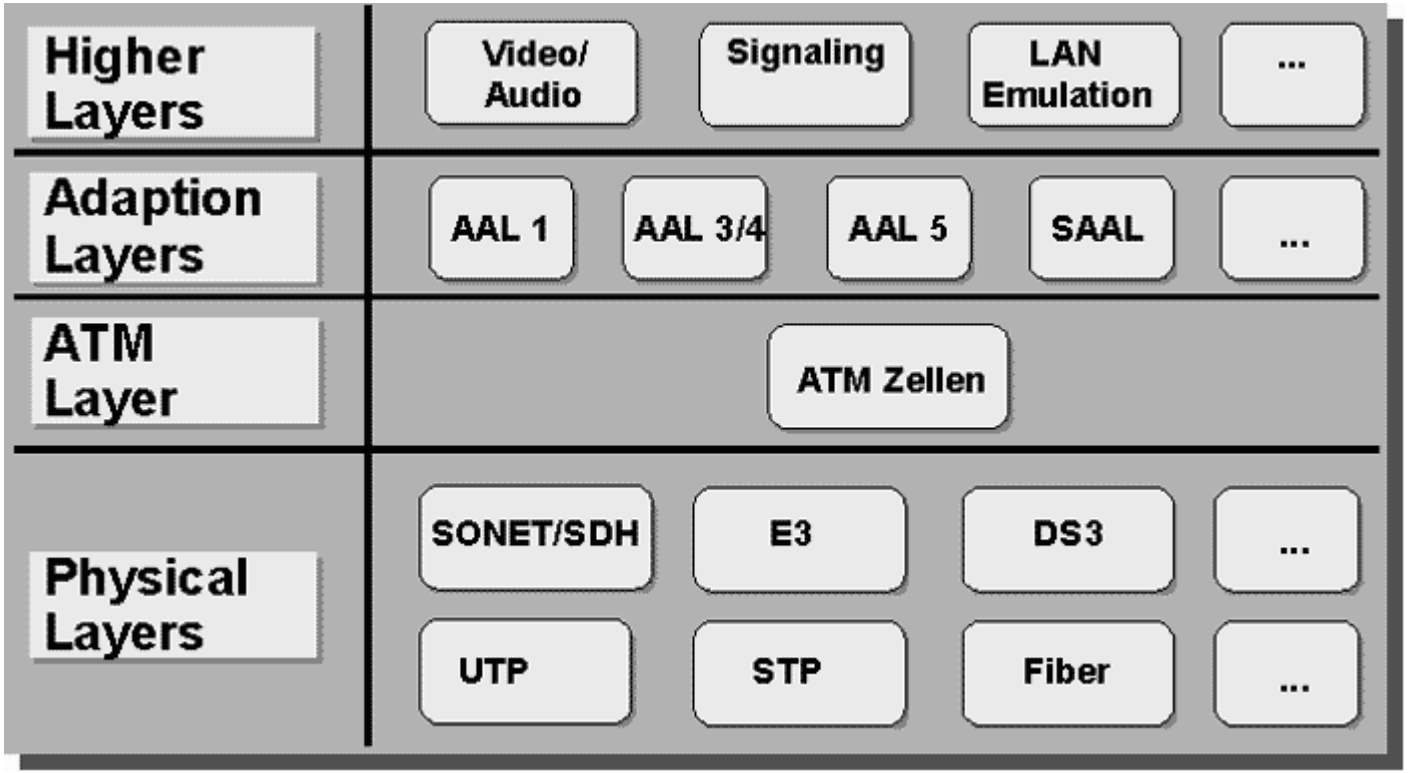
Reference Model



- **According to ITU-T Recommendation I.113 asynchronous means:**
  " ... it is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic." (I113)
- Higher layer provide end-to-end services
- ATM Adaption Layer (AAL):
  - adaption of service data to cells (48 bytes)
- 53 byte cells handled by ATM Layer:
  - 5 byte header (VPI, VCI, HEC)
  - switching/multiplexing of cells

ATM Layer Overview

- Examples:

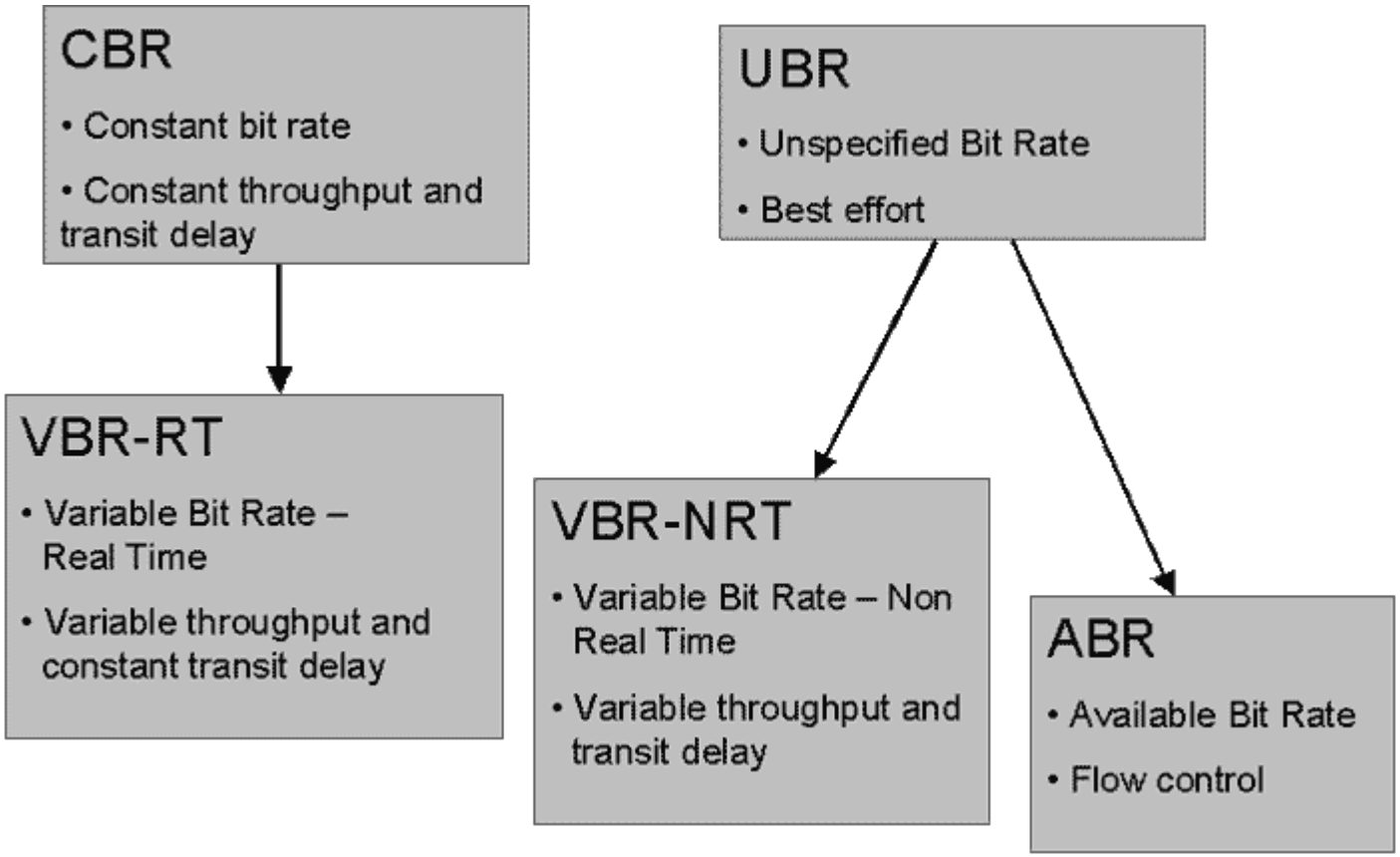


ATM: Traffic Contract

- **No error detection and correction, but ...**
  ... mechanisms to guarantee Quality of Service

The Application	The ATM Network
at the connection set-up	
• specifies its needs in Quality of Service : Type of Traffic, Bit-Rate, Transit Delay, etc	• checks the resources • reserves the bandwidth (CAC) • commits to provide the service
during the communication	
• regulates its traffic according to the contract	• controls if the application abides the contract (UPC)

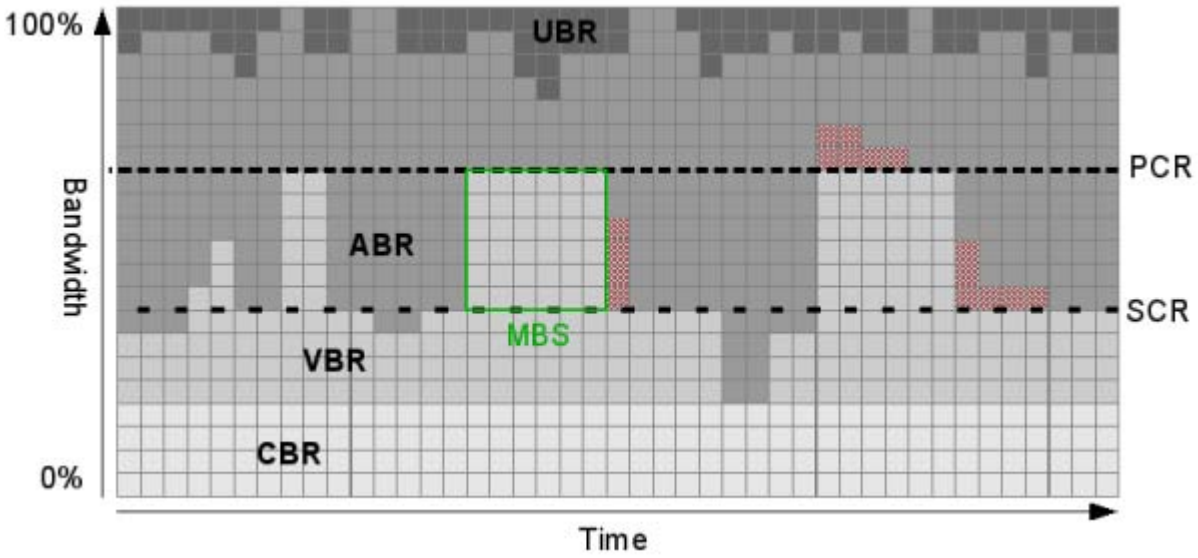
ATM: Service Categories 1



ATM: Service Categories 2

Distribution of bandwidth

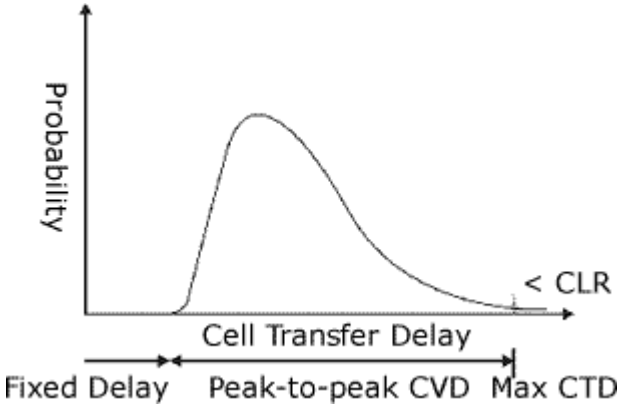
- CBR: constant bit rate
- VBR: variable bit rate, i.e. constant bandwidth up to SCR for a short time (max. burst size) more bandwidth usage up to PCR is possible
- ABR: available bit rate, i.e. network provides feedback of bandwidth available
- UBR: unspecified bit rate, i.e. best-effort



SCR = sustainable cell rate, PCR = peak cell rate, MBS = maximum burst size
duration of a burst: (MBS-1)/PCR; time between two bursts: MBS/SCR

Quality of Service Parameter

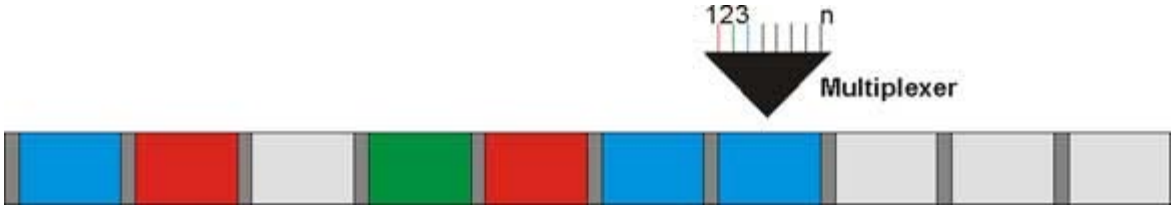
QoS Acronym	Parameter Name	Negotiated?
peak-to-peak	Cell Delay Variation	YES
maxCTD	max. Cell Transfer Delay	YES
CLR	Cell Loss Ratio	YES
CER	Cell Error Ratio	NO
SECBR	Severely Errored Cell Block Ratio	NO
CMR	Cell Misinsertion Rate	NO



→ Probability for exceeding maxCTD must be less than CLR

ATM: Network Access

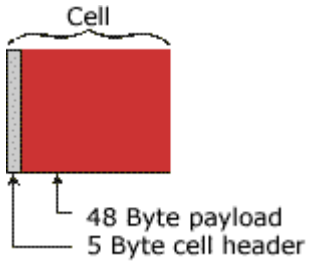
- **ATM = "Asynchronous Transfer Mode" because the "Asynchronous Time Division Multiplexing" (ATDM) is used**

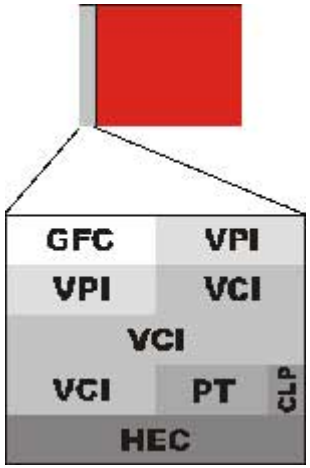


- STDM uses slots; ATDM uses cells
- The sequence of the cells on a link is not fixed (asynchronous)
  - A sender defines a useful sequence
  - Enables arbitrary bandwidth for each connection
  - High efficiency because no empty cells must be sent if no data is available
- Reservation of bandwidth can be handled by the cell multiplexer
- Each cell has a header identifying the connection a cell belongs to

ATM: Cells

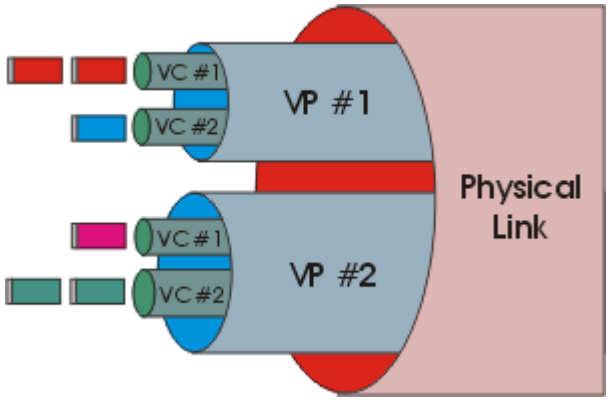
- **Cells are packets of a constant size**
  - Simplifies scheduling of the multiplexer
- **Small size enables low delay even on low bandwidth links**
- **Overhead of cell header ~9,43%**
- **Cell header**
  - Basically: identifier of the connection
    - VPI = Virtual Path Identifier
    - VCI = Virtual Channel Identifier
  - Payload type
    - Label data or management information
  - Cell loss priority
    - In case of congestion drop cells with CLP=1 first
  - Header Error Control – CRC for the first 4 header bytes





ATM: Virtual Path/Circuit

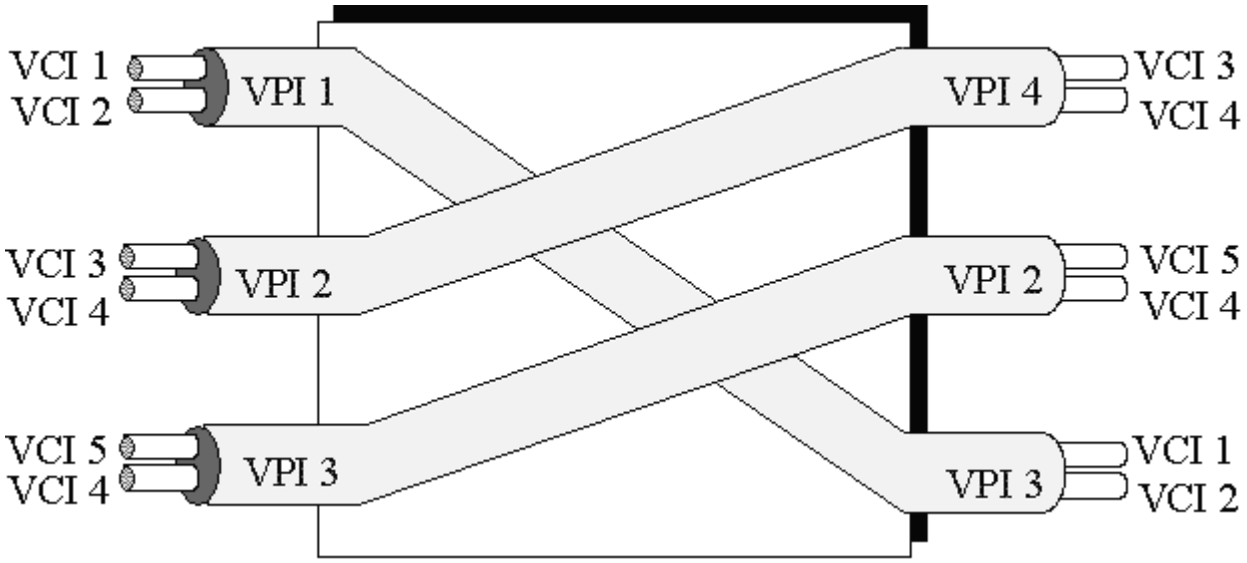
- **ATM is connection oriented**
  - Virtual paths (VP) build a logical topology on top of the physical topology
  - Virtual Circuits Channels(VC) are connections on virtual paths
- **Links:**
  - Physical link: connects two physical devices
  - Virtual Circuit Channel: connects two end-systems
  - Virtual Path: link <= path <= circuit
- **Connections may be**
  - point-to-point (full-duplex)
  - point-to-multipoint (half-duplex)
- **VPs are static**
  = permanent virtual path (PVP)
- **VCs may be static or dynamic**
  = permanent or switched virtual channel (PVC/SVC)



ATM: Characteristics of VC/VP

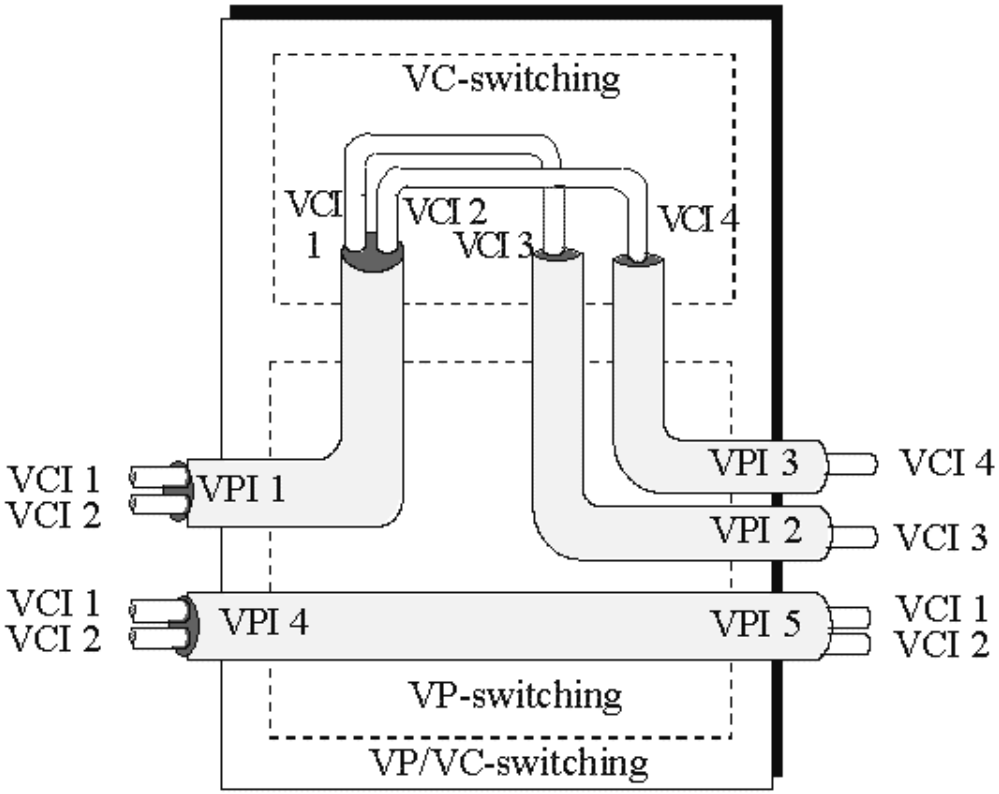
- **Logical association between the endpoints of a link (individual link)**
- **Virtual Channel Characteristics:**
  - Bi-directional data transfer
  - Guaranteed sequential delivery
  - Error detection by HEC and correction of single bit errors
  - QoS characteristic associated with each virtual channel connection and with each direction of a channel
- **Virtual Path Characteristics :**
  - Route through a network
  - Carries various VCs
  - VP also has a QoS (the limit for all VCs)

ATM: Path switching



- Switching with regard to VPI only
- VCI are left unchanged

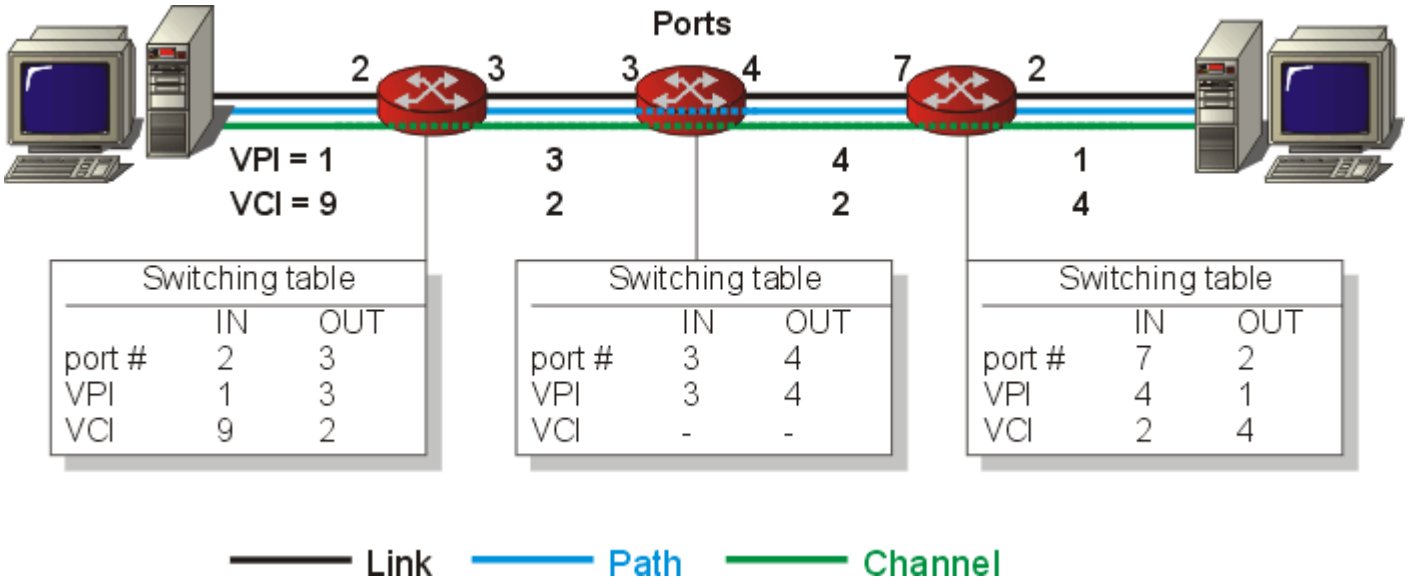
ATM: Circuit Switching



Switching with regard to VPI and VCI

- If the VCI is used for switching, this means the VP ends at that switch
- VCs of one path could be spread over several new paths

ATM: Switching Table



ATM: Usability for Multimedia Data

- **QoS parameters:**
  - guaranteed bandwidth (fixed, variable, feedback)
  - low delay and low delay variation (not guaranteed)
- **Isochronism:**
  - is available
- **Multicast capability:**
  - uni-directional point-to-multipoint is available
- **Flexibility:**
  - bandwidth on demand, limited by physical links and actual system load
  - several traffic types CBR, RT-VBR, NRT-VBR, ABR and UBR
  - independent of physical media
  - mainly used for WAN or in LAN for backbones,
    ATM to the desktop was available but was too expensive to be accepted widely
- **Efficiency:**
  - high bandwidth utilization
  - statistical multiplexing increases utilization, VBR channels:
    - SUM of "sustained cell rates" must be <= 100%
    - SUM of "peak cell rates" may be > 100%
- **Costs:** a complex and therefore an expensive technology

4.2.5. Evolution of Internet Access Technologies

- Success of multimedia systems requires for many services a broadband Internet connection.
- Economic requirement: Connect consumers cost-effectively -- at home and mobile

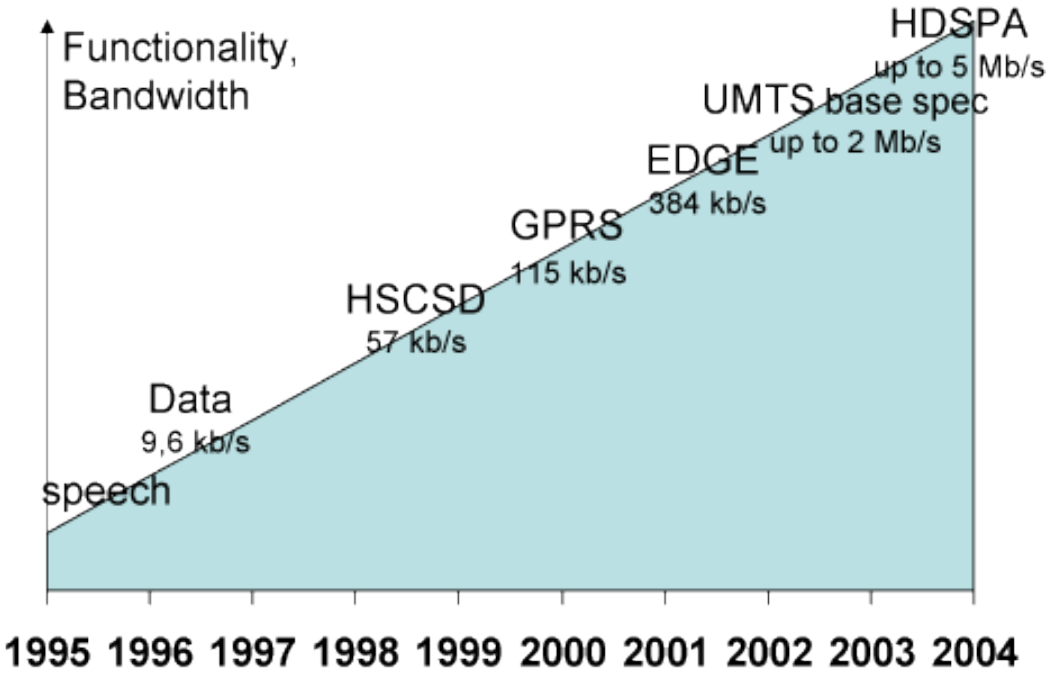
80's	analog access
90's	ISDN, GSM (GPRS et al.)
200x	xDSL (>160Kbit/s), cable, powerline, satellite, WLAN (hot-spots), UMTS
emerging:	WiMAX
future:	4th generation wireless networks, fiber-to-the-home (FTTH)

Criteria for Internet Access Technologies

- A variety of technologies exist for realizing Internet access for devices
- Classification of technologies possible by means of
  - throughput
  - mobility
  - area coverage / availability
  - effort / costs

Development of Mobile Technologies

- GSM to UMTS development: increasing bandwidths



UMTS Services and Applications

- Anywhere-anytime communication
- Multimedia services
  - Telephony
  - Video conferencing
  - Entertainment (interactive gaming, music on demand, video streaming, etc.)
- Personal Services
  - Remote monitoring and control (e.g. of the home)
  - Mobile banking
- Location-based services
  - What movies are playing here?
  - Where is the next Italian restaurant
- Mobile Internet access

UMTS Requirements and Challenges

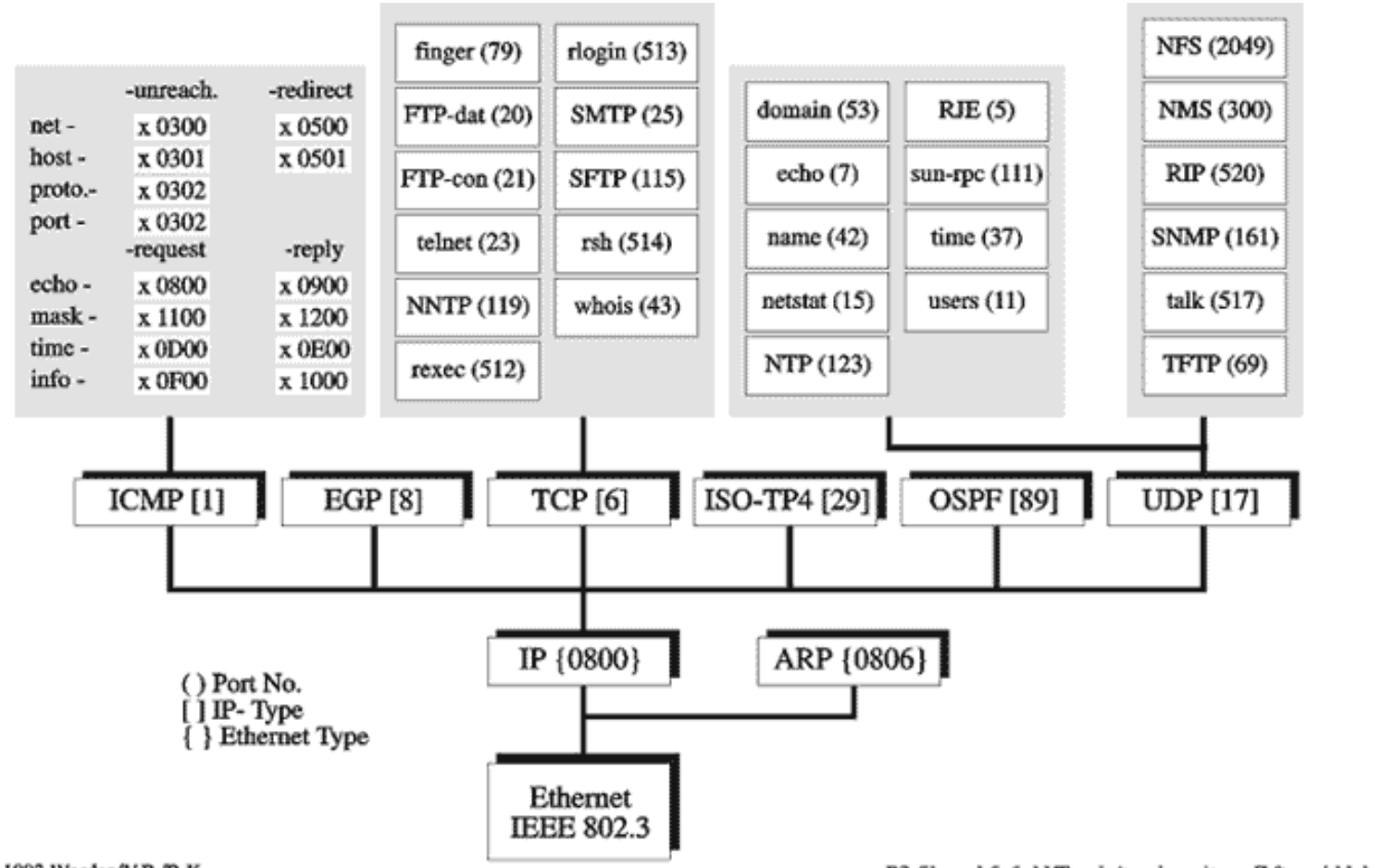
- Global access using a single device
  - Global standard
  - Unified spectrum
  - High coverage
  - Seamless handover
- Support of multimedia services
  - High data rates
  - Variable bandwidths
  - Symmetrical and asymmetrical data transfer
  - Circuit-switched and packet-switched transfer
  - High speech (and multimedia) quality
- Extendable multi-service network
  - Easy to deploy new services
  - Convergence of telephony and Internet services
- Operator services
  - Tight control over network resources by network operator
  - Sophisticated charging functionality
- Backward compatibility to 2G systems(GSM)

4.3. Protocols (Layer 3-7)

Examples for typical protocol tasks:

- Layer 3: End-to-end connectivity (host-to-host)
- Layer 4: Process-to-Process connectivity
- Reliable communication
  - Error detection
  - Error recovery (forward error correction or retransmission)
- Resource management
  - avoid congestion, by flow control
    - within the network
    - within end systems
  - Priorization
  - Resource reservation
- Support for specialized media types
  - Content description
  - Timing / Synchronization Information
- And more …

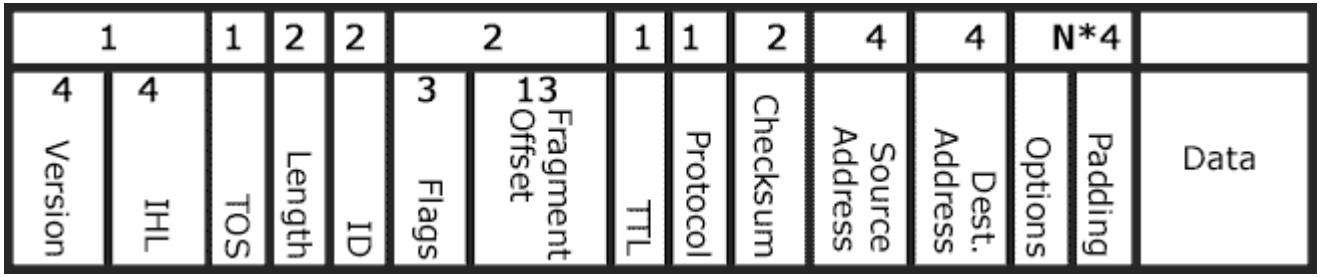
TCP/IP Suite

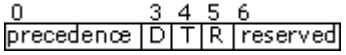

-unreach.
-redirect
net - x 0300 x 0500
host - x 0301 x 0501
proto.- x 0302
port - x 0302
-request
-reply
echo - x 0800 x 0900
mask - x 1100 x 1200
time - x 0D00 x 0E00
info - x 0F00 x 1000
finger (79)
rlogin (513)
FTP-dat (20)
SMTP (25)
FTP-con (21)
SFTP (115)
telnet (23)
rsh (514)
NNTP (119)
whois (43)
rexec (512)
domain (53)
RJE (5)
echo (7)
sun-rpc (111)
name (42)
time (37)
netstat (15)
users (11)
NTP (123)
NFS (2049)
NMS (300)
RIP (520)
SNMP (161)
talk (517)
TFTP (69)
ICMP [1]
EGP [8]
TCP [6]
ISO-TP4 [29]
OSPF [89]
UDP [17]
IP {0800}
ARP {0806}
( ) Port No.
[ ] IP- Type
{ } Ethernet Type
Ethernet
IEEE 802.3
1993 Worden/V.B./R.K.
PS-file: pub/info.kl/Tcp_ip/tcp_ip_suite.ps.Z ftp.uni-kl.de

4.3.2. IP Protocol (RFC 791)

- **Development of IP**
  - DARPA: Defense Advanced Research Projects Agency
    - The research aim was to build a network that is tolerant to extensive damage, e.g. by a nuclear strike
    - 1973/1974 development of TCP/IP, a replacement of NCP (Network Control Protocol)
    - Since 1975 the ARPANET was controlled by the DoD
    - In the early 80'ies the military part was extracted from the ARPANET
    - Since 1983 exclusive use of TCP/IP, defining the term Internet
  - IP is specified in RFC 791
  - "This document is based on six earlier editions of the ARPA Internet Protocol Specification ..."
- **IP characteristics**
  - Provides end-to-end communication
  - Connection less, i.e. state less protocol
  - Provides unreliable transfer of packets
  - Packets may be reordered during transmission
  - Error messages are handled by the separate protocol ICMP (Internet Control Message Protocol)

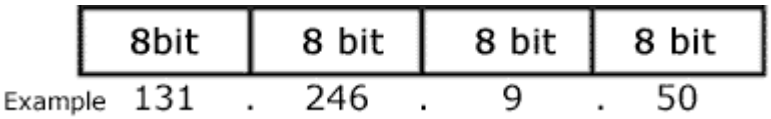
IP Header



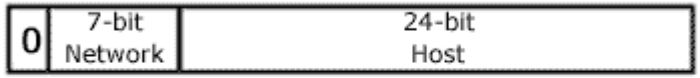
- **Version:**
  - version of IP header
- **IHL**:
  - IP header length in 32 bit words (5+ no. of options)
- **TOS**:
  - Type Of Service 

precedence ~ priority; D,T,R if set optimize for Delay, Throughput, Reliability
- **Length**:
  - length in bytes including the IP header
- **ID**:
  - serial number
- **Flags, Frag. Offset**:
  - used for fragmentation
- **TTL**:
  - Time To Live
  - decremented by each machine to pass t
- **Protocol**:
  - layer 4 protocol, e.g. 1=ICMP, 6=TCP, 17=UDP he packet
- **Checksum**:
  - checksum for the IP header
- **Options**:
  - security, record route, timestamp, source routes

IP Address Classes



Class A Network



128 Networks with **17,000,000** Hosts

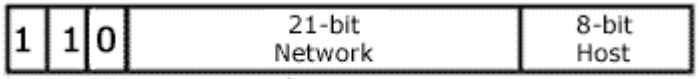
Address	Status
0.0.0.0	*Reserved*
1.0.0.0 - 126.0.0.0	Available
127.0.0.0	*Reserved*

Class B Network

16,000 Networks with **65,000** Hosts

Address	Status
128.0.0.0	*Reserved*
128.1.0.0 - 191.254.0.0	Available
191.255.0.0	*Reserved*

Class C Network



2,000,000 Networks with **255** Hosts

Address	Status
192.0.0.0	*Reserved*
192.0.1.0-223.255.254.0	Available
255.255.255.255	*Reserved*

- An IP address is a unique identifier for an end system
- Each address consists of two parts (hierarchy levels):
  - a network address
  - a host address
- **Usage of classes is out-dated**

IP Addresses and Netmasking

IP Address:

131	.	246	.	9	.	5	dotted decimal format
83		F6		9	.	5	hexadecimal format
10000011	.	11110110	.	00001001	.	00000101	binary format

Netmask:

11111111	.	11111111	.	11111000	.	00000000	binary format
FF		FF		F8	.	0	hexadecimal format
255	.	255	.	248	.	0	dotted decimal format

- Classless inter-domain routing (CIDR)
  - Different network masks enable multiple level of hierarchies
- Prefix notation: IP-Address/n
  - n = number of bits used for netmask
  - Example: 131.246.103.0/24

Routing

- Routers are used to connect networks
- **Routing: making a local forwarding decision based on global topology information, this decision must take into account QoS guarantees / assurances**
- How to obtain topology information:
  - Default routing
  - Static or non adaptive routing
    - Does not take into account changes of the network
  - Dynamic or adaptive routing, requires routing protocols
    - Identifies the topology of the network automatically
    - Different metrics are used to describe distances
      - Number of hops
      - Available bandwidth
      - Error rates
      - ...

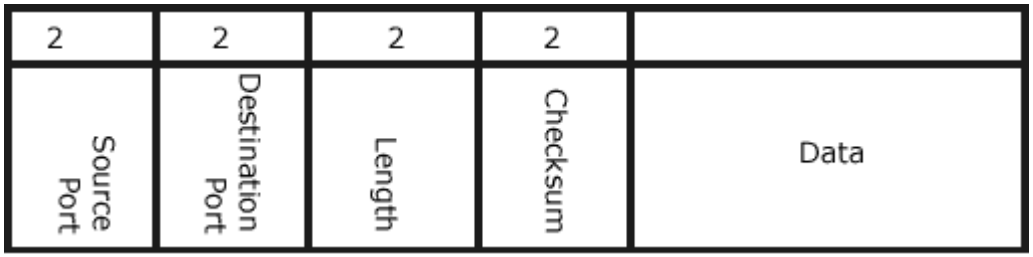
Routing Hierarchy

- **Interior Gateway Protocol (IGP)**
  - Routing within a LAN or administrative domain
  - Each node may know the whole (local) topology
  - Examples: Routing Information Protocol (RIP), IGRP, OSPF
- **Exterior Gateway Protocol (EGP)**
  - Between Service Providers (ISPs), e.g.
  - Example: Border Gateway Protocol (BGP), may be used exterior (EBGP) and interior (IBGP)
- **Routing Protocol types**
  - **Distance-Vector:**
    distribute local routing table to all neighbors. The paths with the lowest advertised costs are added to the local routing table (routing bassed on "direction signs")
  - **Link-State:**
    each router maintains at least a partial map of the network topology. Changes of a link state are flooded through the network (routing bassed on (partial) topology "maps").

4.3.3. UDP (RFC 768) / TCP (RFC 793)

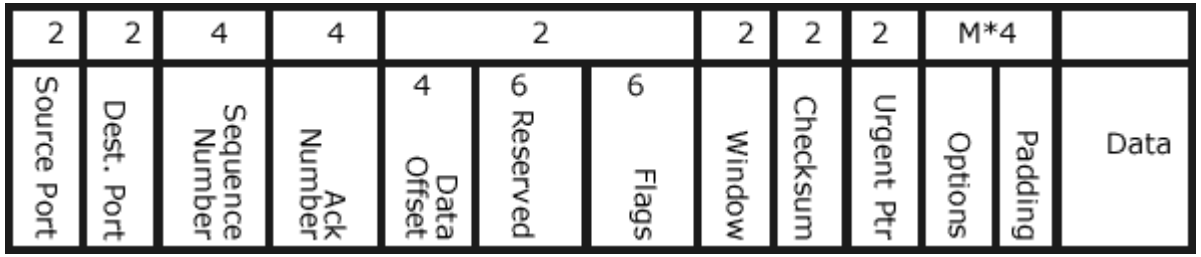
- **Transport protocols (Layer 4)**
  - Provides process to process connectivity
  - Uses port number to identify processes. An IP address and a port number is a unique identifier for a service.
- **Characteristics**
  - Closely related to IP
  - UDP offers a connectionless and unreliable transport service
    - Nearly the same service as IP
    - Data unit name: datagram
  - TCP offers a connection oriented and reliable transport service
    - Recognition of lost data
    - Retransmission of lost data
    - Reordering of data
    - Delete duplicate data
    - Flow control
      - With respect to network congestion
      - With respect to buffer overflow at the receiver side
    - User data is handled as a stream of bytes
      - User data is split into segments
    - Data unit name: segment

UDP Header



- **Source Port, Destination Port:**
  - port number of sender and receiver
- **Length:**
  - length of the UDP datagram
- **Checksum:**
  - the checksum covers the UDP pseudo header and the UDP data
- **The UDP pseudo header includes the UDP Header and 12 bytes of the IP header:**
  - 2*4 byte IP source and destination address
  - 1 byte 0
  - 1 byte protocol
  - 2 byte IP header length

TCP Header



- **Source Port, Destination Port:**
  - port number of sender and receiver
- **Sequence Number:**
  - TCP counts every byte of a stream.
  - This is the number of the first data byte
- **Ack Number:**
  - If the ACK control bit is set this field contains the value of the next sequence number the sender expects to receive
- **Data Offset:**
  - number of 32 bit words in the TCP header
- **Flags:**
  - **urg:** urgent pointer is valid
  - **ack:** ack number is valid
  - **psh:** push data to level above
  - **rst:** reset connection
  - **syn:** synchronize seq. Number
  - **fin:** close this side of the connection
- **Window:**
  - amount of data the sender is willing to accept (flow control)
- **Urgent Pointer:**
  - points to last byte of urgent data
- **Options:**
  - e.g. maximum segment size

TCP Service Mechanisms

- Retransmission
  - default: Go-back-n strategy, simple and robust mechanism but resource consuming
  - widely used: selective acknowledgement, retransmit lost packet only
  - in general retransmission causes unpredictable delay
- Flow control
  - Slow start and congestion avoidance realize considerate resource usage
    - enabling fair and cooperative bandwidth sharing
    - may cause high jitter
- TCPs service mechanisms were designed for reliable data transfer

→ TCP is not suitable for real-time communications

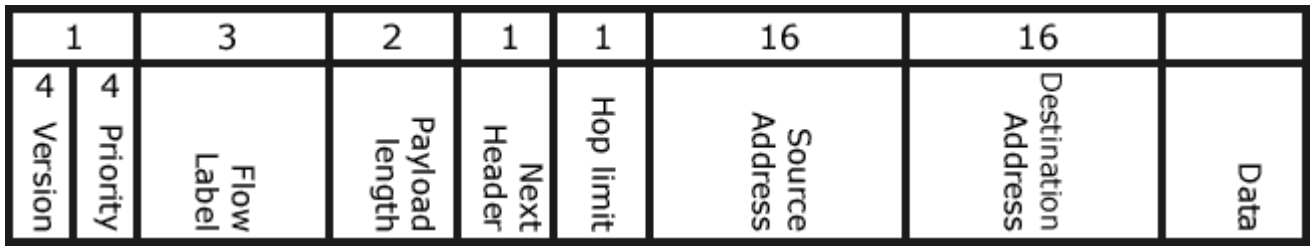
[TCP Summary] [TCP High Performance issues]

4.3.4. IPv6

Development of IPv6

- 1993 the IETF called for the development of an IP next generation IPng (RFC 1550)
- Improvements required
  - Larger address space
  - Reduce size of routing tables
  - Simplification of the protocol, to allow routers to process packets faster
  - Better security
  - Pay more attention to Type of Service
  - Aid multicasting
  - Support roaming
  - Easier extension of the protocol
  - Coexistence with the old IPv4
- 1995 the IETF agreed to specification named IPv6 (RFC1883)
  - Changes to other protocols of the TCP/IP suite are specified in RFC 1884-1887

IPv6 Header



- **Version:**
  - version of IP header
- **Priority:**
  - 0-7 for non real time data, 8-15 for real-time data
- **Flow Label:**
  - may be used to identify a flow, RFC 1809 discusses how the flow label could be used
- **Payload length:**
  - length of the datagram without the header
- **Next header:**
  - options are placed in separate extension header
  - next header identifies an option or the protocol above IPv6
- **Hop limit:**
  - same as Time to Live of IPv4
- **Addresses:**
  - there are $7*10^{23}$ IPv6 addresses per square meter of the world enabling well structured addresses
  - Support of provider based addresses and geographic based addresses

IP Header Extension

- **Hop-by-Hop options:**
  - For example: extending the payload length, enabling datagrams of more than 65535 bytes (so called jumbograms) or exchange information between routers
- **Routing:**
  - Full or partial routing path of a datagram
- **Fragmentation:**
  - Similar to IPv4 fragmentation but fragmentation is handled only by endsystems
- **Authentication:**
  - Identification of the sender
- **Encryption security payload:**
  - Information about encrypted payload
- **Destination options:**
  - Information that should be interpreted by the destination only

IPv6 Further Topics

- Experimental IPv6 networks exist, see the JOIN project of the DFN
- IPv6 is supported by most system software: AIX, BSD, HP-UX, Linux, Solaris, Windows
- To install the IPv6 Protocol for Windows XP:
  - at the command prompt, type: "ipv6 install"
- Many topics are still discussed:
  - geo based IPv6 addresses
  - IPv6 over IPv4, IPv4 over IPv6, IPv6 to IPv4 (6to4)
  - renumbering
  - auto configuration
  - use of the flow label field
  - security
  - mobility
  - ...

QoS in Data Networks

	IP Service Models			Traffic-Engineering Concept	Network Technology
	Best Effort	DiffServ	IntServ	MPLS	ATM
QoS Guarantees	no	aggregated	flow based	flow based and aggregated	flow based and aggregated
QoS Parameter	no	• long term • static • within a domain	• per flow • dynamic • end-to-end	Support for: • DiffServ • IntServ • ATM	• per flow (channel) or per path • dynamic or static • end-to-end or within a domain

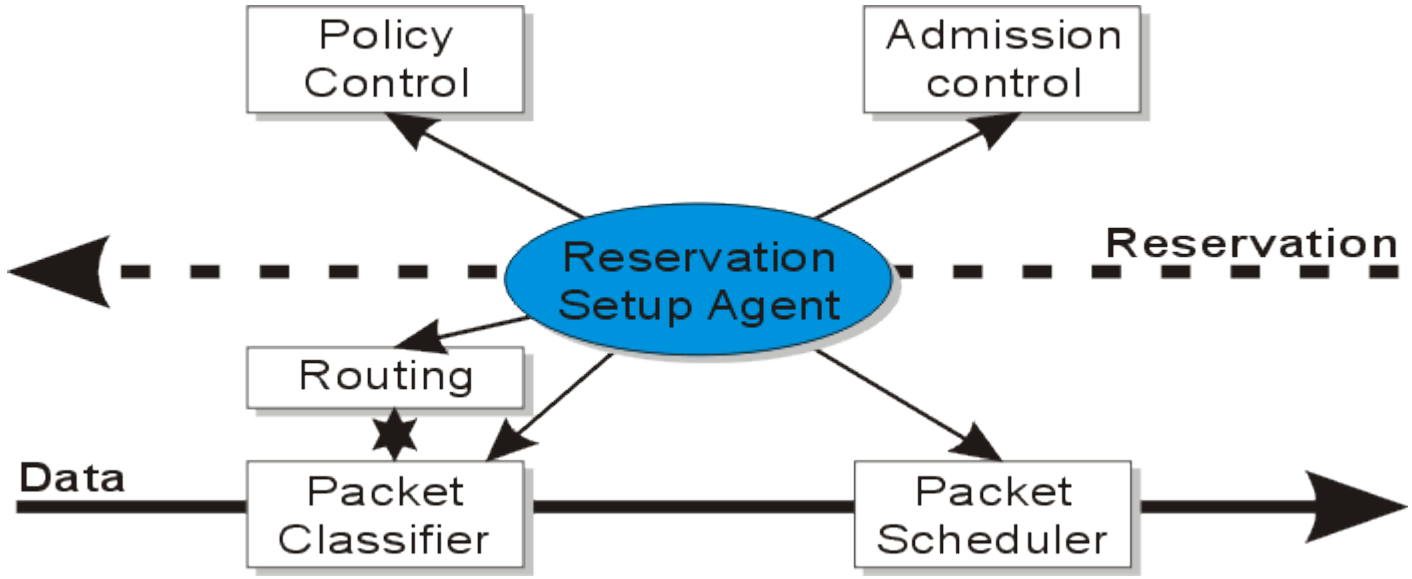
4.3.5. Integrated Services (RFC 1633)

- **Integrated Services (IntServ) is a reservation based model. The intention is to guarantee individual QoS profiles for each flow.**
- **What is a flow?**
  - A flow is a stream of packets originated from the same application session
  - The term "flow" describes semantical coherence of data
- **Categories of applications**
  - Elastic applications, no delivery requirements as long as the packets reach the destination, e.g. TCP traffic (machine to machine)
  - Real Time Tolerant (RTT) applications, demand weak bounds for the maximum transfer delay, also some packet loss is acceptable, e.g. streamed video (machine to human)
  - Real Time Intolerant (RTI) applications, demand minimal delay and jitter, e.g. interactive application or videoconferences (human to human)

IntServ: Service Classes

- **Service Classes**
  - Guaranteed Service for RTI applications
    - Guaranteed amount of bandwidth
    - Deterministic upper bound for delay
  - Controlled Load Service for RTT applications
    - Provides a service equivalent to an unloaded network
    - Most packets will reach the destination
    - The average delay is guaranteed
  - Best Effort Service for all other applications
    - standard use of IP

IntServ: Components



- The Reservation Setup Agent is the only component that communicates with other nodes.
- The Resource Reservation Protocol (RSVP) was designed to meet the signaling requirements of IntServ.

IntServ: Packet Classifier

- **Packet Classifier:**
  - Determines the QoS class for each packet
  - May cooperate with routing mechanisms, packets of the same flow should always use the same path
  - Arbitrary parts of the packet header may be used for classification
    - IP-addresses and port numbers of the sender and/or receiver
    - Application data like frame types of a video stream (e.g. MPEG)
  - For IPv6 the flow label should be used
- **Potential problems:**
  - IP fragmentation must be avoided
    (RSVP compute a minimum MTU for a multicast tree)
  - Variable header length may require the interpretation of protocols
  - IP-level security prevents access to higher layer protocols

IntServ: Packet Scheduler

- **Packet Scheduler:**
  - The QoS capabilities of a Layer-2 network could be utilized to implement the packet scheduler functionality
  - Manages access to the Layer-2 network in order to guarantee the requested QoS
  - Some methods for the QoS implementation
    - Priority queuing
    - Weighted fair queuing
    - Packet level traffic shaping
- **Potential problems:**
  - The IntServ model can not guarantee QoS if anywhere in the data path
    - a non IntServ capable router must be passed
    - a non QoS capable Layer-2 network must be shared with a non IntServ capable node

IntServ: Admission and Policy Control

- **Admission Control**
  - resource management
  - decides whether the local system is able to support the requested traffic flow
- **Policy Control**
  - is optional
  - determines whether the requester has administrative permissions to make the reservation

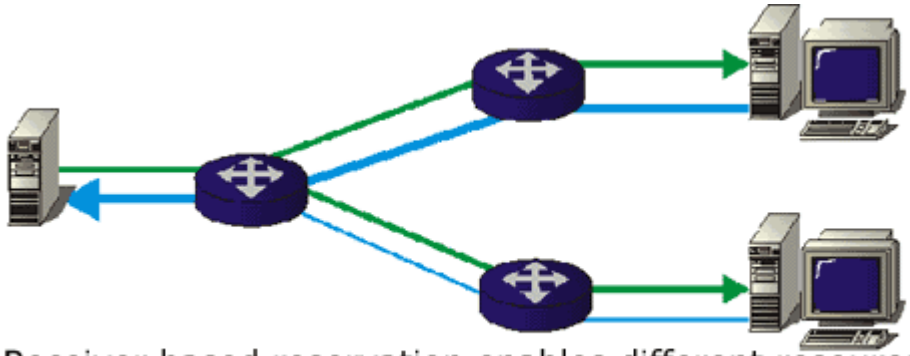
If either check fails the request is rejected, PDUs of that flow may be discarded or forwarded with a lower priority

4.3.6. RSVP - Resource Reservation Protocol (RFC 2210)

- **RSVP is a general signaling protocol for QoS control services**
  - The signaled objects are opaque for RSVP
- **A main focus of RSVP is to support multicast communication**
  - Unicasts are treated as special cases of multicast only
  - RSVP performs receiver oriented reservations
    - Support different requirements of many receivers
    - Support heterogeneous networks
- **RSVP uses soft-states, i.e. signaled information is valid for a fixed time interval only**
  - Simplifies cooperation with connection less IP
  - Reservations must be refreshed periodically
    - Resource consuming
    - Prevents usage of RSVP in large networks
- **Merging of reservation supports multiple senders in a multicast environment**

RSVP Receiver oriented Reservation (1)

- RSVP implements hybrid negotiation



Receiver based reservation enables different resource usage within one multicast tree

RSVP Receiver oriented Reservation (2)

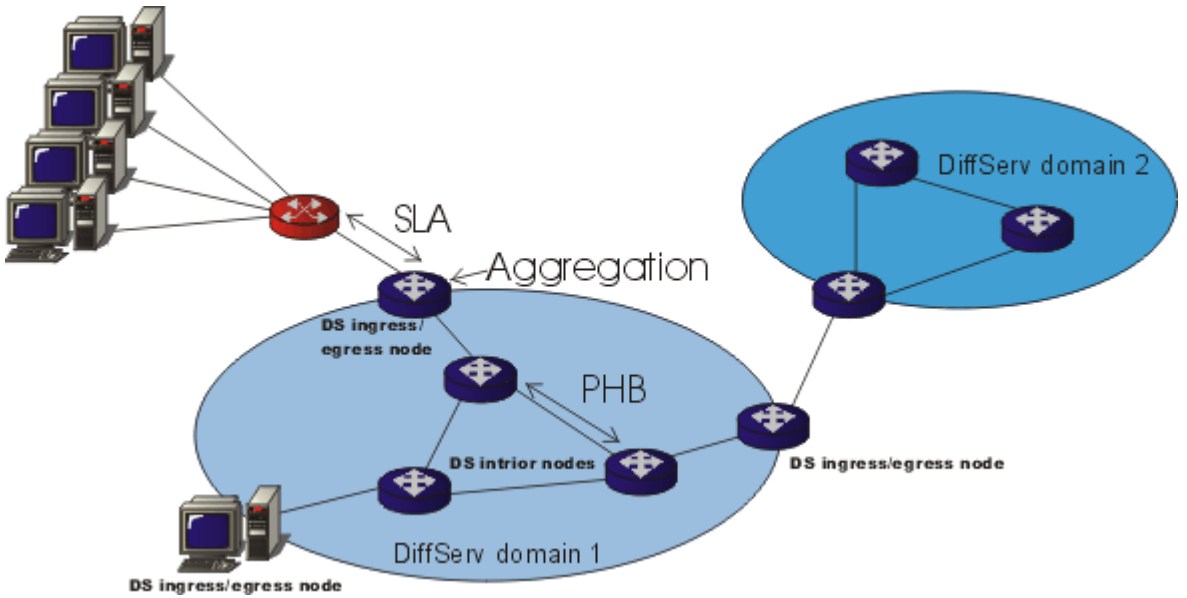
- **A PATH message is sent from sender to receiver**
  - The sender specifies its traffic specification (sender TSpec)
  - The sender specifies its traffic characteristic (ADSPEC)
  - Detection of path characteristics
    - Detected bandwidth limitations, minimum packet size (MTU), may modify ADSPEC
    - RSVP capable nodes get to know their RSVP capable neighbors
  - RSVP does not perform routing; routing is done by standard components which do not know anything about QoS
- **A RESV message is sent from receiver to sender**
  - The RESV message travels the path backward, perform reservations
  - The receiver application determines the required resource reservation and replies with
    - Traffic specification (receiver Tspec)
    - Requested Service Specification (receiver Rspec)

4.3.7. Differentiated Services RFC 2475

- **Differentiated Services (DiffServ, DS) is a model to differentiate services on the Internet.**
- The key goals are:
  - fast determination of a service class for a (IP) packet
  - being scalable
- The key concepts are:
  - traffic classification and service realization are separated
  - each DiffServ domain has its own set of services
  - traffic classification is done only at the border of a DiffServ domain
  - assume that only a few different static services are required
    - it is sufficient to specify services in long term contracts
    - many flows will receive the same service, i.e. will share the resources of a service
    - admission and usage control is necessary in order to guarantee a specific QoS

DiffServ Domains

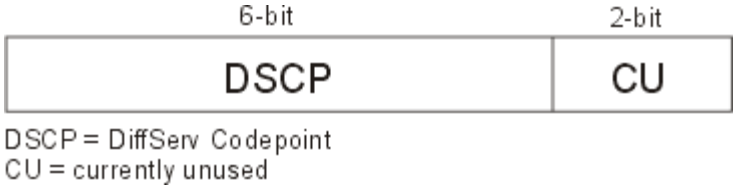
- Example:



- SLA = Service Level Agreement, between user and provider
- Aggregation = all traffic flows that will receive the same service
- PHB = Per Hop Behaviour, is the externally observable forwarding behavior

DiffServ Codepoint RFC 2474

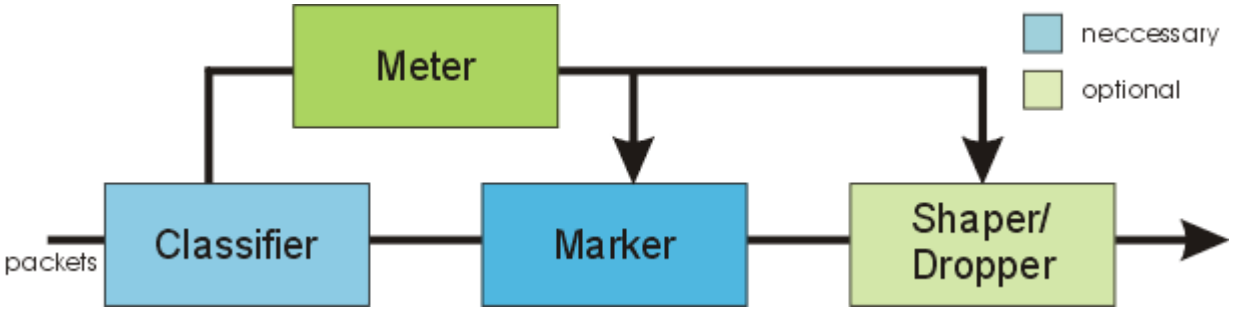
- Within a DiffServ domain each packet is marked by a 6-bit codepoint.
- All packets with the same codepoint build a so called "Behavior Aggregate" which is also called "Aggregate".



- **IPv4:**
  - The Codepoint overwrites the TOS field in the IPv4 header
  - Some routers use the precedent bits of the TOS field, therefore some DiffServ domains may use a limited Codepoint of 3 bits
- **IPv6:**
  - The Codepoint overwrites the priority field of the IPv6 header

DiffServ Traffic Classification

- Logical view of packet classification and conditioning:



- **Classification:**
  - performed at ingress node
  - depends on Service Level Agreement (SLA) between user and provider
  - based on packet data or an already assigned codepoint
- **Meter:**
  - perform policing according to a specified traffic profile (average bandwidth, peak-bandwidth, burstsizes, ...)
- **Marker:**
  - assigns a 6-bit codepoint
  - different codepoints may be assigned to "in-profile" and "out-of-profile" packets
- **Shaper/Droper:**
  - may delay or drop "out-of-profile" packets (traffic conditioning)

DiffServ Per-Hop-Behavior (1)

- **The Per-Hop-Behavior (PHB) describes the service of a specific aggregate.**
  - DiffServ does not define a fixed set of parameters describing a PHB, i.e. DiffServ does not specifiy the service types which may be supported by a DiffServ domain (except the default PHB)
  - A PHB is described by the externally observable forwarding behavior
  - A PHB is identified by the codepoint of each IP packet
- **PHBs may be specified by:**
  - resource description (buffer usage, bandwidth, ...)
  - priorities relative to other PHBs
  - observable traffic characteristics (delay, loss, ...)
  - Example: guarantee a minimal bandwidth allocation of X% of a link, with proportional fair sharing of any excess link capacity

DiffServ Per-Hop-Behavior (2)

- **Suggested PHB types:**
  - default PHB, standard IP service = best-effort service
    codepoint: 000000
  - Class-Selector PHB, provides backward compatibility to IPv4 precedent bits
    codepoint: xxx000, x = 0 or 1
  - Assured Forwarding PHB (RFC 2597), defines four traffic classes and three drop precedence per class. According to the SLA buffer and bandwidth resources will be assigned to each class. Out-of-Profile traffic may be marked with a higher drop precedence

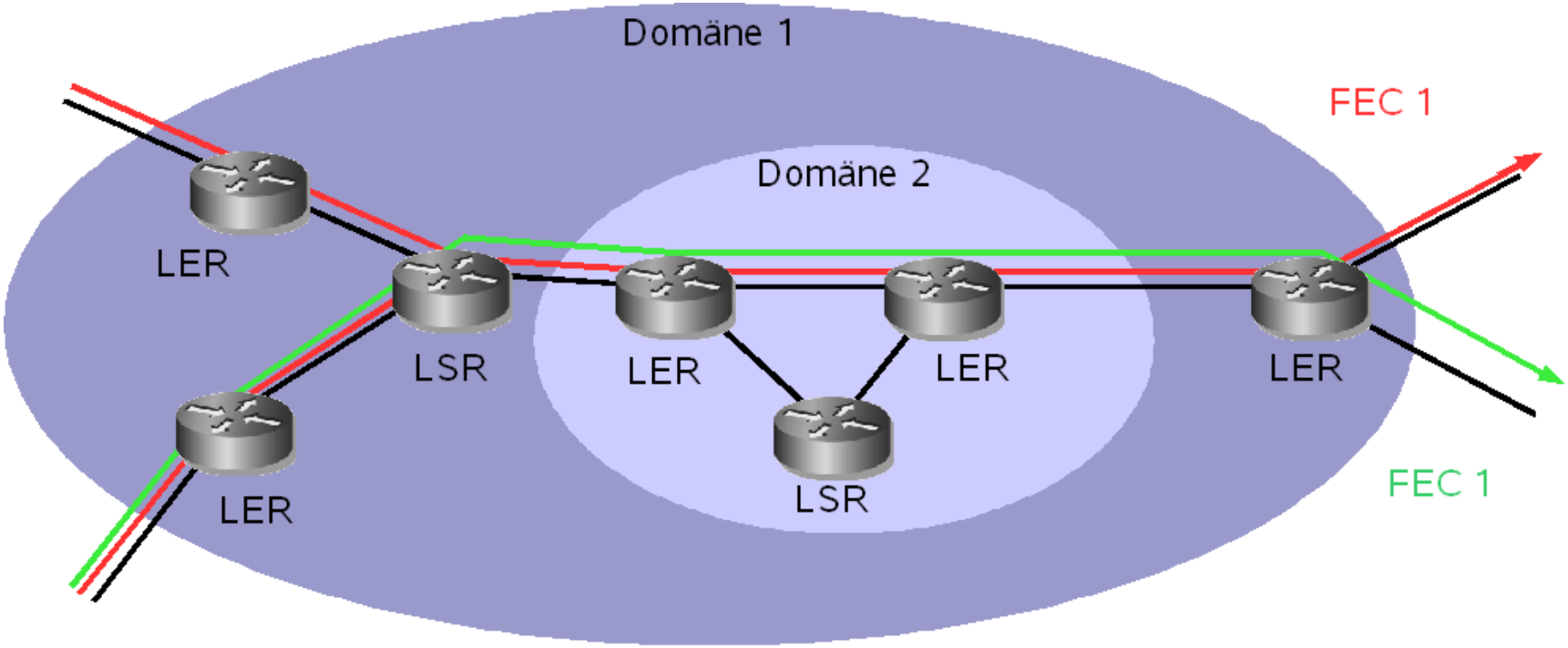
Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low drop precedence	001010	010010	011010	100010
Medium drop precedence	001100	010100	011100	100100
High drop precedence	001110	010110	011110	100110

  - Expedited Forwarding PHB (RFC 2598), guarantees a specified bandwidth (according to the SLA)
    codepoint 101110

4.3.8. Multiprotocol Label Switching (MPLS) RFC 3031

- **MPLS is a traffic-engineering model**
- **Main goals:**
  - replace complex routing decisions by much more simpler packet forwarding (switching) technologies
  - enable traffic engineering, i.e. explicit control of data flows
  - separate signaling and data flow
  - interact with existing: routing protocols, L2 and L3 protocols and QoS capabilities
- **Basic concepts:**
  - assume that there are many packets in a network domain that will be treated in an equivalent manner
    equivalence = the packets leave the domain at the same (logical) link (and the packets receive the same QoS)
  - classify packets at the domain borders, i.e. assign a packet to a Forward Equivalence Class (FEC)
  - packets of the same FEC are marked with a label, within a MPLS domain packets may be forwarded (switched) based on that label.
  - Note: conventional routing is like assigning a packet to an FEC in each router

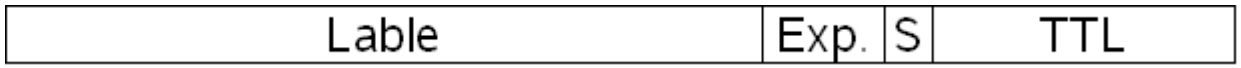
MPLS Example



- LER = Label Edge Router: add and remove labels
- LSR = Label Switching Router: forward packets based on labels
- FEC = Forwarding Equivalence Class

MPLS Label Encoding

- A label is a short fixed length locally significant identifier for an FEC.
- For most Layer-3 technologies the label is encoded in a so called Shim-Header:

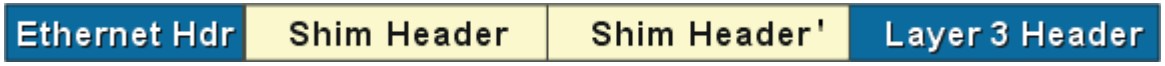


  - Lable (20 bit) = the identifier of an FEC
  - Exp (3 bit) = experimental, suggestion: use as a diffserv 3-bit codepoint
  - S (1 bit) = marker for last lable on stack
  - TTL (8 bit) = time to live, copied from higher layer protocols, e.g. IP

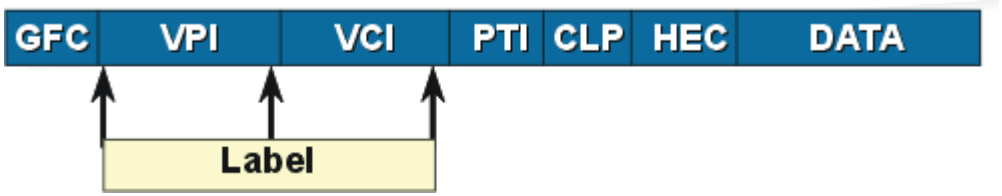
MPLS Label Placement

- Insert Header in Ethernet Frame:

- Multiple lables are stacked:



- Use VPI/VCI field of ATM for MPLS label:



MPLS and QoS

- MPLS lables can be mapped to ATM cell headers.
  - ATM can be integrated in an MPLS environment and the ATM QoS capabilities can be utilized for FECs
- MPLS is able to offer services similar to IntServ and can even interact with IntServ
  - Contraint-based routing-LDP (CR-LDP), extends the LDP by resource reservation request, which is similar to ATM VBR QoS Traffic characteristic specification
  - RSVP-TE, extends the RSVP protocol by lable distribution for MPLS. Thus it is possible to request a resource reservation within an MPLS domain in the same way as in an IntServ environment
- MPLS lables can be used to support DiffServ
  - The 3-bit "extension field" of the MPLS lable can be used to differentiate 8 DiffServ classes
  - Portions of the MPLS lable can be used/mapped to a DiffServ codepoint

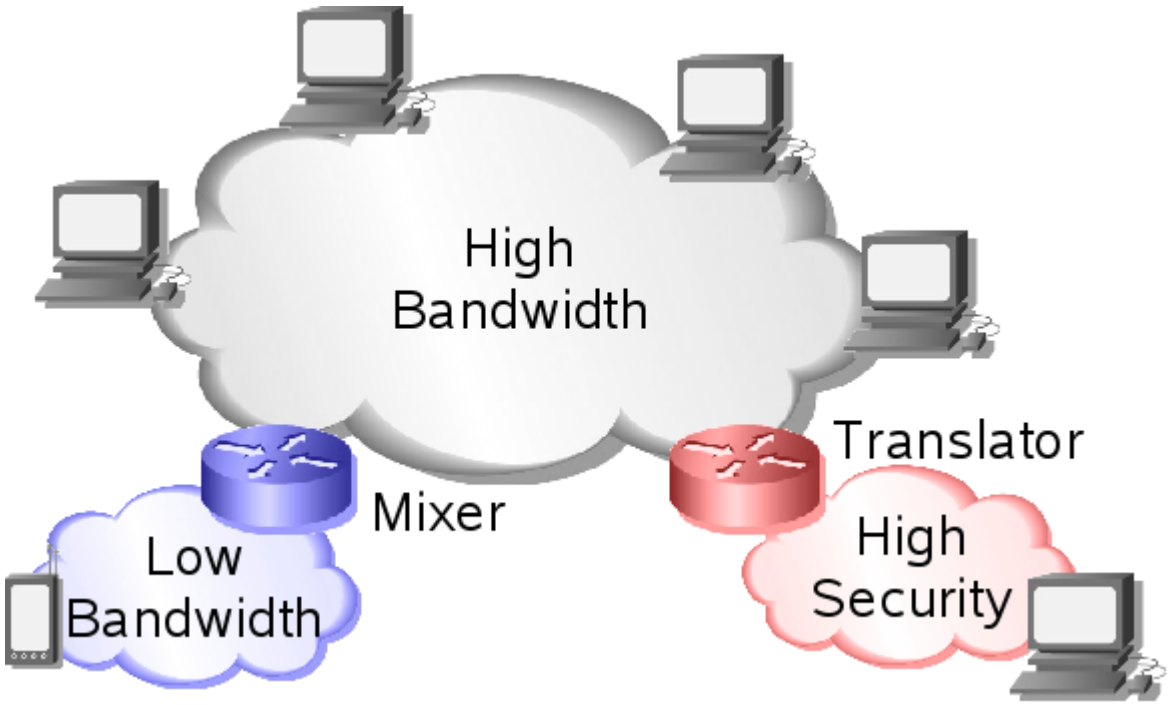
MPLS Remarks

- MPLS was not designed to support any QoS. Identification of flows or "traffic aggregates" makes QoS implementation much easier. MPLS may support QoS by
  - supporting DiffServ
  - utilizing ATM for IP traffic
  - request resource reservation for each FEC, by extending label distribution with qoS parameters (RSVP-TE or CR-LDP)
- Advantages of MPLS
  - connection setup or connection release is not required
  - is limited by domains, i.e. networks belonging to different administrative domains do not need to cooperate. Therefore MPLS may be utilized in parts of a network only, e.g. WAN or backbones
  - MPLS is protocol independent

4.3.9. RTP - Real-Time Transport Protocol (RFC 1889)

- **Consists of two closely-linked parts:**
  - the real-time transport protocol (RTP), carries data with real-time properties
  - the RTP control protocol (RTCP), monitors QoS and distributes this information to all participants of a session
- **RTP makes no reservations and does not guarantee any service**
- **RTP is a protocol framework, not a complete protocol**
  - a profile specification defines payload types and may extend RTP
  - a payload specification defines payload formats and encoding types must be specified
  - therefore RTP will typically be part of an application

RTP - Scenario

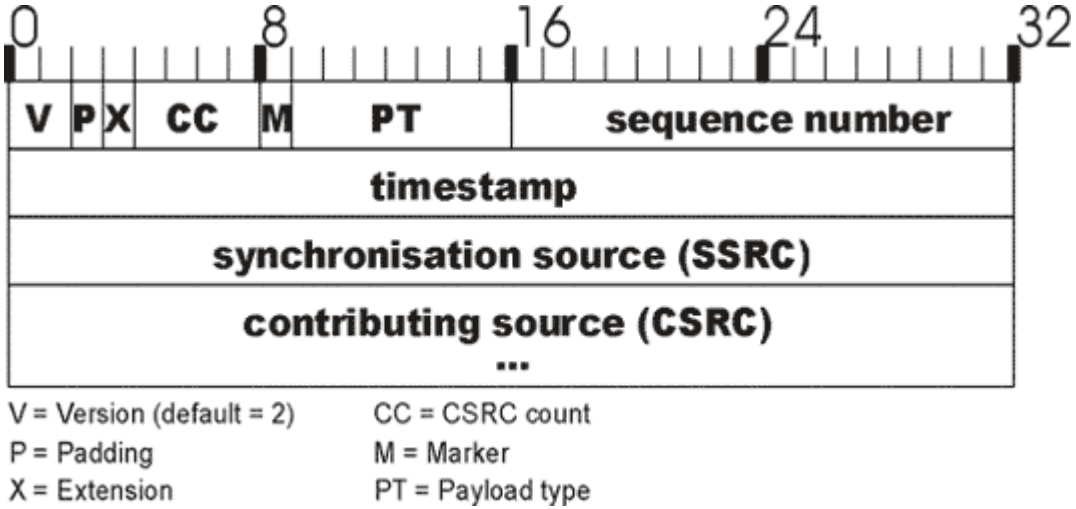


many-to-many communication (e.g. video conference)

RTP - Definitions

- **RTP-Session:**
  - is a set of participants
  - each participant is identified by a host and a destination port address
  - each medium is carried in a separate RTP-session
- **Mixer:**
  - is an intermediate system that receives data from one or more sources, possibly changes the data format and combines packets in some manner
  - a mixer will make timing adjustments and generate an own timing for combined data
- **Translator:**
  - is an intermediate system that forwards data without changing media or synchronization
  - encryption and addresses may be changed
  - multicast may be mapped to unicast and vice versa

RTP - Header



- the payload type is defined by the applications profile
- the sequence number enables receivers to detect lost RTP-PDUs
- the timestamp reflects a sampling instant. i.e. the timestamp unit depends on the encoding and does not need to correspond with the system clock
- SSRC identifies the last sync. entity; it is unique within a session
- CCSR identifies the contributor of a source

RTCP - RTP Control Protocol

- **RTP enables receiver to monitor the QoS:**
  - Delay, jitter, PDU loss rate
- **RTCP periodically transmits control packets between all participants of an RTP session:**
  - the primary function is to provide feedback about the QoS
  - carries transport-level identifiers for RTP sources, the canonical name (the SSRC may change over the time; the canonical name is fixed, e.g. a user name)
  - the rate of sent RTCP packets depends on the number of participants in order to make RTCP scalable
  - optionally, further information about the participants could be distributed to realize a simple session control

Interesting Links

- Routing Basics
  - http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Routing-Basics.html
- Size of BGB Tables
  - http://bgp.potaroo.net/
- Internetworking Technology Handbook
  - http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
- Its Latency
  - http://www.potaroo.net/papers/isoc/2004-01/latency.html
- TCP - How it works
  - http://www.potaroo.net/papers/isoc/2004-07/tcp1.html
- Visualroute
  - http://www.webhits.de/english/index.shtml?visualroute.html