ATM Protocol Architecture

- similarities between ATM and packet switching:
  - transfer of data in discrete chunks
  - allow multiple logical connections over single physical interface
- packets are of fixed size (called cells)
- ATM is a streamlined protocol with minimal error and flow control capabilities
  - reduced overhead of processing ATM cells
  - reduced the number of overhead bits
- data rates (physical layer) 25.6Mbps to 622.08Mbps
Reference Model Planes

- **User plane**
  - provides for user information transfer, along with the associated controls (e.g., flow control, error control)
- **Control plane**
  - performs call control and connection control
- **Management plane**
  - plane management
  - performs whole system functions and provides coordinates between the planes
  - layer management
  - performs management functions relating to resources and parameters in protocol entities

ATM Logical Connections

- referred to as Virtual Channel connections (VCC)
- VCC is analogous to virtual circuit in X.25
- VCC is set up between two end users through the network and a variable-rate, full duplex flow of fixed-size cells is exchanged over the connection
- VCC are also used for user-network exchange (control signaling) and network-network exchange (network management and routing)
- **Virtual Path Connection (VPC) concept**
  - bundle of VCC with the same end points
  - i.e., all of the cells flowing over all of the VCCs in a single VPC are switched together

ATM Connection Relationships

Advantages of Virtual Paths

- simplified network architecture
  - network transport functions can be separated into those related to an individual connection and those related to a group of logical connection
- increased network performance and reliability
  - the network deals with few aggregated entities
- reduced processing and short connection set up time
  - much of the work is done when the virtual path is set up
  - capacity reservation, i.e. simple connection admission functions performed at endpoints and no connection processing required at transit nodes
- enhanced network services
  - the virtual path is used internal to the network but also visible to the end user
  - e.g., closed user groups
Call Establishment Using VPs

- The process of setting up a virtual path connection is decoupled from the process of setting up an individual VCC.
- The virtual path control mechanisms include calculating routes, allocating capacity, and storing connection state information.
- To set up a virtual channel, there must be a virtual path connection to the required destination with sufficient available capacity to support the virtual channel, with appropriate QoS. A VC is set up by storing the required state information (VC/VP mapping).

Virtual Channel Connection Uses

- Between end users:
  - End-to-end user data
  - Control signals
- Between end user and network:
  - Control signaling
- Between network entities:
  - Network traffic management
  - VPC can be used to define a common route for the exchange of network management information.

Control Signaling - VCC

- A mechanism is needed for the establishment and release of VCCs and VPCs.
- The exchange of information is referred as control signaling and takes place on separate connection.
- Semi-permanent VCC, no control signaling is required.
- Meta-signaling channel:
  - If there is no pre-established call control signaling channel, than one must be set up.
  - For that propose, a control signaling exchange must take place between user and network on some channel.
  - Used as permanent control signal channel.
- User to network signaling virtual channel:
  - Meta-signaling is used to set up this VCC between user and network.
  - For control signaling.
  - Used to set up VCCs to carry user data.
- User to user signaling virtual channel:
  - Meta-signaling is used to set up this VCC between users.
  - It must be set up within pre-established VPC.
  - Used by two end users without network intervention to establish and release user to user VCC to carry user data.
Control Signaling - VPC

- A VPC can be established on **semi-permanent** basis by prior agreement:
  - No control signaling is required
- VPC establishment/release may be **customer controlled**:
  - The customer uses a signaling VCC to request the VPC from the network
- VPC establishment/release may be **network controlled**:
  - The network establishes a VPC for its own convenience

ATM Cells

- **Fixed size**
- 5 octet header
- 48 octet information field
- Small cells reduce queuing delay for high priority cells
- Small cells can be switched more efficiently
- Easier to implement switching of small cells in hardware

ATM Cell Format

Header Format

- Generic flow control
  - Only at user to network interface
  - Controls flow only at this point
- Virtual path identifier
- Virtual channel identifier
- Payload type
  - Indicates the type of information
  - E.g. user info or network management
- Cell loss priority
- Header error control
Transmission of ATM Cells

- Available data rates
  - 622.08Mbps
  - 155.52Mbps
  - 51.84Mbps
  - 25.6Mbps
- Two approaches
  - Cell based physical layer
  - SDH based physical layer

ATM Service Categories

- Real time
  - Constant bit rate (CBR)
  - Real time variable bit rate (rt-VBR)
- Non-real time
  - Non-real time variable bit rate (nrt-VBR)
  - Available bit rate (ABR)
  - Unspecified bit rate (UBR)

Real Time Services

- Amount of delay
- Delay variation (jitter)

CBR

- Fixed data rate continuously available
- Tight upper bound on delay
- Uncompressed audio and video
  - Video conferencing
  - Interactive audio
  - Audio/Video distribution and retrieval
rt-VBR

- time sensitive application
- tightly constrained delay and delay variation
- rt-VBR applications transmit at a rate that varies with time
- e.g. compressed video
  - produces varying sized image frames
  - original (uncompressed) frame rate constant
  - compressed data rate varies
- can statistically multiplex connections

nrt-VBR

- may be able to characterize expected traffic flow
- improve QoS in loss and delay
- end system specifies
  - peak cell rate
  - sustainable or average rate
  - measure of how bursty traffic is
- e.g. airline reservations, banking transactions

UBR

- may be additional capacity over and above that used by CBR and VBR traffic
  - not all resources dedicated
  - bursty nature of VBR
- for application that can tolerate some cell loss or variable delays:
  - e.g. TCP based traffic
  - cells forwarded on FIFO basis
- best efforts service

ABR

- application specifies peak cell rate (PCR) and minimum cell rate (MCR)
- resources allocated to give at least MCR
- spare capacity shared among all ARB sources
- e.g. LAN interconnection
ATM Bit Rate Services

- Available Bit Rate and Unspecified Bit Rate
- Variable Bit Rate
- Constant Bit Rate

ATM Adaptation Layer

- to support for information transfer protocols not based on ATM
  - e.g., PCM (voice)
    - to assemble bits into cells
    - to reassemble into constant flow
  - e.g., IP
    - to map IP packets onto ATM cells
    - to fragment IP packets

Adaptation Layer Services

- defined in ITU-T I.362
- handling of transmission errors
- segmentation and re-assembly, to enable larger blocks of data to be carried
- handling of lost and misinserted cells
- flow control and timing control

Supported Application types

- circuit emulation
  - to support TDM transmission over an ATM network
- VBR voice and video
- general data service
- IP over ATM
- multiprotocol encapsulation over ATM (MPOA)
  - supporting of the IPX, AppleTalk, DECNET
- LAN emulation
  - i.e., support of LAN broadcast capability
  - designed to allow an easy transition from a LAN environment to an ATM environment
AAL Protocols

- AAL layer is organized in two logical sublayers
  - Convergence Sublayer (CS)
    - support for specific applications
    - AAL user attaches at SAP (address of the application)
    - service dependent sublayer
  - Segmentation and Re-assembly Sublayer (SAR)
    - to pack and to unpack info received from CS into cells
    - packs any SAR headers and trailers plus CS info into 48-octets block
  - four types
    - Type 1
    - Type 2
    - Type 3/4
    - Type 5

AAL Type 1

- CBR source
- SAR packs and unpacks bits
- each block is accompanied by
  - sequence number (SN field), so that errored PDUs can be tracked
  - sequence number protection (SNP field), which is for an error protection

AAL Type 2

- VBR
- analog applications
  - intended for analog applications that require timing information but do not require a CBR
  - e.g., audio/video
### AAL Type 3/4
- VBR
- the service may be connectionless or connection oriented
- service may be message mode or stream mode

### AAL Type 5
- streamlined transport for connection oriented higher layer protocols
- this type of AAL was introduced to
  - reduce protocol processing overhead
  - reduce transmission overhead

### Segmentation and Reassembly PDU

### Frame Relay
- originally is designed to provide more efficient transmission scheme than X.25
- developed before ATM
- larger installed base than ATM
- ATM now of more interest on high speed networks, but the popularity of frame relay still exists
**Frame Relay Background - X.25**

- X.25 key issues
  - Call control packets are carried on the same channel and same VC as data packets, i.e. in band signaling
  - Multiplexing of virtual circuits at layer 3
  - Layer 2 and 3 include flow and error control
  - Considerable overhead
  - Not appropriate for modern digital systems with high reliability

**Frame Relay - Differences**

- Call control signaling is carried on a separate logical connection from user data
- Multiplexing and switching of logical connection performed at layer 2 (instead of layer 3 in X.25):
  - Eliminates one layer of processing
- No hop-by-hop error or flow control
- End-to-end flow and error control (if used) are done by higher layer:
  - Single user data frame sent from source to destination and ACK (from higher layer) sent back

**Disadvantages and Advantages**

- Lost the ability of link-by-link error and flow control
  - Increased reliability makes this disadvantage negligible
- Streamlined communications process
  - Reducing of the processing at user-network interface and internal network interface
  - It potentially produces lower delay and higher throughput
- ITU-T recommend frame relay up to 2Mbps

**Control Plane**

- Between subscriber and network
- Separate logical channel used
  - Similar to common channel signaling for circuit switching services
- Data link layer
  - LAPD (Q.921) is used to provide reliable data link control service with
    - Error and flow control
  - Between user (TE) and network (NT)
  - Used for exchange of Q.933 control signal messages
**User Plane**

- end-to-end functionality
- transfer of info between ends
- LAPF (Link Access Procedure for Frame Mode Bearer Services) Q.922:
  - frame delimiting, alignment and transparency
  - frame mux and demux using addressing field
  - ensure frame is integral number of octets (zero bit insertion/extraction)
  - ensure frame is neither too long nor short
  - detection of transmission errors
  - congestion control functions

---

**VLAN: Prerequisites**

- Local Area Network (LAN) was originally defined as a network of computers located within the same area
- today, LANs are defined as a single broadcast domain
- it means that if a user broadcasts information on his/her LAN, the broadcast will be received by every other user on the LAN
- broadcasts are prevented from leaving a LAN by using a router
- the disadvantage of this method is routers usually take more time to process incoming data compared to a bridge or a switch
- the formation of broadcast domains depends on the physical connection of the devices in the network
- **Virtual Local Area Networks (VLAN's) were developed as an alternative solution to using routers to contain broadcast traffic**

---

**Some facts on LAN (1/2)**

- in a traditional LAN, workstations are connected to each other by means of a hub or a repeater
- if two stations within one domain attempt to send information at the same time
  - a collision will occur and all the transmitted data will be lost
- once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters
- the original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources
- to prevent collisions from travelling through all the workstations in the network, a bridge or a switch can be used
  - these devices will not forward collisions, but will allow broadcasts (to every user in the network) and multicasts (to a pre-specified group of users) to pass through
  - a router may be used to prevent broadcasts and multicasts from travelling through the network

---

**Some facts on LAN (2/2)**

- the workstations, hubs, and repeaters together form a LAN segment
- a LAN segment is also known as a collision domain since collisions remain within the segment
- the area within which broadcasts and multicasts are confined is called a broadcast domain or LAN
  - thus a LAN can consist of one or more LAN segments
- defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together, it means that everyone on a LAN must be located in the same area (see figure on next slide)
What are VLANs?

- VLAN allow a network manager to logically segment a LAN into different broadcast domains (see picture on next slide).
- Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together.
- Users on different floors of the same building, or even in different buildings can now belong to the same LAN.
- VLAN’s also allow broadcast domains to be defined without using routers.
- Bridging software is used instead to define which workstations are to be included in the broadcast domain.
- Routers would only have to be used to communicate between two VLANs.
Advantages of VLAN (1/4)

- **Performance**
  - In networks where traffic consists of a high percentage of broadcasts and multicasts, VLANs can reduce the need to send such traffic to unnecessary destinations.
  - In a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic.
  - The use of VLANs reduces the number of routers needed, since VLANs create broadcast domains using bridges instead of routers.
  - I.e., compared to bridges, routers require more processing of incoming traffic. As the volume of traffic passing through the routers increases, so does the latency in the routers, which results in reduced performance.

Advantages of VLAN (2/4)

- **Formation of Virtual Workgroups**
  - Nowadays, it is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research.
  - These workgroups are usually formed for a short period of time and during this period communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them.
  - With VLANs it is easier to place members of a workgroup together.

Advantages of VLAN (3/4)

- **Simplified Administration:**
  - Seventy percent of network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, re-cabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN, other administrative work can be reduced or eliminated.
  - However, the full power of VLANs will only really be felt when good management tools are created which can allow network managers to drag and drop users into different VLANs or to set up aliases.
  - Despite this saving, VLANs add a layer of administrative complexity, since it now becomes necessary to manage virtual workgroups.

Advantages of VLAN (4/4)

- **Reduced Cost**
  - VLANs can be used to create broadcast domains which eliminate the need for expensive routers.

- **Security**
  - Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data.
  - VLANs can also be used to:
    - Control broadcast domains
    - Set up firewalls
    - Restrict access
    - Inform the network manager of an intrusion.
How VLAN works? (1/2)

* When a LAN bridge receives data from a workstation, it tags the data with a VLAN identifier indicating the VLAN from which the data came. This is called explicit tagging.
* It is also possible to determine to which VLAN the data received belongs using implicit tagging. In implicit tagging the data is not tagged, but the VLAN from which the data came is determined based on other information like the port on which the data arrived. Tagging can be based on the port from which it came, the source Media Access Control (MAC) field, the source network address, or some other field or combination of fields.
* VLAN's are classified based on the method used. To be able to do the tagging of data using any of the methods, the bridge would have to keep an updated database containing a mapping between VLAN's and whichever field is used for tagging. For example, if tagging is by port, the database should indicate which ports belong to which VLAN. This database is called a filtering database.

How VLAN works? (2/2)

* Bridges would have to be able to maintain this database and also to make sure that all the bridges on the LAN have the same information in each of their databases.
* The bridge determines where the data is to go next based on normal LAN operations. Once the bridge determines where the data is to go, it now needs to determine whether the VLAN identifier should be added to the data and sent. If the data is to go to a device that knows about VLAN implementation (VLAN-aware), the VLAN identifier is added to the data. If it is to go to a device that has no knowledge of VLAN implementation (VLAN-unaware), the bridge sends the data without the VLAN identifier.
* In order to understand how VLAN work, we need to look at the types of VLAN, the types of connections between devices on VLAN, the filtering database which is used to send traffic to the correct VLAN, and tagging, a process used to identify the VLAN originating the data.

VLAN standard

* VLAN Standard: IEEE 802.1Q Standard
* standardizes VLAN support over frame-based networks

Types of VLAN

* VLAN membership can be classified by:
  * port
  * MAC address
  * protocol type
Layer 1 VLAN: by port

* Membership in a VLAN can be defined based on the ports that belong to the VLAN
* For example, in a bridge with four ports, ports 1, 2, and 4 belong to VLAN 1 and port 3 belongs to VLAN 2 (see figure)
* The main disadvantage of this method is that it does not allow for user mobility
  If a user moves to a different location away from the assigned bridge, the network manager must reconfigure the VLAN

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Layer 2 VLAN: by MAC address

* Switch tracks the MAC addresses which belong to each VLAN. Since MAC addresses form a part of the workstation's network interface card, when a workstation is moved, no reconfiguration is needed to allow the workstation to remain in the same VLAN. This is unlike Layer 1 VLAN's where membership tables must be reconfigured.
* The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is no easy task. Also, in environments where notebook PC's are used, the MAC address is associated with the docking station and not with the notebook PC. Consequently, when a notebook PC is moved to a different docking station, its VLAN membership must be reconfigured.

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5 : 34...</td>
<td>1</td>
</tr>
<tr>
<td>67 : 00...</td>
<td>1</td>
</tr>
<tr>
<td>B2 : AA...</td>
<td>2</td>
</tr>
<tr>
<td>98 : 46...</td>
<td>1</td>
</tr>
</tbody>
</table>

Layer 2 VLAN: by protocol type

* VLAN membership for Layer 2 VLAN's can also be based on the protocol type field found in the Layer 2 header

<table>
<thead>
<tr>
<th>Protocol</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>1</td>
</tr>
<tr>
<td>IPX</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Layer 3 VLAN: by IP subnet addr.

* Membership is based on the Layer 3 header. The network IP subnet address can be used to classify VLAN membership;
* Although VLAN membership is based on Layer 3 information, this has nothing to do with network routing and should not be confused with router functions. In this method, IP addresses are used only as a mapping to determine membership in VLAN's. No other processing of IP addresses is done.
* In Layer 3 VLAN’s, users can move their workstations without reconfiguring their network addresses. The only problem is that it generally takes longer to forward packets using Layer 3 information than using MAC addresses.

<table>
<thead>
<tr>
<th>IP subnet</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.2.24</td>
<td>1</td>
</tr>
<tr>
<td>26.21.3</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
**Higher Layer VLAN**

- It is also possible to define VLAN membership based on applications or service, or any combination thereof. For example, file transfer protocol (FTP) applications can be executed on one VLAN and telnet applications on another VLAN.
- The 802.1Q standard defines Layer 1 and Layer 2 VLAN’s only. Protocol type based VLAN’s and higher layer VLAN’s have been allowed for, but are not defined in this standard. As a result, these VLAN’s will remain proprietary.

**Types of connections**

- Devices on a VLAN can be connected in three ways based on whether the connected devices are VLAN-aware or VLAN-unaware.
- A VLAN-aware device is one which understands VLAN memberships (i.e. which users belong to a VLAN) and VLAN formats.

**Trunk link**

- All the devices connected to a trunk link, including workstations, must be VLAN-aware.
- All frames on a trunk link must have a special header attached. These special frames are called tagged frames.

**Access link**

- An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged).
- The VLAN-unaware device can be a LAN segment with VLAN-unaware workstations or it can be a number of LAN segments containing VLAN-unaware devices (legacy LAN).
Hybrid link

- This is a combination of the previous two links. This is a link where both VLAN-aware and VLAN-unaware devices are attached.
- A hybrid link can have both tagged and untagged frames, but all the frames for a specific VLAN must be either tagged or untagged.
- It must also be noted that the network can have a combination of all three types of links.

Frame processing

- Bridge keeps track of VLAN members:
  - By using of filtering database which it uses to determine where the data is to be sent.
- Bridge on receiving data determines to which VLAN the data belongs:
  - By using of tagging.

Filtering database / Static entries

- Membership information for a VLAN is stored in a filtering database. The filtering database consists of the following types of entries:

  Static Entries:
  - Static information is added, modified, and deleted by management only. Entries are not automatically removed after some time (ageing), but must be explicitly removed by management. There are two types of static entries:
    - Static Filtering Entries: which specify for every port whether frames to be sent to a specific MAC address or group address and on a specific VLAN should be forwarded or discarded, or should follow the dynamic entry, and
    - Static Registration Entries: which specify whether frames to be sent to a specific VLAN are to be tagged or untagged and which ports are registered for that VLAN.

Filtering dbase / Dynamic entries

- Dynamic Entries:
  - Are learned by the bridge and cannot be created or updated by management. The learning process observes the port from which a frame, with a given source address and VLAN ID (VID), is received, and updates the filtering database. The entry is updated only if all the following three conditions are satisfied:
    - This port allows learning;
    - The source address is a workstation address and not a group address;
    - There is space available in the database;
Filtering database / Dynamic entries

Entries are removed from the database after a certain amount of time specified by management is expired, entries allow automatic reconfiguration of the filtering database if the topology of the network changes. There are three types of dynamic entries:

- Dynamic Filtering Entries: which specify whether frames to be sent to a specific MAC address and on a certain VLAN should be forwarded or discarded;
- Group Registration Entries: which indicate for each port whether frames to be sent to a group MAC address and on a certain VLAN should be filtered or discarded. These entries are added and deleted using Group Multicast Registration Protocol (GMRP). This allows multicasts to be sent on a single VLAN without affecting other VLAN's;
- Dynamic Registration Entries: which specify which ports are registered for a specific VLAN. Entries are added and deleted using GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol.

Dynamic entries / GVRP

GVRP is used not only to update dynamic registration entries, but also to communicate the information to other VLAN-aware bridges.

In order for VLAN's to forward information to the correct destination, all the bridges in the VLAN should contain the same information in their respective filtering databases. GVRP allows both VLAN-aware workstations and bridges to issue and revoke VLAN memberships. VLAN-aware bridges register and propagate VLAN membership to all ports that are a part of the active topology of the VLAN. The active topology of a network is determined when the bridges are turned on or when a change in the state of the current topology is perceived.

Summary on VLAN

There are significant advances in the field of networks in the form of VLAN's which allow the formation of virtual workgroups, better security, improved performance, simplified administration, and reduced costs;

- VLAN's are formed by the logical segmentation of a network and can be classified into Layer1, 2, 3 and higher layers;
- only Layer 1 and 2 are specified in the draft standard 802.1Q;
- tagging and the filtering database allow a bridge to determine the source and destination VLAN for received data;
- VLAN's if implemented effectively, show considerable promise in future networking solutions.

ATM VLANs

Manufacturers currently implementing the ATM Forum's LAN emulation (LANE) standard to configure VLANs within ATM switching networks;

- this standard preserves the functionality of configured LANs (Ethernet, Token Ring, FDDI) across an ATM network;
- ATM networks appear as a single transparent connectionless broadcast to end devices that reside on shared LANs, and are called emulated LANs (ELANs).
LAN and ATM

- A key to ATM success will be the ability to allow for interoperability between LAN technologies and ATM;
- Few users will tolerate the presence of islands of ATM without connectivity to the remainder of the enterprise network;
- The key to such connectivity is the use of the same network layer protocols, such as IP and IPX, on both existing networks and on ATM, since it is the function of the network layer to provide a uniform network view to higher level protocols and applications;
- Two fundamentally different ways of running network layer protocols across an (overlay mode) ATM network (see figure on next slide):
  - Native mode operation: address resolution mechanisms are used to map network layer addresses directly into ATM addresses, and the network layer packets are then carried across the ATM network;
  - LAN emulation (LANE).

LANE basics

- The function of the LANE protocol is to emulate a local area network on top of an ATM network;
- Specifically, the LANE protocol defines mechanisms for emulating existing LAN networks such as IEEE 802.3 Ethernet or other;
- Main idea of LANE functioning:
  - Protocol defines a service interface for higher layer (that is, network layer) protocols, which is identical to that of existing LANs, and that data sent across the ATM network are encapsulated in the appropriate LAN MAC packet format;
  - It does not mean that any attempt is made to emulate the actual media access control protocol of the specific LAN concerned (that is, CSMA/CD for Ethernet or token passing for 802.5).
- In other words, the LANE protocols make an ATM network look and behave like for example an Ethernet or Token Ring LAN, but LANE operating much faster than a real such network.
**LANE specifics**

- with implementation of LANE it requires no modifications to higher layer protocols to enable their operation over an ATM network;
- since the LANE service presents the same service interface of existing MAC protocols to network layer drivers, no changes are required in those drivers;
- LANE does not directly impact ATM switches;
- LANE protocols operate transparently over and through ATM switches, using only standard ATM signaling procedures;
- ATM switches may well be used as convenient platforms upon which to implement some of the LANE server components;
- logical decoupling is one of the great advantages of the overlay model, since they allow ATM switch designs to proceed independently of the operation of overlying internetworking protocols, and vice versa.

**LANE protocol architecture**

- the basic function of the LANE protocol is to resolve MAC addresses into ATM addresses;
- by doing so, it actually implements a protocol for MAC bridging on ATM, hence the close fit with current LAN switches;
- the goal of LANE is to perform such address mappings so that LANE end systems can set up direct connections between themselves and forward data.

**LANE components**

- the LANE protocol defines the operation of a single emulated LAN (ELAN);
- multiple ELANs may coexist simultaneously on a single ATM network since ATM connections do not "collide";
- a single ELAN emulates existing LAN standard, and consists of the following entities:
  - LAN Emulation Client (LEC);
  - LAN Emulation Server (LES);
  - Broadcast and Unknown Server (BUS);
  - LAN Emulation Configuration Server (LECS);
  - Selective Multicast Server (SMS).

**LAN Emulation Client**

- LAN Emulation Client (LEC): a LEC is the entity in an end system that performs:
  - data forwarding;
  - address resolution;
  - other control functions for a single end-system within a single ELAN;
- a LEC also provides a standard LAN service interface to any higher layer entity that interfaces to the LEC;
- an ATM NIC (Network Interface Card) or LAN switch interfacing to an ELAN supports a single LEC for each ELAN to which they are connected;
- end-system that connects to multiple ELANs (perhaps over the same UNI) will have one LEC per ELAN.
- each LEC is identified by a unique ATM address, and is associated with one or more MAC addresses reachable through that ATM address;
- the LEC would be associated with all the MAC addresses reachable through the ports of that LAN switch which are assigned to the particular ELAN;
- this set of addresses may change, both as MAC nodes come up and down, and as particular paths are reconfigured by logical or physical changes in the LAN network topology (e.g. through the use of a spanning tree protocol, for instance).
**LES, BUS**

- LAN Emulation Server (LES) implements the control function for a particular ELAN;
- there is only one logical LES per ELAN, and to belong to a particular ELAN means to have a control relationship with that ELAN's particular LES;
- each LES is identified by a unique ATM address.
- the Broadcast and Unknown Server (BUS) is a multicast server that is used to flood unknown destination address traffic and forward multicast and broadcast traffic to clients within a particular ELAN.
- the BUS to which a LEC connects is identified by a unique ATM address. In the LES, this is associated with the broadcast MAC address ("all ones"), and this mapping is normally configured into the LES.

**LECS and SMS**

- LAN Emulation Configuration Server (LECS) is an entity that assigns individual LANE clients to particular ELANs by directing them to the LES that correspond to the ELAN. There is logically one LECS per administrative domain, and this serves all ELANs within that domain;
- Selective Multicast Server (SMS) are designed for the single purpose of efficiency forwarding multicast frames;
- SMSs may be used to offload much of the multicast processing from the BUSs, which also have to be forward broadcast frames and frames for unresolved LAN destinations.

**Interfaces**

- the LANE protocol does not specify where any of the server components described here should be located; any device or devices with ATM connectivity would suffice, but for the purposes of reliability and performance, however, it is likely that most vendors will implement these server components on networking equipment, such as ATM switches or routers, rather than on a workstation or host.
- the LANE protocol specifies the operation of the LAN Emulation User to Network Interface (LUNI) between a LEC and the network providing the LANE service and LAN Emulation NNI (LNNI) interface, which operates between the server components within a single ELAN system.

**LNNI and LUNI protocols**

[Diagram showing the relationships between LECS, LES, BUS, SMS, and LEC clients]
**LANE’s entities communications**

- LANE entities communicate with each other using a series of ATM connections.
- LECs maintain separate connections for:
  - control traffic
  - data transmission.

**LANE control connections**

- Configuration Direct VCC: bi-directional point-to-point VCC set up by the LEC (or other entity) to the LECS;
- Control Direct VCC: bi-directional point-to-point VCC set up by the LEC to the LES for sending control traffic;
- Control Distribute VCC: unidirectional VCC set up from the LES back to the LEC; this is typically a point-to-multipoint connection.

**LANE data connections**

- Data Direct VCC: bi-directional point-to-point VCC set up between two LECs that want to exchange data. Two LECs will typically use the same data direct VCC to carry all packets between them, rather than opening a new VCC for each MAC address pair between them, so as to conserve connection resources and connection set-up latency;
- Multicast Send VCC: bi-directional point-to-point VCC set up by the LEC to the BUS;
- Multicast Forward VCC: unidirectional VCC set up from the BUS, this is typically a point-to-multipoint connection, with each LEC as a leaf.

**LANE operation**

- initialization and configuration:
  - LEC must obtain ATM address;
  - establishing of Configuration direct VCC between LEC and LECS;
  - other;
- joining:
  - LEC establishes its control connection to the LES;
  - once joining has been completed successfully, the LEC has been assigned a unique LEC identifier (LECID), knows the emulated LAN’s features (type of LAN, etc.)
- initial registration:
  - LEC may register any number of unicast or multicast destinations;
  - allows LEC to verify uniqueness of its local addresses and before completing initialization and becoming operational;
- connection to BUS:
  - ATM address determination of the BUS.
**LANE v1 and LANE v2**

- **LANE v1:**
  - No LNNI support;
  - No SMS support;
  - No QoS support;
  - Supports only non-multiplexed VCCs;
  - Etc.

- **LANE v2:**
  - Increased scalability;
  - Enhanced and improved broadcasting and multicasting;
  - Supporting of MPOA (Multi-Protocol Over ATM);
  - Interoperability between v1 and v2:
    - Supported.

**Quality of Service, LANE v2**

- LANE v2 allows QoS sets (or types) to be locally defined per LEC;
- Each QoS set defines a set of call setup;
- Up to 8 levels of QoS;
- Each Data Direct VCC is established using the parameters corresponding to one of the QoS sets;
- Client minimally has a single QoS set corresponding to the default parameters for LANE UBR connections;
- A LANE v2 LEC always has at least a UBR QoS set and, if supported, an ABR QoS set, one of which will be used for frames requiring the default QoS and frames passed down with no QoS;
- Received frames are not associated with a QoS Set.

**LANE and VLANs**

- LANE is used by vendors to provide a VLAN service on ATM backbones;
- Higher capacity;
- Superior allocation and management of network capacity;
- Easier management of the constantly changing LAN membership;
- Access to multiple VLANs from the same physical interface;
- Ease of evolution to new applications.

**WLAN – basic info**

- A wireless local area network (LAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN
- Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections
- Today wireless LANs are more widely recognized as a general-purpose connectivity alternative for a broad range of business customers
- Currently WLAN IEEE 802.11b mostly is under implementation
Advantages of WLAN (1/2)

- **Mobility:**
  - Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization;
  - mobility supports productivity and service opportunities not possible with wired networks;

- **Installation Speed and Simplicity:**
  - Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings;

- **Installation Flexibility:**
  - Wireless technology allows the network to go where wire cannot go;

- **Reduced Cost-of-Ownership:**
  - While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower;
  - Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes;

Advantages of WLAN (2/2)

- **Scalability:**
  - Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations;
  - Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area;

Issues of WLAN

- **Error rate:**
  - For wired LAN, errors are relatively rare, for radio, error rate is much higher;
  - Noise, multipath (see next slide), attenuation, spread spectrum interference, etc are all common causes for errors in wireless environment;

- **Security:**
  - Radio waves are not confined at the boundary of building or campus, there exists the possibility for eavesdropping and intentional interference;

- **Interference:**
  - In wired LAN, the only machines you hear are the ones connected to the network. In a wireless LAN you may hear other networks, as well as cordless phones, microwave ovens, etc. Any of these can interfere with your transmission of data;

- **Power conservation:**
  - Wireless LANs are typically related to mobile applications, and in this type of applications battery power is a scare resource.

Multipath interference
ISM bands

- Wireless LANs are typically designed to operate in Instrumentation, Scientific, Medical (ISM) radio bands.
- Federal Communications Commission (FCC) in USA governs radio transmission, but FCC does not require the end-user to purchase license to use the ISM bands.
- ISM bands include 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, and 5.725-5.875 GHz.

IEEE 802.11 basics

- In June 1997, the IEEE 802.11 Working Group ratified a standard for WLANs operating at a maximum speed of 2 Mbps.
- This standard was lacking in many areas, resulting in no guarantee of interoperability.
- This resulted in all of the major WLAN manufacturers working together with the University of New Hampshire Interoperability Lab to ensure that products are interoperable across multiple vendor platforms.
- The IEEE 802.11 Working Group is now concentrating its efforts on producing standards for high-speed WLAN.
- High-speed PHY extension in the 2.4 GHz band was developed [IEEE 802.11b] with the current maximum throughput being 11 Mbps.

IEEE 802.11 reference model

- Physical Layer Convergence Procedure (PLCP) Sublayer;
- PLCP adapts the capabilities of the physical medium dependent system to the Physical Layer service;
- PLCP defines a method of mapping the 802.11 PHY sublayer Service Data Units (PSDU) into a framing format suitable for sending and receiving user data and management information between two or more stations using the associated physical medium dependent system. This allows 802.11 MAC to operate with minimum dependence on the PMD sublayer.
- Physical Media Dependent (PMD) Sublayer.
- PMD defines the characteristics and method of transmitting and receiving data through a wireless medium between two or more stations each using the same modulation system.

MAC Layer: CSMA/CA

- IEEE 802.11 use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to access medium;
- The basic idea of CSMA/CA is:
  - if a station wants to transmit, it first senses the medium;
  - if the medium is busy, the state defers its transmission to a later time;
  - otherwise, it is allowed to use the medium;
  - because of the Hidden Node Problem, collision could occur: on the next slide, if both station A and C try to send data to station B at the same time, collision will occur.
- To avoid collisions, a RTS/CTS mechanism is implemented:
  - when a station gets the chance to send, it sends a short message first: Ready To Send (RTS);
  - the destination returns a Clear To Send (CTS) message;
  - after that, the source station can begin to send the data;
  - since collisions may not be detected by source station, the destination will ACK every packet.
Hidden Node Problem

Topolog

IEEE 802.11 has two different network topologies:

- ad-hoc and infrastructure: every station can communicate with any other station. There is no structure to the network;
- infrastructure configuration, there are some fixed points called Access Point (AP). A group of stations using the same radio frequency is called Basic Service Set (BSS). The mobile stations communicate through the AP.

HIPERLAN

European Telecommunications Standards Institute (ETSI) is one of the world's recognized Standards bodies

HIPERLAN was developed by ETSI, whose goal was to achieve higher data rate than IEEE 802.11 data rates

HIPERLAN includes a family of four standards

- HiperLAN type 1
- HiperLAN type 2
- HiperAccess (HiperLAN type 3)
- HiperLINK (HiperLAN type 4)

HIPERLAN: family of standards

<table>
<thead>
<tr>
<th>Application</th>
<th>HiperLAN type 1</th>
<th>HiperLAN type 2</th>
<th>Hiper Access</th>
<th>HiperLink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>5 GHz</td>
<td>5 GHz</td>
<td>5 GHz</td>
<td>17 GHz</td>
</tr>
<tr>
<td>Data Rate</td>
<td>23.5 Mbps</td>
<td>20 Mbps</td>
<td>20 Mbps</td>
<td>155 Mbps</td>
</tr>
</tbody>
</table>