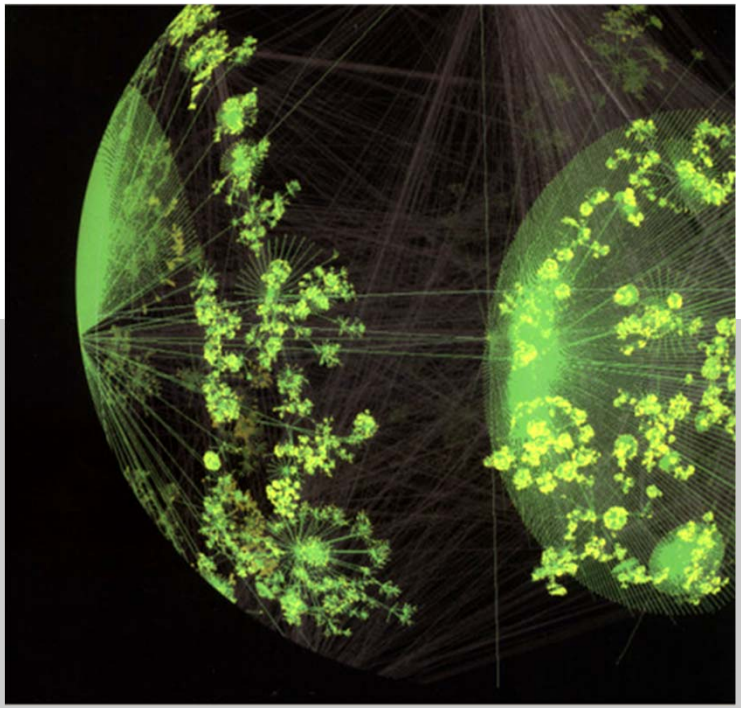


Chapter 7
Multicast and Real-Time Service

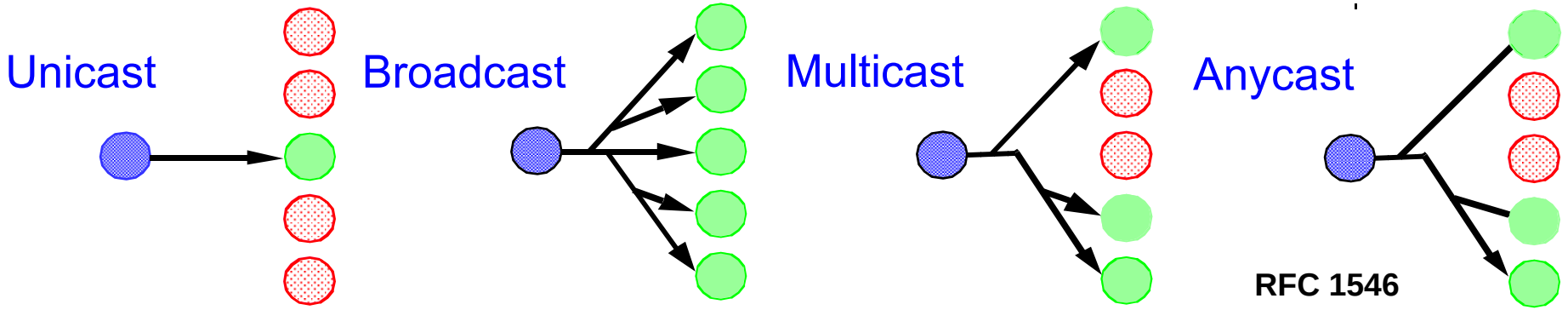
TCP/IP Essentials

A Lab-Based Approach

Spring 2017

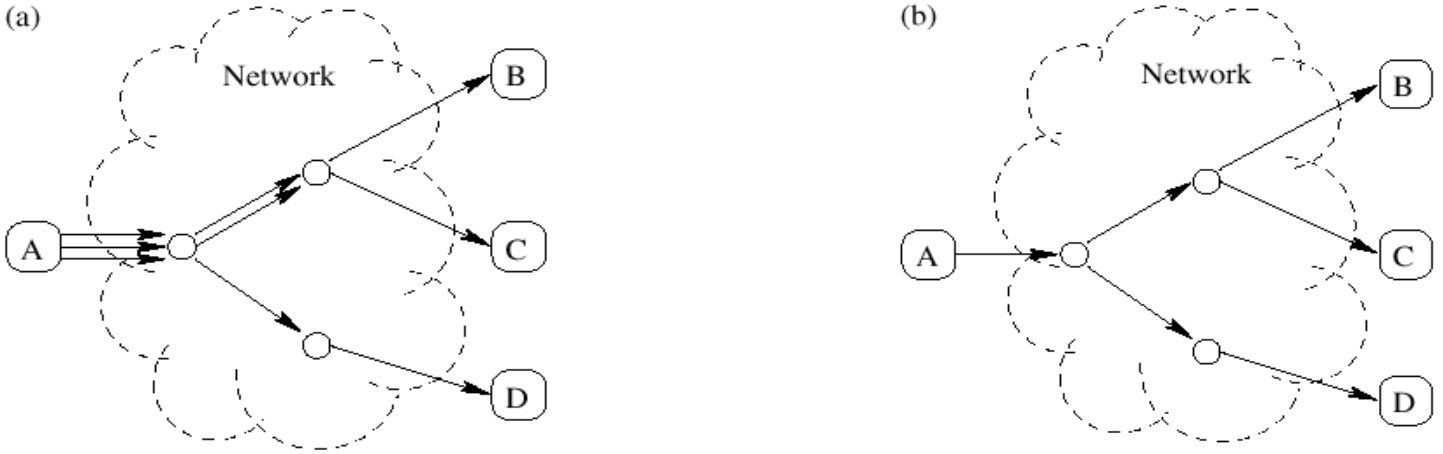
Multicast

- Multicasting is one-to-many or many-to-many communications.
- A simple implementation of multicasting can be built on top of the unicast (point to point) service …
  - Each multicast source send N-1 copies for total N members in the multicast group that leads to an inefficient N^2 problem
  - But in the desired case a packet should be transmitted on one link exactly once (for the least packet replication in network)
- IP Multicasting uses less network resources.
- IP supports multicasting via the help of IGMP and additional routing protocols.



IP Unicast and Multicast

When A wants to send a packet to B, C and D



- Unicast
  - A sends three copies of the packet, each to a different address.
  - Each copy may take a different path.
  - For a group of N nodes, N(N-1)/2 paths are needed.
- Multicast
  - A sends one copy of the packet to a group address.
  - The packet will be forwarded in a multicast tree to B, C and D.
  - Less network resources are used.

IP Multicast Supported Services

- DNS multicast query: provides a way to locate nearby domain name servers without knowing their IP addresses. The Recursion Desired bit should not be set in order to avoid excessive load on both network and DNS servers.
- RIPv2 multicast RIP messages only to RIP routers (224.0.0.9) instead of to all routers in RIPv1.
- SNMP implementation can use multicast to support group communication between managers and broker agents.
- ICMP router solicitation and router advertisement: a host can multicast an ICMP router solicitation massage to all routers in this subnet (specified by 224.0.0.2) after bootstrapping to build its routing table.
- IP Multimedia Streaming for video teleconferencing, Internet audio, IPTV, and video streaming.

IP Multicasting Key Components

- Multicast group management
  - The multicast group is dynamic, meaning that users may join and leave the group during the multicast session.
  - A multicast router needs to keep track of the memberships of all the multicast groups.
  - A participant may want to know who else is in the group.
- Multicast addressing
  - Define a common group IP address for all nodes in each multicast group.
  - Map a multicast group IP address to a MAC address of layer 2 network
- Multicast routing
  - Find and maintain a multicast tree from one participating node to all other nodes in the group.
  - The tree should be updated when
    - > The network topology changes, or
    - > The group membership changes.

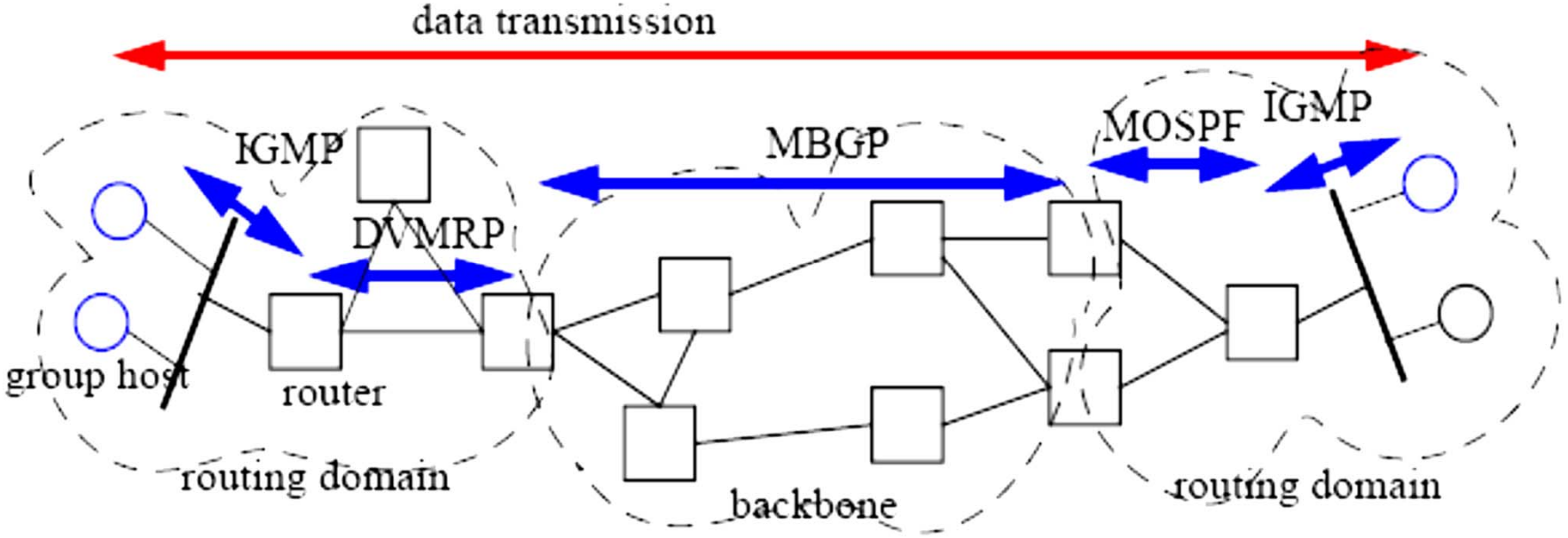
Semantics of IP Multicast

- A multicast group consists of a number of participating hosts.
- Multicast groups are identified by a class D IP address.
  - Leading bits: 1110 → 224.0.0.0 l – 239.255.255.255
- Hosts (more precisely: interfaces) can join and leave a multicast group dynamically.
- Every IP datagram sent to a multicast group is transmitted to all members of the group.

Hierarchical Levels of IP Multicast Routing

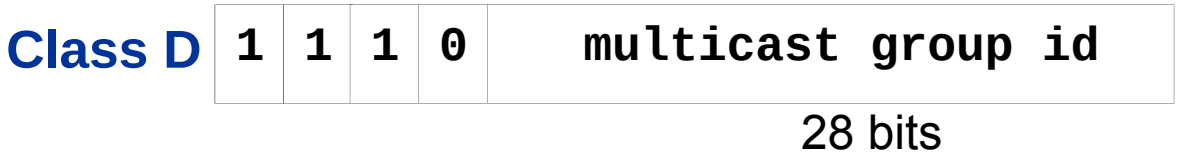
Three multicast routing levels:

- IGMP protocol monitors group existence on the local subnet; IGMP messages are sent between each multicast router and its served group hosts
- Interior multicasting protocols, e.g. DVMRP or MOSPF, manage routing data sent between routers within a routing domain.
- Exterior multicasting protocols, e.g. MBGP, manage routing data sent between routers into the backbone domain.



IP Multicast Addressing

- Desired properties of multicast group addressing
  - Decouple group from group members
  - Dynamic group members for a well-known group
- All Class D addresses are designated as multicast IP addresses
  - Receiving: members of a multicast group receive every multicast packets with the group multicast address.
  - Sending: any host can send a multicast packet to a group, no need to belong to the group.



Class	From	To
D	224 .0.0.0	239 .255.255.255

Reserved Multicast Addresses

Examples of reserved IP multicast addresses:

224.0.0.1	All systems in this subnet
224.0.0.2	All routers in this subnet
224.0.0.4	All Distance Vector Multicast Routing Protocol (DVMRP) routers in this subnet
224.0.0.5	All Multicast Extension to OSPF (MOSPF) routers in this subnet
224.0.0.9	Used for RIP-2
224.0.0.13	All Protocol Independent Multicast (PIM) routers in this subnet
224.0.1.1	Used for Network Time Protocol (NTP)

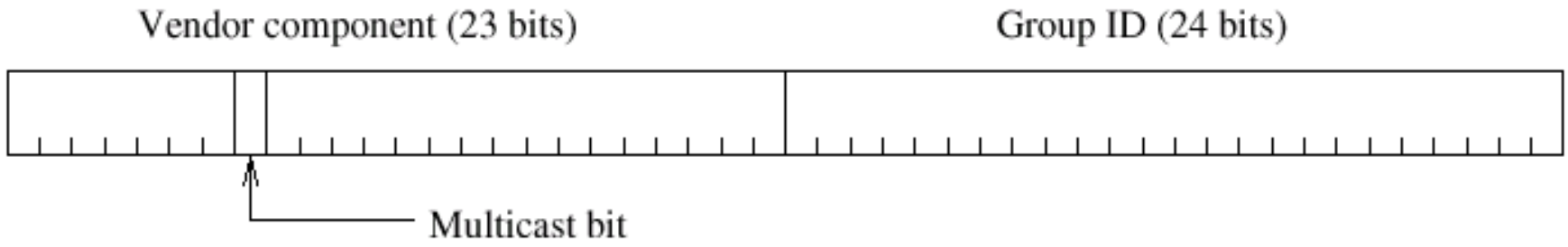
Ethernet Multicast Address

A 48-bit long Ethernet address consists of

- A 23-bit vendor component
- A 24-bit group identifier: assigned by vendor
- A multicast bit: set if the address is an Ethernet multicast address.

An example

- The vendor component of Cisco is 0x00-00-0C.
- Then the multicast Ethernet address used by Cisco made hardware starts with 0x01-00-0C.



Ethernet Multicast Address (cont'd)

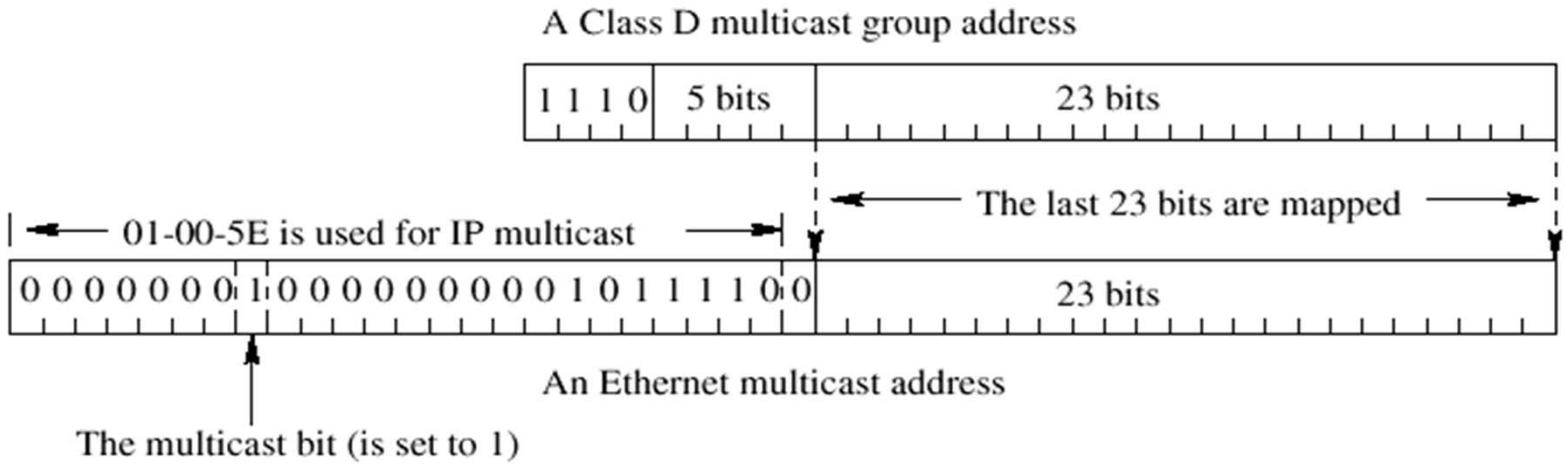
- Ethernet frames with a value of 1 in the least-significant bit of the first octet are flooded
- Ethernet switch generally does not distinguish between multicast and broadcast frames
- Some multicast Ethernet frames may be treated differently, e.g.
  - Dropped by a filter to reduce CPU load
  - Processed when encapsulated with layer-2 control protocol messages

Some well known Ethernet multicast addresses:

Address	Type Field	Usage
FF-FF-FF-FF-FF-FF	Various	Broadcast
01-80-C2-00-00-00	0x0802	IEEE 802.1D Spanning Tree Protocol
01-80-C2-00-00-08	0x0802	IEEE 802.1AD Q-in-Q Spanning Tree Protocol
01-00-0C-CC-CC-CC	0x0802	Cisco Discovery Protocol (CDP)
01-00-5E-xx-xx-xx	0x0800	IPv4 Multicast
33-33-xx-xx-xx-xx	0x86DD	IPv6 Multicast

Multicast Address Mapping: IP ←→ Ethernet

- Ethernet addresses corresponding to IP multicasting are in the range of 01:00:5e:00:00:00 to 01:00:5e:7f:ff:ff.
- At the sender, a multicast destination IP address is directly mapped to an Ethernet multicast address.
  - No need for ARP request and reply
  - Only the last 23 bits of the IP address is mapped into the multicast MAC address.
- Ethernet frames with multicast MAC address are often broadcasted.



Multicast Address Mapping (cont'd)

- Mapping procedure is not unique
  - Only 23 bits of an IP multicast address are mapped into the Ethernet multicast address.
  - 2^5 = 32 Class D IP addresses will map to the same multicast Ethernet address (since there are 5 bits ignored)
  - Example:

    224.128.64.32 (hex: e0.80.40.20)

    and

    224.0.64.32 (hex: e0:00:40:20)

    both map to an Ethernet multicast address

    01:00:5e:00:40:20.
- Ethernet device driver or IP module may need to perform packet filtering since the interface card may receive multicast frames in which the host is really not interested.

Multicast Address Mapping at the Receiver

A router interface should then be able to receive all the multicast IP datagrams.

At the receiver

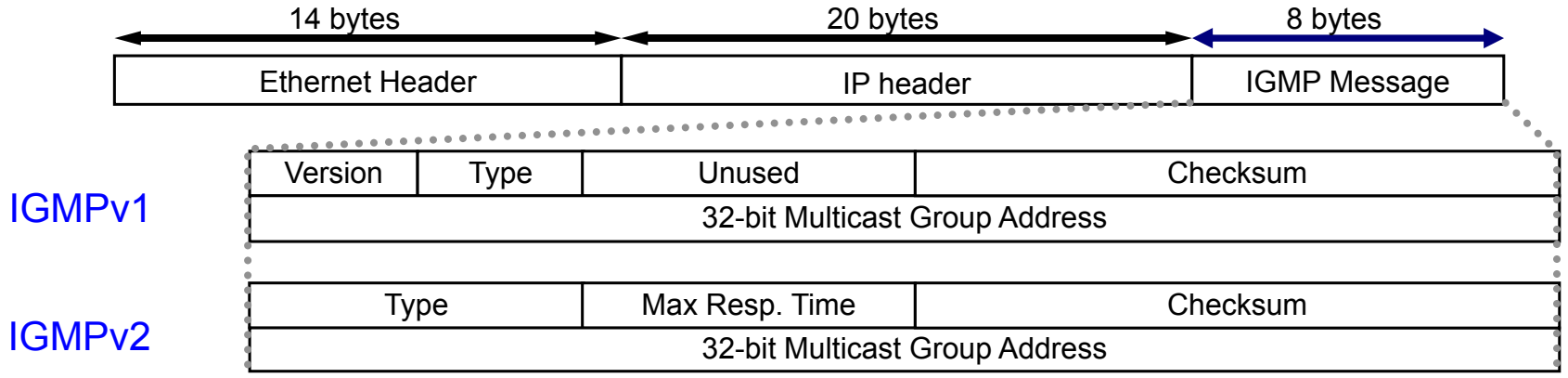
- The upper layer protocol should be able to ask the IP module to join or leave a multicast group.
- The IP module maintains a list of group memberships, which is updated when an upper layer process joins or leaves a group.
- The network interface should be able to join or leave a multicast group.
  - > When a network interface joins a new group, its reception filters are modified to enable reception of multicast Ethernet frames belonging to the group.

Internet Group Management Protocol (IGMP)

- IGMP is used by multicast routers to keep track of membership in a multicast group.
- Support for:
  - Joining a multicast group
  - Query membership
  - Send membership reports
- IGMP is originally defined in RFC1112, then RFC2236, RFC4604 define IGMPv2, IGMPv3 respectively
- RFC4604 also specifies Multicast Listener Discovery Protocol version2 (MLDv2) for IPv6 hosts – providing similar functionality as IGMPv3

IGMP Packet Format and Revisions

- IGMP messages are carried in IP datagrams with protocol number 2.
- IGMPv1 and IGMPv2 messages are only 8 bytes long
- IGMP Type field:
  - 0x11 for membership query with IGMPv2, and IGMPv1 – backward-compatibility
  - 0x12 for version 1 membership report to maintain backward-compatibility with IGMPv1
  - 0x16 for version 2 membership report
  - 0x17 for leaving the group introduced by IGMPv2
  - 0x22 for version 3 membership query
- Max Response Time: applicable only to membership query messages, specifying the maximum allowed time before sending report message in units of 1/10 sec.



IGMP Packet Format and Revisions (cont'd)

- IGMPv3 major revision: allows hosts to specify a list of hosts from which they want to receive traffic from. Traffic from other hosts is then blocked.
- Three type of queries
  - General Query: Group address set to 0 when sent; group address is specified when replied
  - Group-Specific Query: Group address set to the address being queried – introduced by IGMPv2
  - Group-and-Source-Specific Query: Both group address and source address(es) being queried are specified – introduced by IGMPv3

IGMPv3 membership query message

Type = 0x11			Max Resp Time	Checksum
Group Address				
Resv = 0	S	QRV	QQIC	Number of Sources (N)
Source (unicast) Address [1]				
Source (unicast) Address [2]				
… …				
Source (unicast) Address [N]				

IGMP General Multicast Group Management

- Multicast router periodically send host membership queries to discover which multicast groups have members on their attached local networks.
  - By default, the queries are sent at 60 second intervals.
  - Queries are sent to the class D address 224.0.0.1 (all host in the subnet) with a TTL of 1.
  - A general query use 0.0.0.0 as the Group Address for all multicast groups
- Multicast router maintains a multicast group membership table.
  - The table records which groups have members in the local networks attached to each interface of the router.
  - The router uses the table to decide which ports to forward a multicast datagram to.

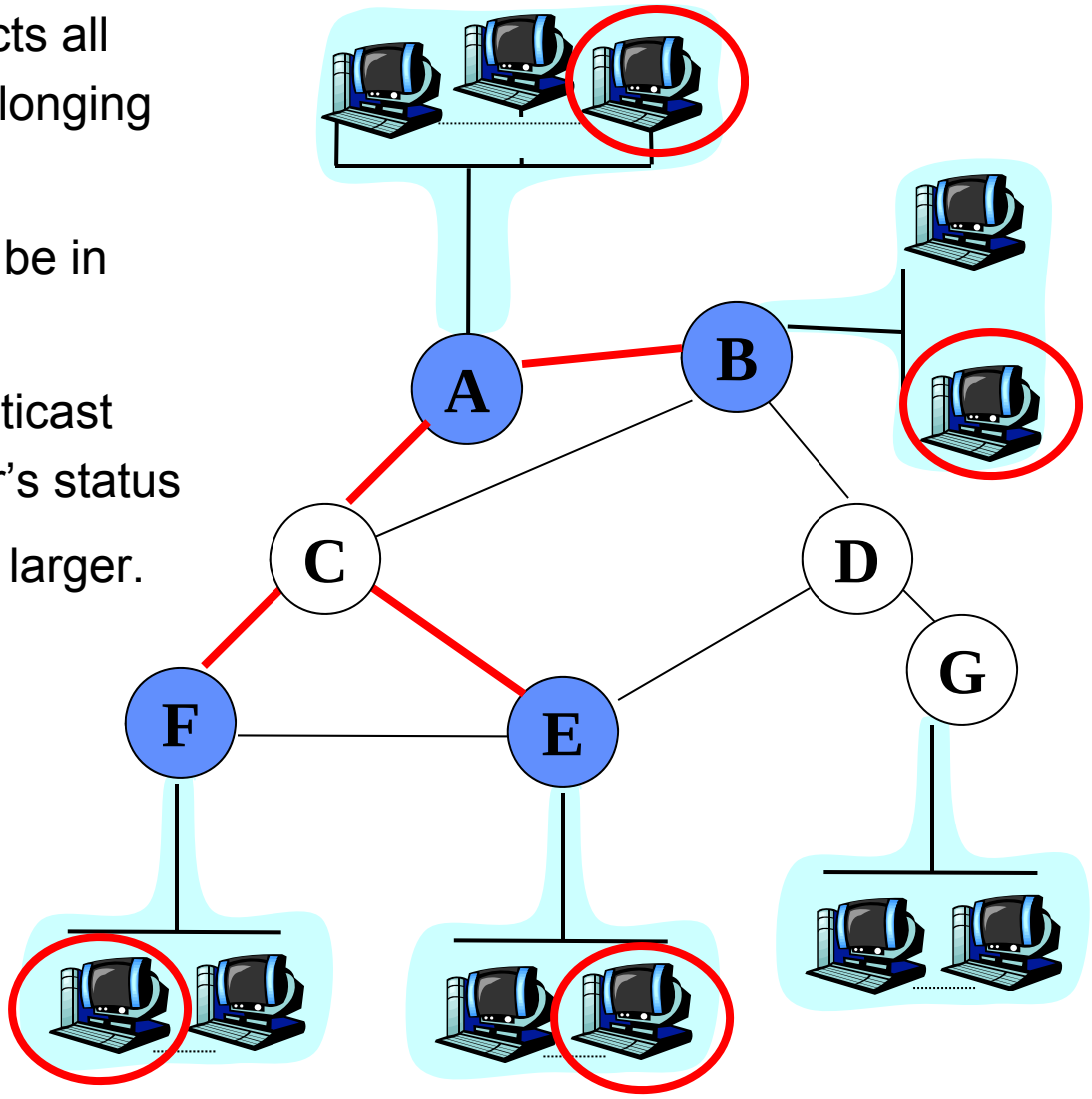
IGMP General Multicast Group Management (cont'd)

- A host responds to a IGMP query with one IGMP report for each multicast group in which it is a member.
  - The destination IP address is identical to the multicast group it is reporting on.
  - In order to avoid a flood of reports, a host can delay an IGMP report for a random amount of time. If it overhears a report reporting on the same group address, it cancels the report.
- When a host leaves a multicast group
  - It does nothing in IGMPv1. Its membership record at the router will expire and be removed.
  - In later versions of IGMP, it may report to all routers (with Type value of 0x17).

IP Multicast Routing

Goal: find a tree of links that connects all routers that have attached hosts belonging to a multicast group

- The participants in a group could be in different geographical locations.
- A host can join and leave the multicast session at will → impact its router's status
- The size of a group could be 1 or larger.



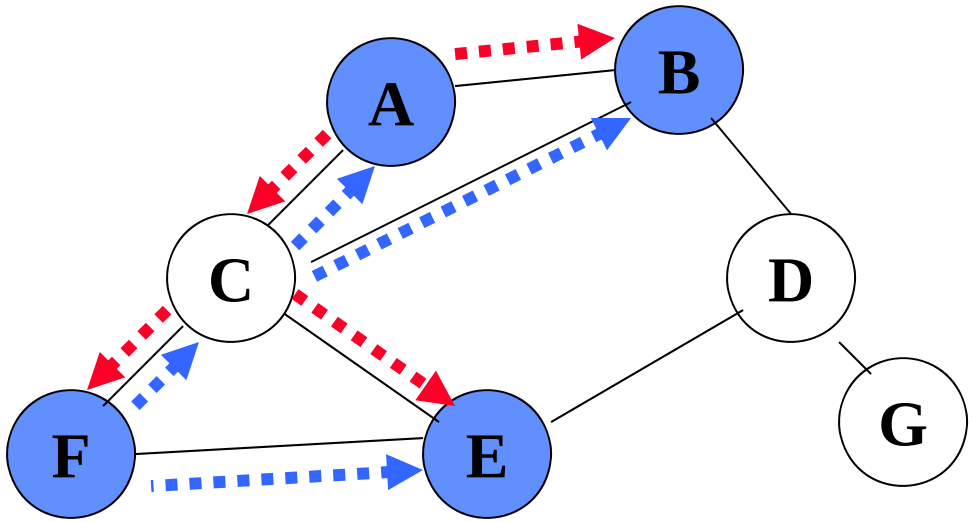
LEGEND

Multicast router with attached group member

Multicast router with no attached group member

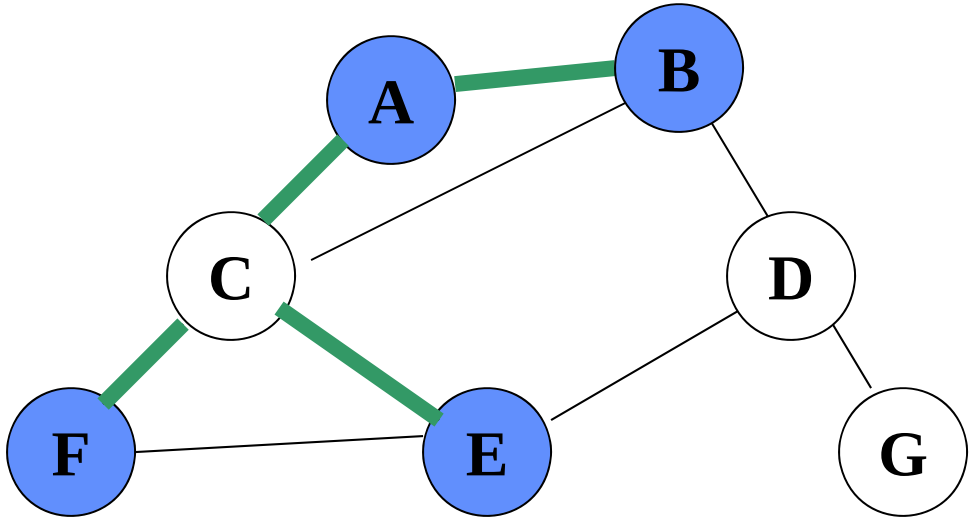
Source-Based Tree

- An individual routing tree is constructed for each sender in the multicast group
- In a multicast group with N hosts, N different routing trees will be constructed for each sender in the multicast group



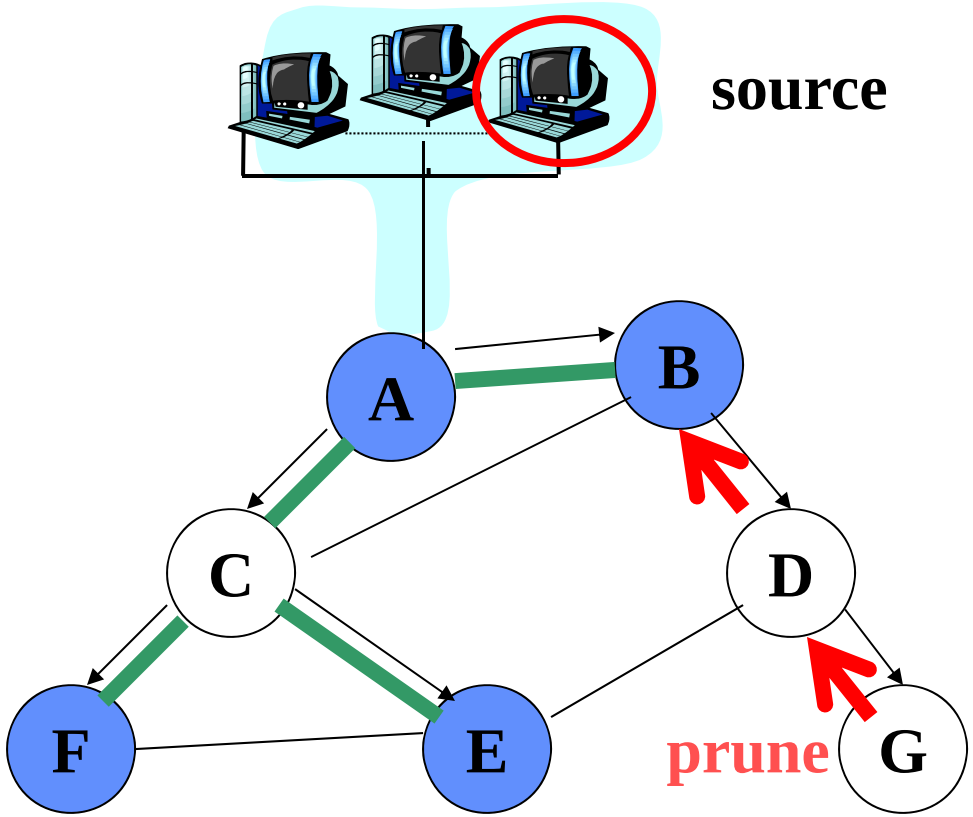
Group-Shared Tree

- A single routing tree is constructed for the entire multicast group



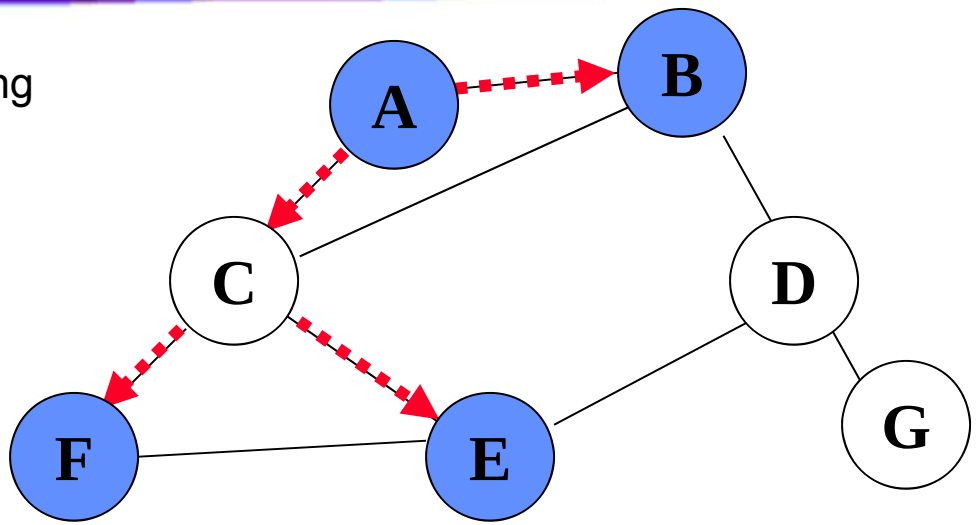
Multicast Tree Pruning

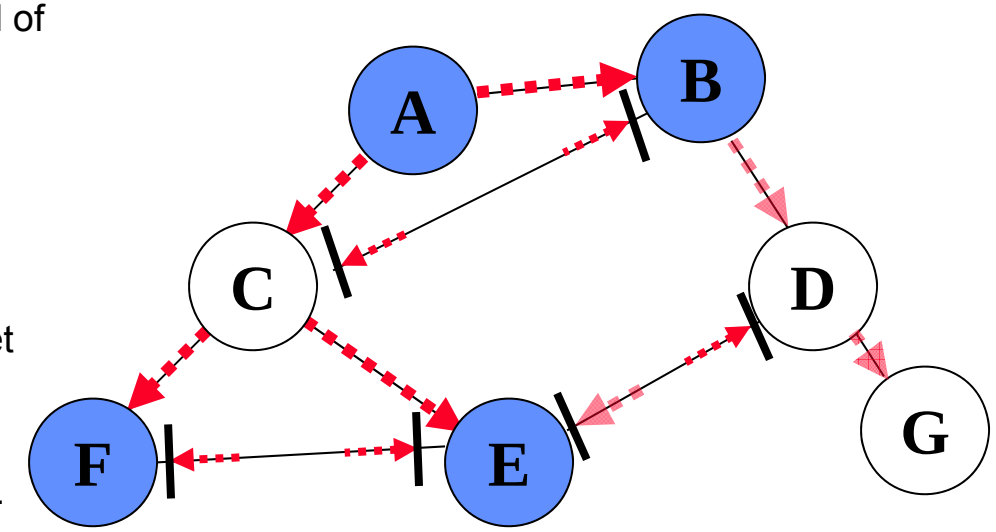
- When a router receives unwanted multicast packets and has no attached hosts joined to that multicast group will send a prune message to its upstream router
- If a router receives a prune message from one of its downstream routers
  - It stop forward multicast packets of the multicast group
  - It can forward a prune message upstream if it also has no attached hosts jointed to that multicast group



Implementing Source-Based Tree

- Shortest Path Tree: use multicast forwarding to send the traffic away from the source towards all receivers
  - Dijkstra's algorithm
- Use Reverse Path Forwarding (RPF)
  - When a router receives a multicast packet with a given address, it transmits the packet on all of its outgoing links (except the one on which it was received) only if the RPF check (see below) is successful.
  - RPF check gets passed if the received packet arrived from the link/port that is on its routing table for the unicast route back to the sender.





Two types of multicast routing protocols

- Source-tree based protocols
  - Facilitate a more even distribution of the multicast traffic
  - Multicast datagrams from a source are distributed in the shortest path tree, resulting in a better delay performance
  - Each multicast router has to maintain state for all sources in all the multicast groups. Too costly for a large number of multicast sessions.
- Shared-tree based protocols
  - Use a shared tree for all the sources in a multicast group. Greatly reduce the number of states in the routers
  - Has the traffic concentration problem
  - The shared tree may not be optimal for all the sources, resulting in larger delay and jitter.
  - The performance depends on how the Rendezvous Point (RP) is chosen.

Flood-and-Prune

- A source broadcasts the first multicast IP datagram.
- A router R forwards a multicast packet from source S if, and only if,
  - The packet comes from the shortest route from R back to S. (RPF)
  - R forwards the packet only to the child links for S.
    - > A Child link of R for S: the link that has R as parent on the shortest path tree where S is the root.
    - > The child links are found by the multicast routing updates.
- Prune – as previously discussed
- Grafting
  - A DVMRP router that realizes new membership in the multicast group through IGMP sends a grafting message to the upstream router.
  - The upstream router then will resume the packets forwarding.

Multicast Routing

DVMRP: Distance Vector Multicast Routing Protocol

- Source-based trees with RPF, details [RFC1075]
- Flood-and-pruning

MOSPF: Multicast Open Shortest Path First

- Source-based trees

CBT: Core-Based Trees

- Group-shared tree

Inter-Autonomous System Multicast Routing

- e.g., BGMP (Border Gateway Multicast Protocol)

PIM: Protocol Independent Multicast

- Two modes: dense/sparse according to members

Distance Vector Multicast Routing Protocol (DVMRP)

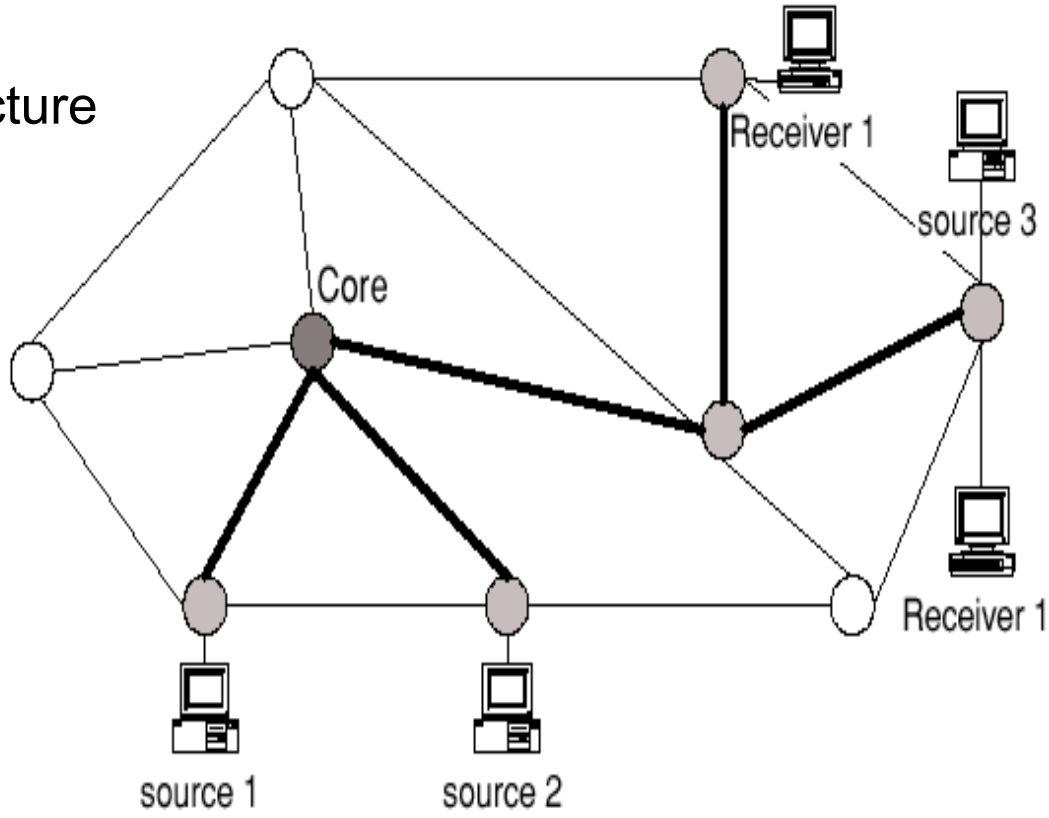
- DVMRP is a distance vector based multicast routing protocol. Has the count-to-infinity problem as RIP.
- A DVMRP router exchanges multicast routing information with its neighbors and builds the multicast routing table → source-based tree
- Flood-and-prune approach is used in routing.
- DVMRP assigns various values to the TTL field of multicast datagrams to control the scope of the broadcast.
- Each link can be assigned with a TTL threshold in addition to the routing cost.
  - A router will not forward a multicast/broadcast datagram if its TTL is less than the threshold.

Multicast Extension to OSPF (MOSPF)

- MOSPF, like OSPF, is a Link State Algorithm based intra-domain multicast routing protocol
  - each router maintains the entire topology of the network
  - each router run Dijkstra's shortest path algorithm to get shortest path to each destination → source-based tree
- To incorporate multicast – a new group membership LSA (Link–State Advertisement) is used to include group membership in link information
- MOSPF, like DVMRP, uses multiple multicast trees with each source as the root, i.e. Source-based Tree
- MOSPF, like DVMRP, performs tree calculation *on-demand* triggered by the 1st arriving multicast packet to a group

Core Based Tree (CBT)

- Source-based Tree is very costly
- Core Based Tree (CBT) is also called as Group-Shared Tree for all the sources in the multicast group
- CBT forms an hierarchical structure
  - A Core router is chosen first
  - All other tree routers request to Join the core to build the routing table for each multicast group



CBT (cont'd)

- CBT does not broadcast the first datagram.
  - Traffic load is greatly reduced.
  - Suitable for multicasting in large-scale and dense networks.
- The routing table size is greatly reduced
  - A router only needs to store information for each multicast group
  - The number of CBT router entries is the same as the number of active groups.
  - Different from DVMRP and MOSPF
    - > In DVMRP and MOSPF, a router stores information for each source in each multicast group
    - > In DVMRP router, entries of $\Sigma_{i \in (\text{active groups})}$ (No. of sources in group i).
- CBT has the traffic concentration problem
  - All source traffic may concentrate on a single link
  - May lead to congestion and a larger delay than multiple-tree schemes.

Protocol Independent Multicast (PIM)

- It is difficult to find a single protocol which is suitable for all scenarios, with various
  - Number of participants and their locations
  - Number of sources
  - Traffic sent by each source
- Protocol Independent Multicast Protocol (PIM) has two modes:
  - Dense mode
    - > Source-based trees are used, works like DVMRP
  - Sparse mode
    - > A group-shared tree is built from a Rendezvous Point (with backups), like CBT
    - > For a high-rate source, its local router may initiate a switch to the source-based tree mode and use a source-based shortest path tree
    - > One or more additional source-based trees may be warranted if there is enough traffic from the sources in network
      - ~ Justifiable if dense area of activities observed far from the RP
      - ~ Source-based tree does not have to involve the RP

MBone

- MBone stands for the multicast backbone.
  - Created in 1992, initially used to send live IETF meetings.
  - has evolved to become a semi-permanent IP multicast testbed.
- MBone is an overlay network with a double-layer structure.
  - Lower layer
    - > consists of a large number of multicast islands (local networks that directly support IP multicast).
    - > Multicast IP datagram are sent and forwarded within the islands.
  - Upper layer
    - > consists of a mesh of point-to-point links, or tunnels, connecting the islands.
    - > A multicast IP datagram is encapsulated in a unicast IP datagram when sent through a tunnel.

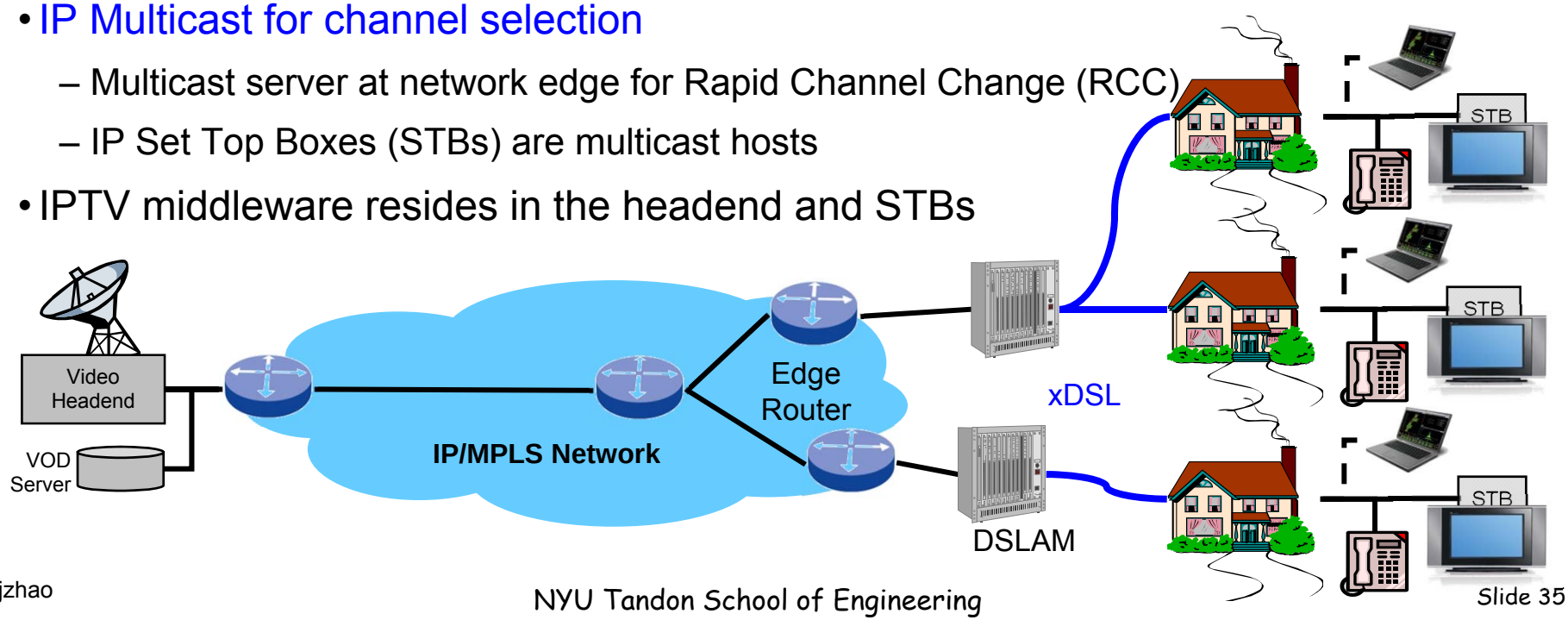
Configuring a Multicast Router

Please read section 7.2.5 for

- Configuring IGMP
- Configuring multicast routing
- Cisco IOS multicast diagnostic tools

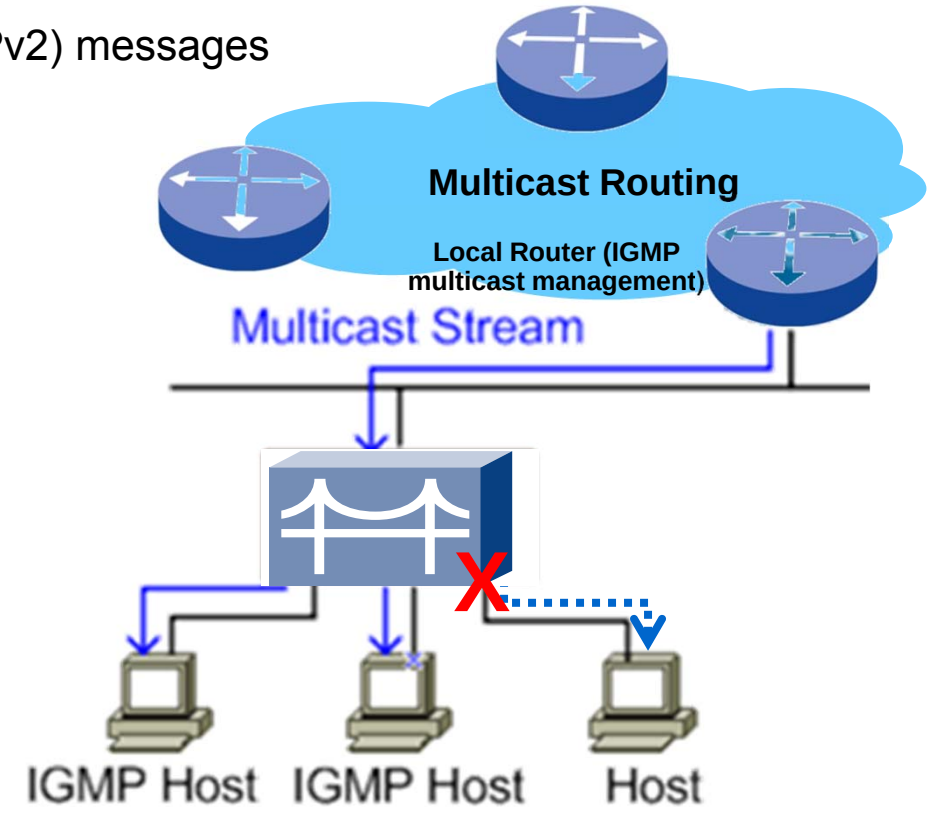
Service Provider IPTV

- Leverage household access and existing IP network to provide bundled phone, internet, TV (triple play) services
- IPTV is implemented with two parts
  - IPTV broadcast for switched digital broadcast channels, DVR, EPG – Pt2MPt services
  - Pt2Pt service like Video-on-Demand (VOD), interactive TV applications, targeted advertising
- Video Headend to provide digital video content
- IP Multicast for channel selection
  - Multicast server at network edge for Rapid Channel Change (RCC)
  - IP Set Top Boxes (STBs) are multicast hosts
- IPTV middleware resides in the headend and STBs



IGMP Snooping (for Broadcast IPTV)

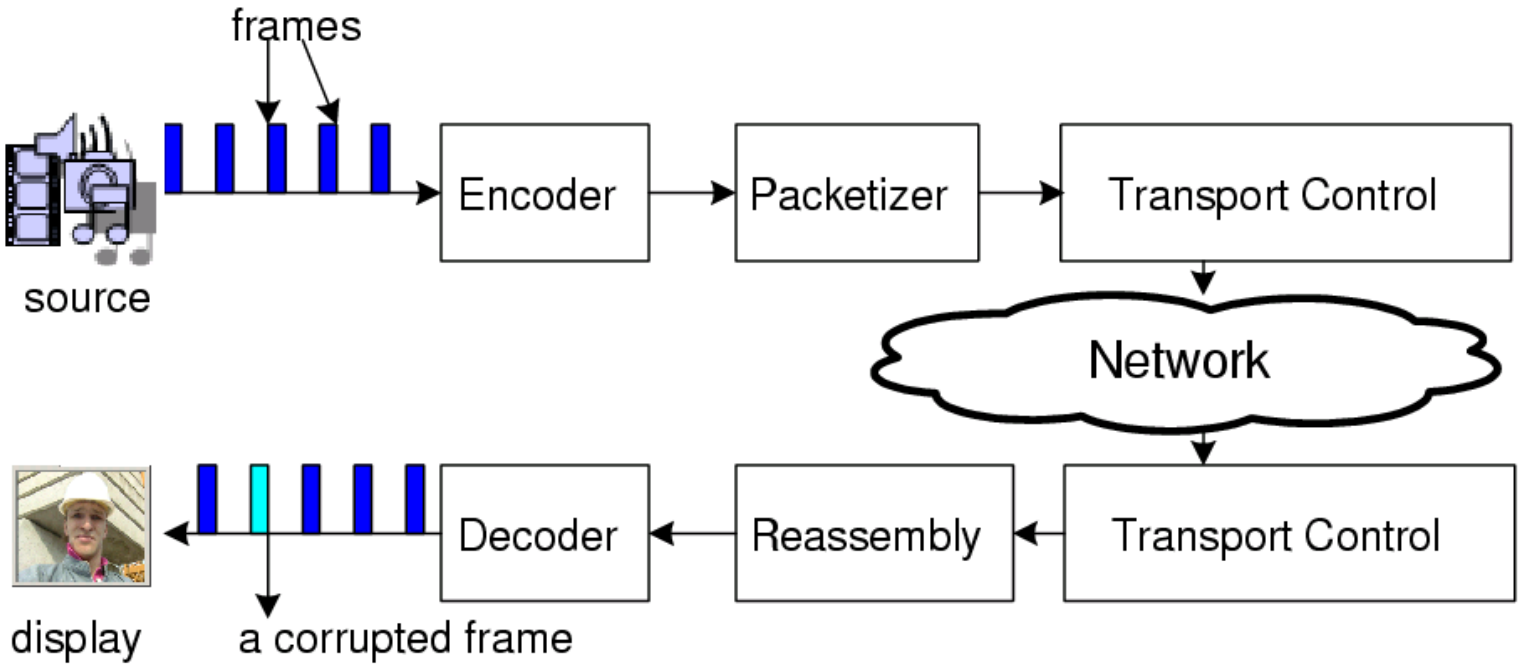
- Deployed in a layer-2 device to passively snoop on IGMP packets to learn the multicast group membership
  - Packets transferred between IP multicast routers and hosts
  - Look into Query, Report and Leave (IGMPv2) messages
- Without IGMP snooping, multicast traffic is treated as broadcast traffic – it is forwarded to all ports
- With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group
- IGMP Snooping network impact
  - Generate no additional network traffic
  - Significantly reduce multicast traffic delivered to or passing through downstream devices



Realtime Multimedia Streaming

Realtime multimedia applications

- Video teleconferencing
- Internet Telephony (VoIP)
- Internet audio, video streaming



The Architecture of video streaming

Multimedia Networking Applications

Application Classes:

1) Streaming stored audio and video

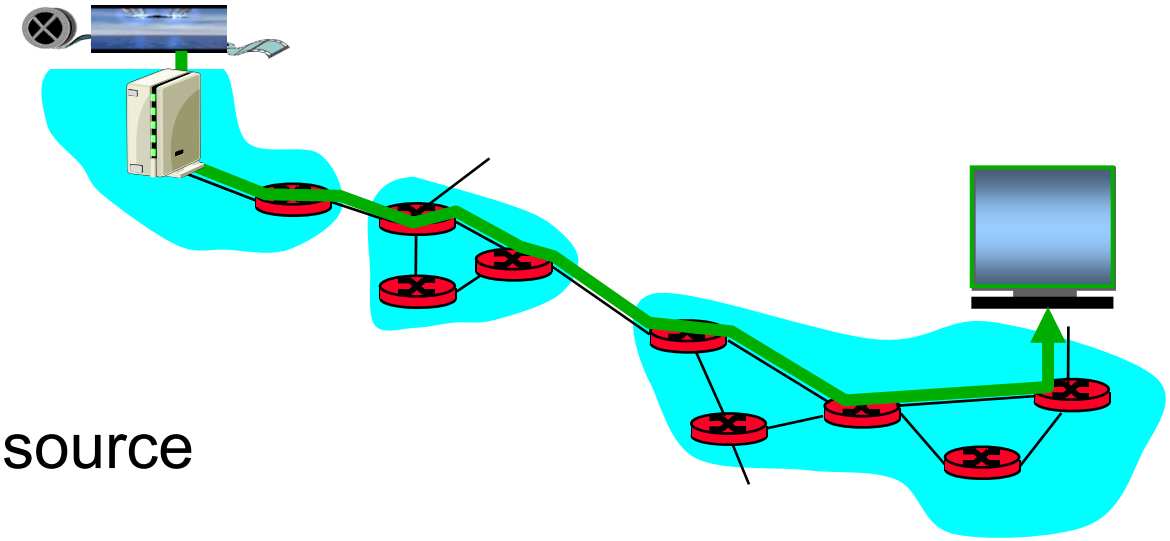
2) Streaming live audio and video

3) Real-time interactive audio and video

Fundamental characteristics:

- Antithesis of data applications, email, file sharing, which are loss intolerant but delay tolerant.
- Typically delay sensitive
  - end-to-end delay
  - delay jitter
- But loss tolerant: infrequent losses cause minor glitches

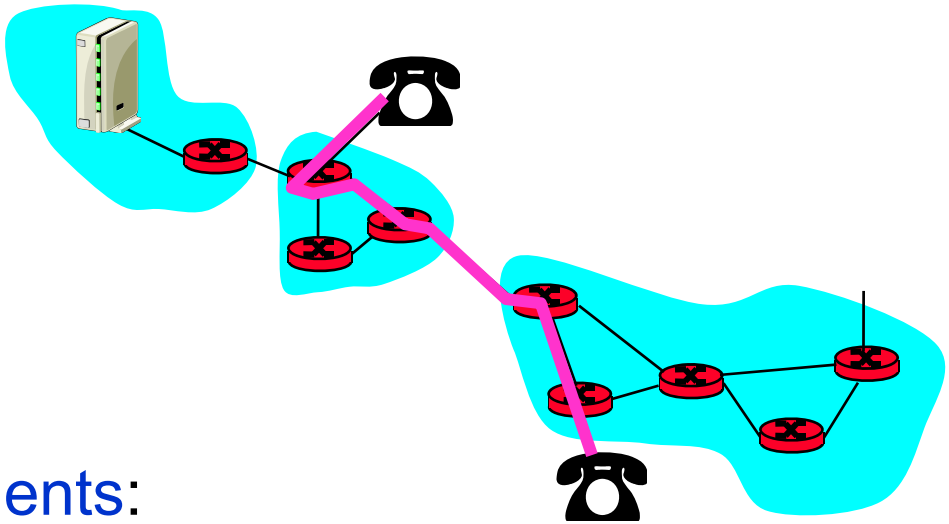
Streaming Stored Multimedia



Streaming:

- Media stored at source
- Transmitted to client
- Streaming: client playout begins *before* all data has arrived
  - timing constraint for still-to-be transmitted data: in time for playout

Interactive, Real-Time Multimedia



- Applications: IP telephony,

  video conference, … …

- End-to-end delay requirements:
  - audio: < 150 ms good, < 300 ms acceptable
    - includes application-level (packetization) and network delays
    - higher delays noticeable, impair interactivity
- Session initialization
  - How does callee advertise its IP address, port number, encoding algorithms?

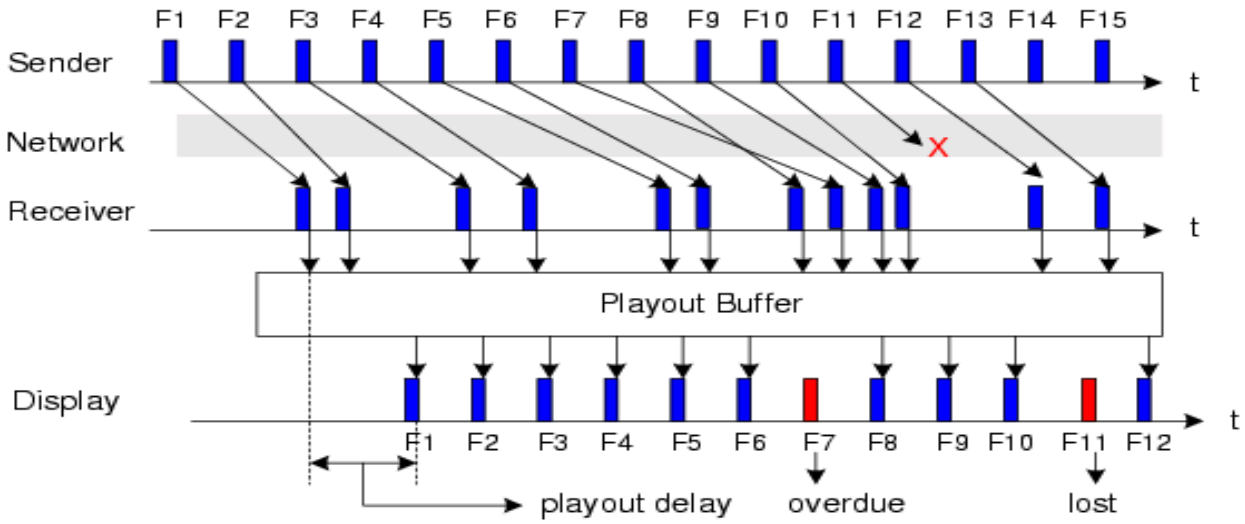
QoS Concerns

TCP/IP protocol suite is not designed to accommodate real–time traffic

- Lack of support to synchronous, real-time demands
- Traffic loss and variable delays (due to bandwidth limit, non-cooperative network behavior from other data traffic)
- Long call setup time
- Connection-less nature
- Reliability

Jitter Control

- Jitter: the variation in the inter-arrival times of received packets
- Jitter Control
  - Larger playout delay, each frame is due to play at a later time, makes the real time streaming application more tolerable to jitter
  - Interactive realtime applications, like VoIP, require tight jitter control due to the strict requirement on end-to-end round trip delay



An example: the playout buffer is used to absorb jitter

Streaming Multimedia: UDP or TCP?

UDP

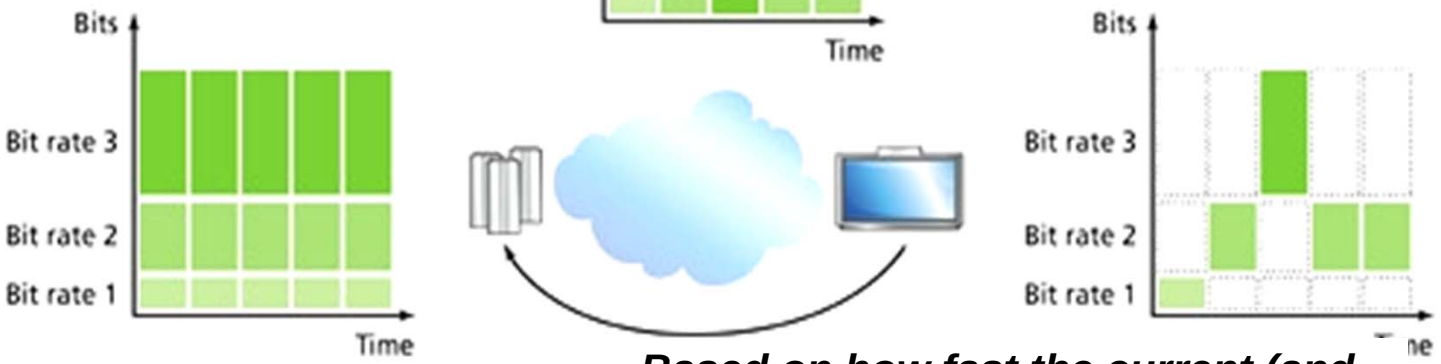
- Server sends at rate appropriate for client (oblivious to network congestion !)
  - –often send rate = encoding rate = constant rate
  - –then, fill rate = constant rate - packet loss
- Short playout delay (2-5 seconds) to compensate for network delay jitter
- Error recover: time permitting
- Usually used for multimedia services

TCP

- Not applicable in multicast!
- Send at maximum possible rate under TCP
- Fill rate fluctuates due to TCP congestion control
- Larger playout delay is intolerable to meet real-time requirements
- HTTP/TCP passes more easily through firewalls
- There are also some advantages to use TCP! HAS example in next two slides …

HTTP Adaptive Streaming (HAS)

- HAS adapts to available bandwidth
- ISO Standardised: MPEG–DASH
- HAS variants: MS–Silverlight, Apple HLS
- Reliable – uses TCP
- Reuses web technology
- Goes through firewalls



Based on how fast the current (and previous segments) are downloaded, the bit rate of the next segment is selected

HAS Operation

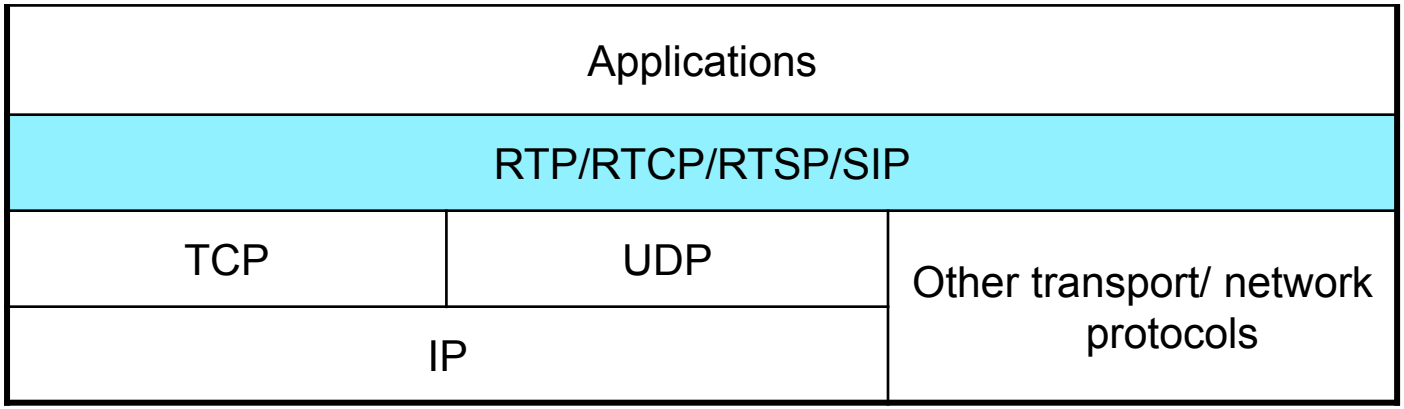
- HAS with Adaptive Bit Rate works as follows:
  - Videos are fragmented into 2-10sec chunks
  - Each chunk is encoded with several video rates
  - A Manifest is sent to the client which describes the available bit rates to choose from
  - The client algorithms for choosing bit rates are based on heuristics and vary from client to client
- The client generally starts a the lowest bit rate and increases based on the response time it perceives (how fast segments are delivered)
- The client will adjust the encoding rate up or down while trying to maintain a nominal buffer fill level

More Performance Requirements

- End-to-end transport control
  - Sequencing – need it in upper layer since UDP does not support sequence numbering
  - Timestamping – for playout, jitter and delay calculation
  - Payload type identification – for media interpretation
  - Error control – need it on upper layer since UDP/IP does not support Forward Error Control (FEC), ARQ, …
  - Error concealment – method to cover up errors from lost packets by using the redundancy in most adjacent-frame image information
  - QoS – from the receiver to the sender for operation adjustment
  - Rate control – from the sender to reduce sending rate adaptively to network congestion
- Network support
  - Bandwidth reservation
  - Call admission and scheduling policy
  - QoS specific routing
  - Traffic shaping and policing

Protocol Stack for Multimedia Services

- Realtime Transport Protocol (RTP)
- Realtime Transport Control Protocol (RTCP)
- Real Time Streaming Protocol (RTSP)
- Session Initiation Protocol (SIP)
  - Basic components: SIP user agent and SIP network server
  - Widely used in IP telephony, voice over LTE (VoLTE).



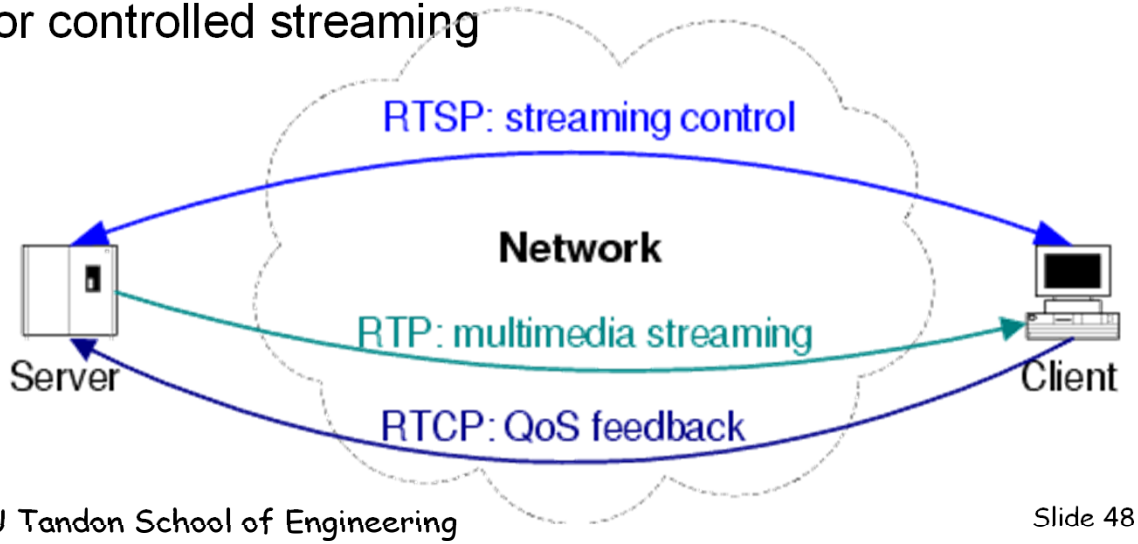
Multimedia Streaming Example

Real Time Transport Control Protocol (RTCP)

- QoS feedback reports containing number of packets lost at receiver, interarrival jitter that allows senders to adjust data rate
- Binding across multiple medias sent by a user (SDES for source description)
- Rate control of RTCP packets by noting how many participants are on session
- Minimal session control

Real Time Streaming Protocol (RTSP)

- Internet VCR remote control, initiating and directing realtime streaming
- Transported using UDP or TCP
- Works with RTP/RTCP for controlled streaming



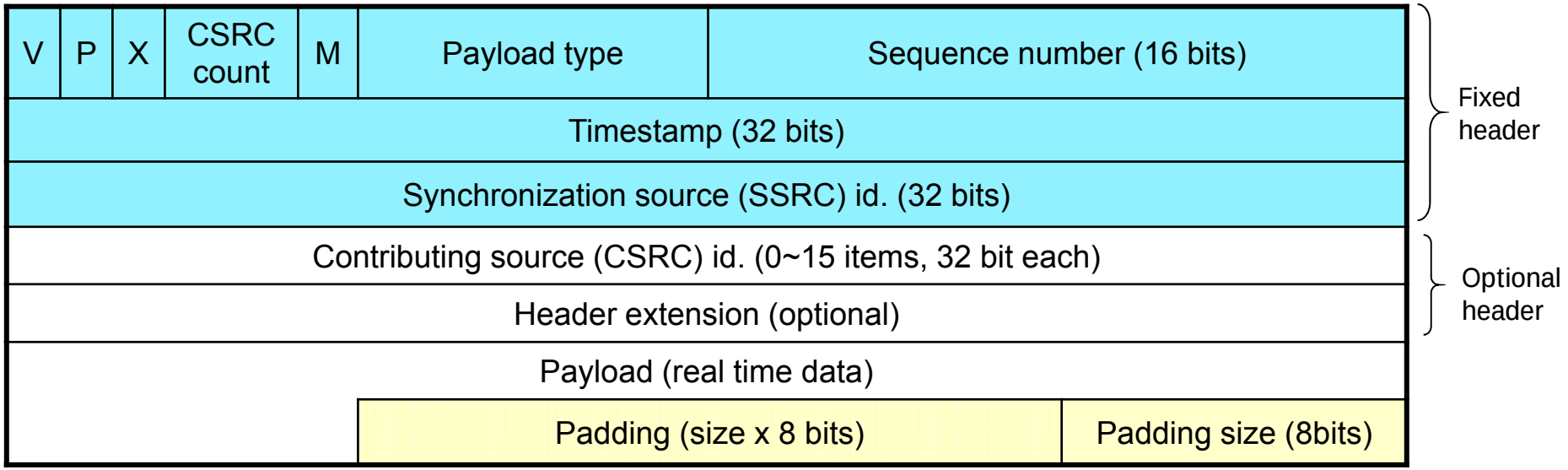
RTP and RTCP

- Two closely linked key parts: data + control
  - RTP encapsulates realtime data
  - RTCP provides QoS monitoring and session control
- RTP is also used to support distributed computing
- RTP/RTCP are application layer protocols
  - Usually integrated into applications
  - Independent of the underlying transport and network layer protocols
  - Does not provide timely delivery or other QoS guarantees
  - Rely on the lower-layer protocols for reliable service

RTP Introduction

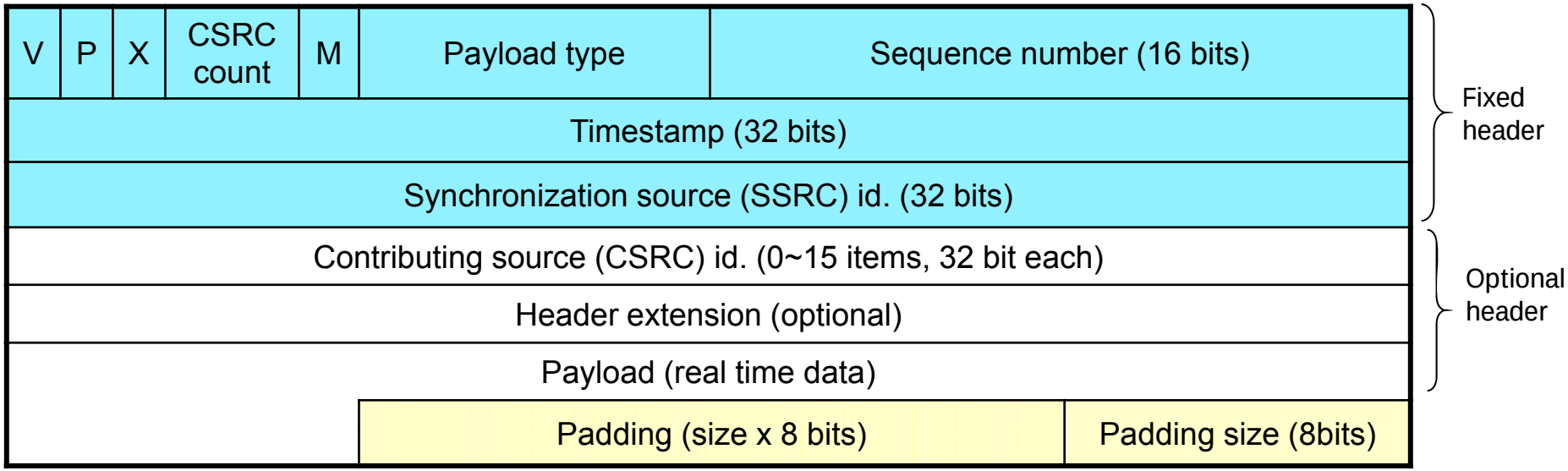
- Provides end-to-end transport functions for real-time applications
  - –Identify different payload types
  - –Packet sequence numbering
  - –Delay-oriented protocol with time stamping
- Usually carried in UDP but port number varies (default = 5004)
- Does NOT assume the underlying network is reliable and delivers packets in sequence
- New style – Application level framing and integrated layer processing
  - –Deliberately not complete in order to integrate into applications rather than a separate module
  - –Complete RTP specification needs other documents for each particular application
    - > Profile specification documents defines sets of payload type codes, and their mapping to payload formats
    - > Payload format specification document define how to carry a specific encoding

RTP Packet Format



- Version (V, 2bits): =2
- Padding (P, 1bit): If set to 1, last byte of payload is padding size that align the payload to the 32-bit word boundary
- Extension (X, 1bit): If set, variable size header extension exists
- CSRC count (4 bits): number of Contributing SouRCe (CSRC) identifiers in the CSCR list field
- Marker (M, 1bit): used to mark a significant event in the payload (e.g., the boundary of a video frame)
- Payload Type (PT, 7bits): identifies the format of the RTP payload and determines its interpretation by the application, e.g. JPEG is 26, H.261 is 31, MPEG2 video 33, … use this field to indicate encoding change in middle of conference.

RTP Packet Format (cont'd)



- Sequence Number (16bits): the sequence number of the RTP packet. Increments by one for each RTP packet sent. Can be used for loss detection and re-sequencing.
- Timestamp (32bits): identifies the sampling instant of the first octet of the RTP payload, used for synchronization and jitter calculation.
- Synchronization Source (SSRC) Identifier (32bits): identifies the Synchronization SouRCe (the source of a RTP packet stream). Each SSRC needs a RTP session.
- Contributing Source (CSRC) Identifier List: 0 to 15 items, each with 32bits. The list of identifiers of the sources whose data is carried in the payload.

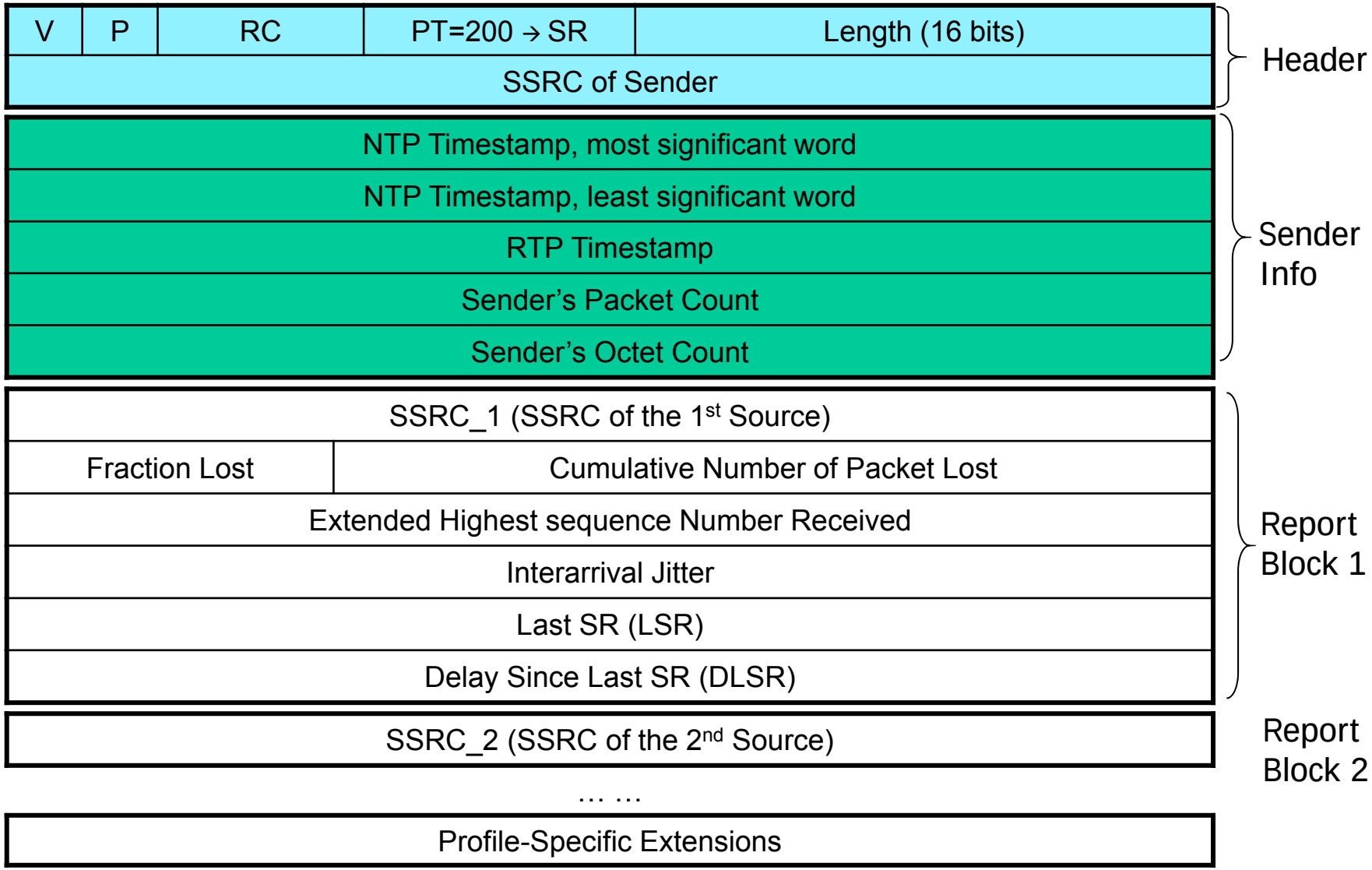
Real-Time Control Protocol (RTCP)

- Works in conjunction with RTP
- Each participant in RTP session periodically transmits RTCP control packets to all other participants.
- Each RTCP packet contains sender and/or receiver reports
  - report statistics useful to the application
- Statistics include number of packets sent, number of packets lost, interarrival jitter, etc.
- Feedback can be used to control performance
  - Sender may modify its transmissions based on feedback

RTCP Packet Types

- Sender Report (SR): statistics from active sender
  - May also includes RR blocks
- Receiver Report (RR): statistics from participants that are not active senders
  - RTCP RR packet sent if a node is only a receiver
- Source description item (SDES)
  - e-mail address of sender, sender's name, SSRC of associated RTP stream.
  - Provide mapping between the SSRC and the user/host name.
- BYE: indicates end of participation
- APP: application specific functions

RTCP Sender Report Format



RTCP Sender Report Fields

RTCP Header:

- Version (V) and Padding (P): As described for RTP data packet above
- Packet Type (PT, 8 bits): The packet type constant 200 designates an RTCP SR packet. RTCP RR is 201.
- Length (16 bits): The length of this RTCP packet in 32-bit words minus one, including the header and any padding.

Sender information block:

- NTP timestamp: wallclock time (absolute time as per Network Time Protocol) when packet is sent
- RTP timestamp: time when packet is sent according to the clock used to send RTP data packet timestamps; used for intra&inter media synchronization
- Sender's packet count: total number of packets sent since the start of session
- Octet count: total number of bytes sent since the start of session

RTCP Sender Report Fields (cont'd)

Multiple receiver report blocks, one for each source from this host receives packets

- SSRC_n: identifies source whose data this report block is about
- Fraction lost: fraction of packets lost since last report was sent
- Cumulative number of lost packets since the beginning of reception
- Highest sequence number received
- Inter-arrival jitter
- Last SR (LSR): The NTP timestamp of the last sender report received from the source
- Delay since Last SR (DLSR): Delay between receiving the last SR from this source and sending this RR

User Control of Streaming Media: RTSP

HTTP

- Does not target multimedia content
- No commands for fast forward, etc.

RTSP: RFC 2326

- Client-server application layer protocol.
- For user to control display: rewind, fast forward, pause, resume, repositioning, etc…

What it doesn't do:

- Does not define how audio/video is encapsulated for streaming over network
- Does not restrict how streamed media is transported; it can be transported over UDP or TCP
- Does not specify how the media player buffers audio/video

RTSP: Out of Band Control

FTP uses an "out-of-band" control channel:

- A file is transferred over one TCP connection.
- Control information (directory changes, file deletion, file renaming, etc.) is sent over a separate TCP connection.
- The "out-of-band" and "in-band" channels use different port numbers.

RTSP messages are also sent out-of-band:

- RTSP control messages use different port numbers than the media stream: Port 554
- The media stream is considered "in-band".

RTSP Operation Example