IP Multicasting & Related Security Issues

Digital Communication
Semester Project
Presentation

Vivek Ramachandran

Introduction to Multicast

- Why multicast?
  - When sending same data to multiple receivers
  - Better bandwidth utilization
  - Lesser host/router processing
  - Receivers' addresses unknown
- Applications
  - Video/audio conferencing
  - Resource discovery/service advertisement
  - Stock distribution
  - Eg. Vat, Vic, IP/TV, Pointcast

IP Multicast Applications

Live TV and Radio Broadcast
to the Desktop

Corporate Broadcasts

Multicast File Transfer
Data and File Replication
Whiteboard/Collaboration

Distance Learning

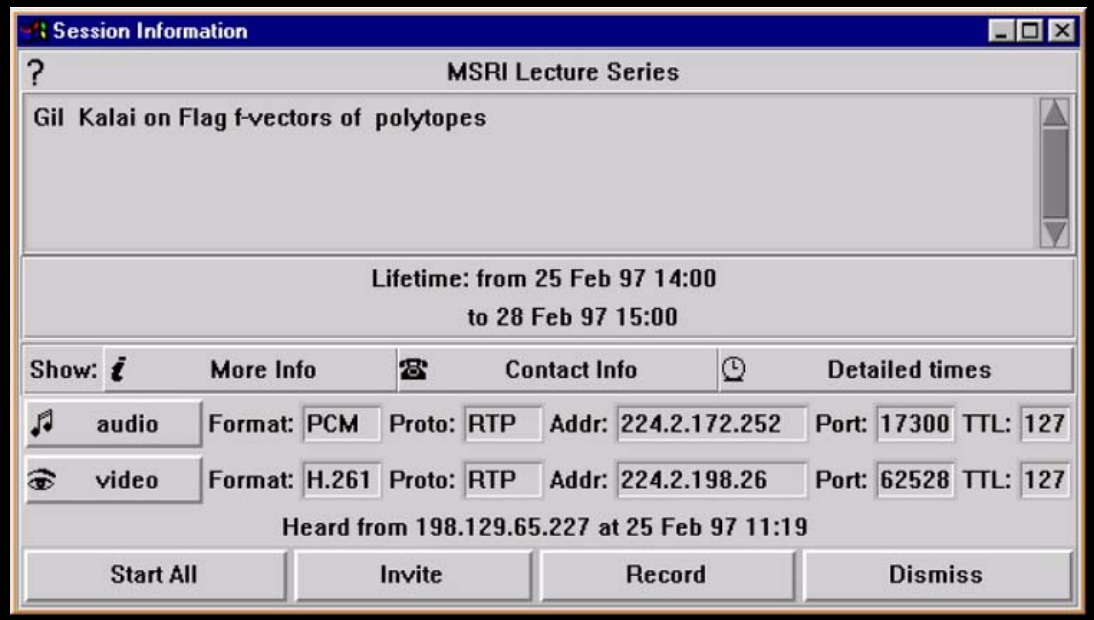
Training

Video Conferencing

Video-On-Demand

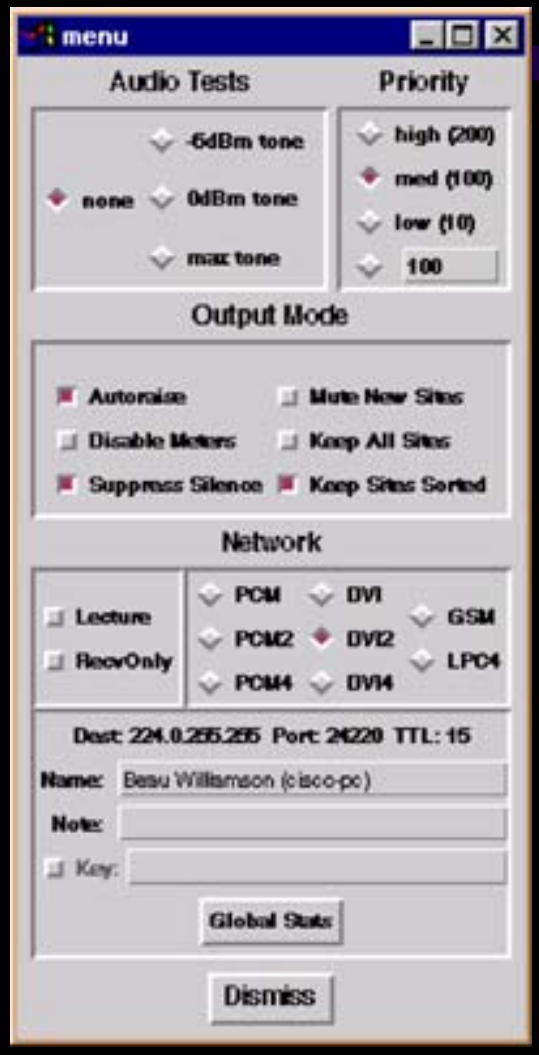
Real-Time Data Delivery—Financial

SDR —Session Directory

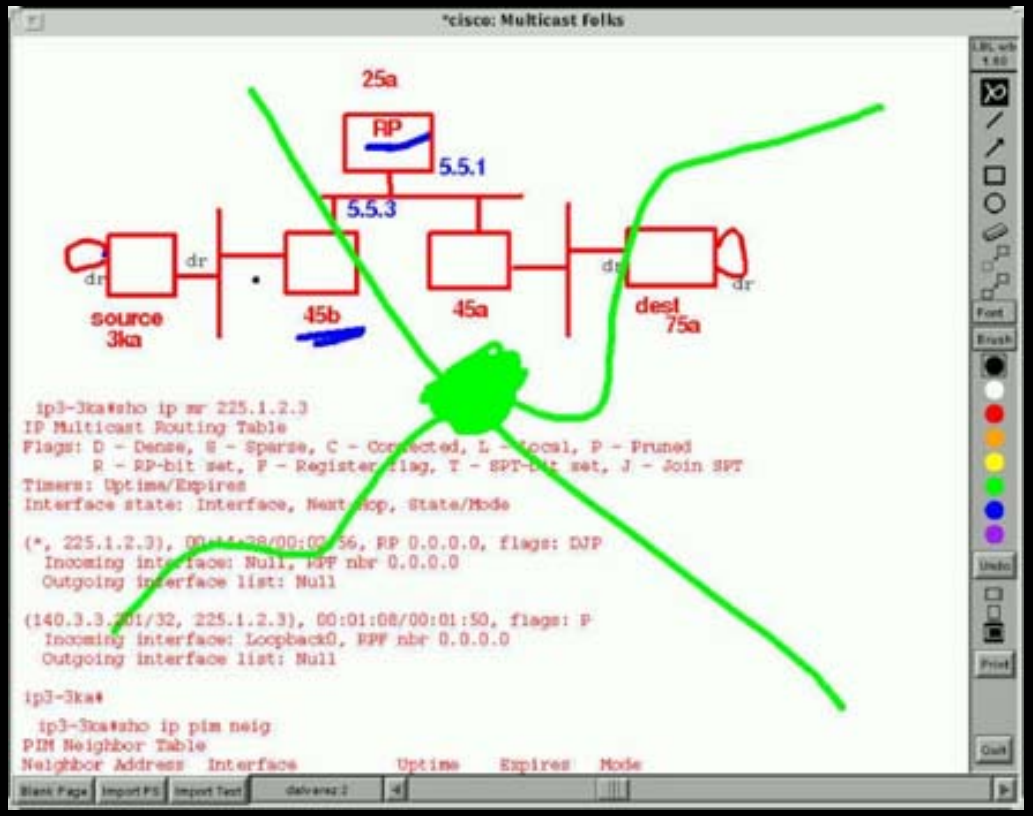


VIC —Video Conferencing

VAT —Audio Conferencing



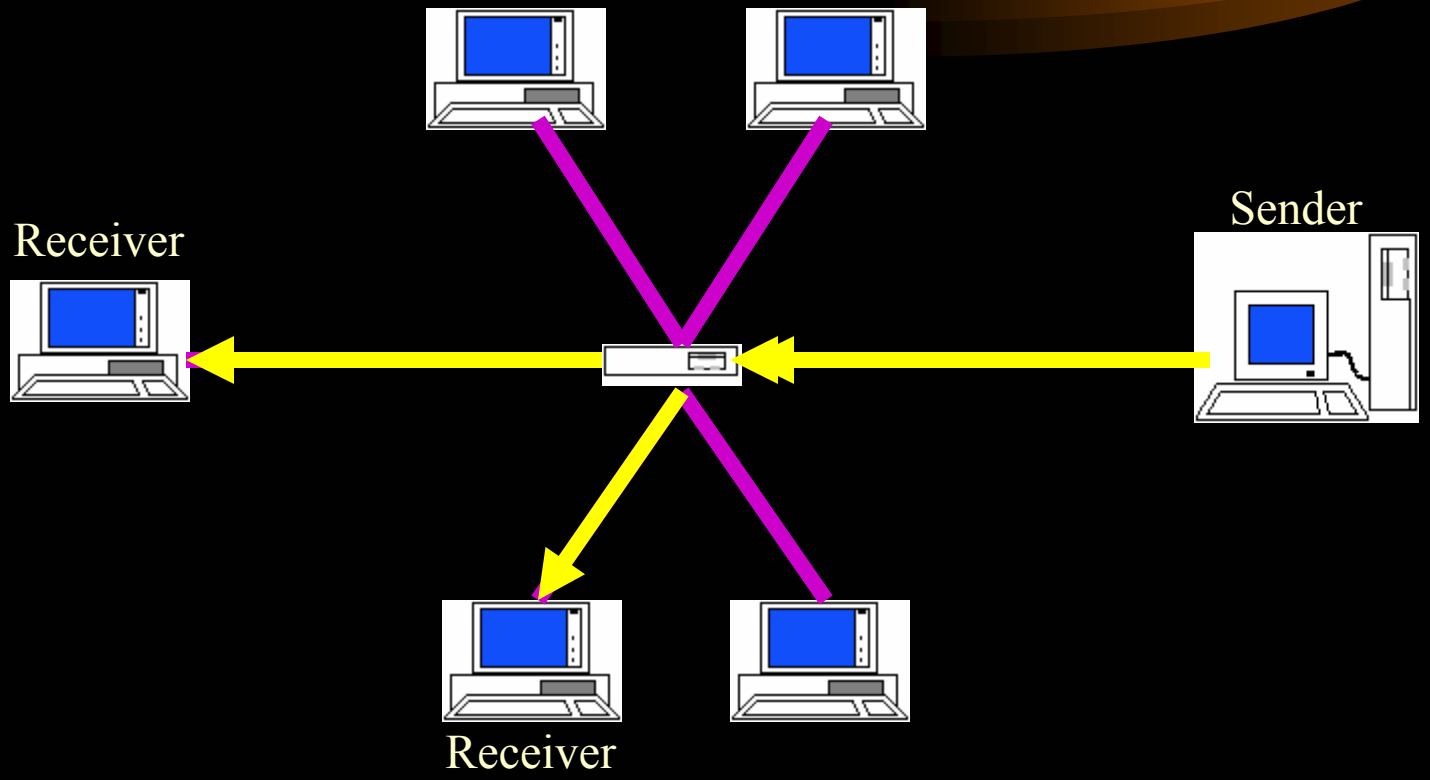
WB —White Board



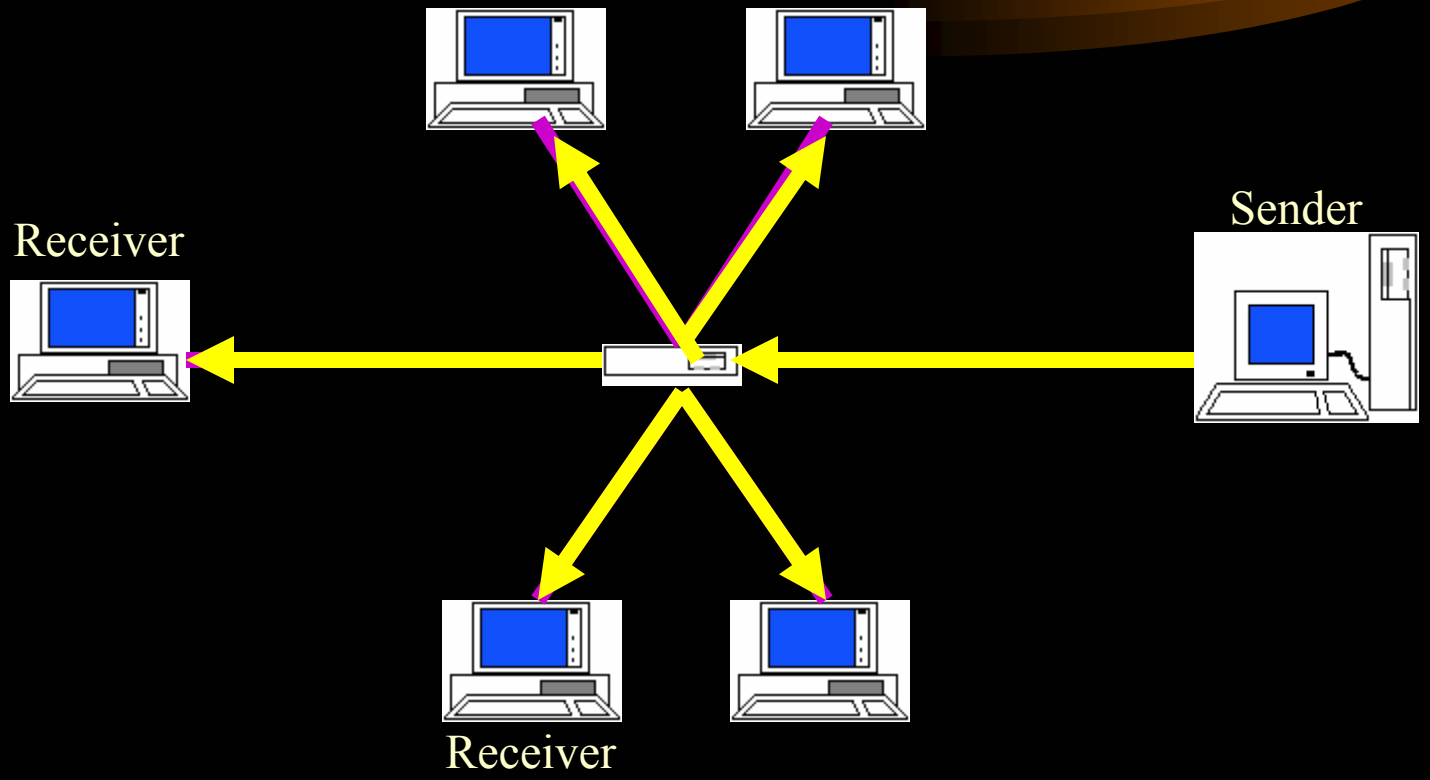
Types Of Communication

- 1. Unicasting
- 2. Broadcasting
- 3. Multicasting

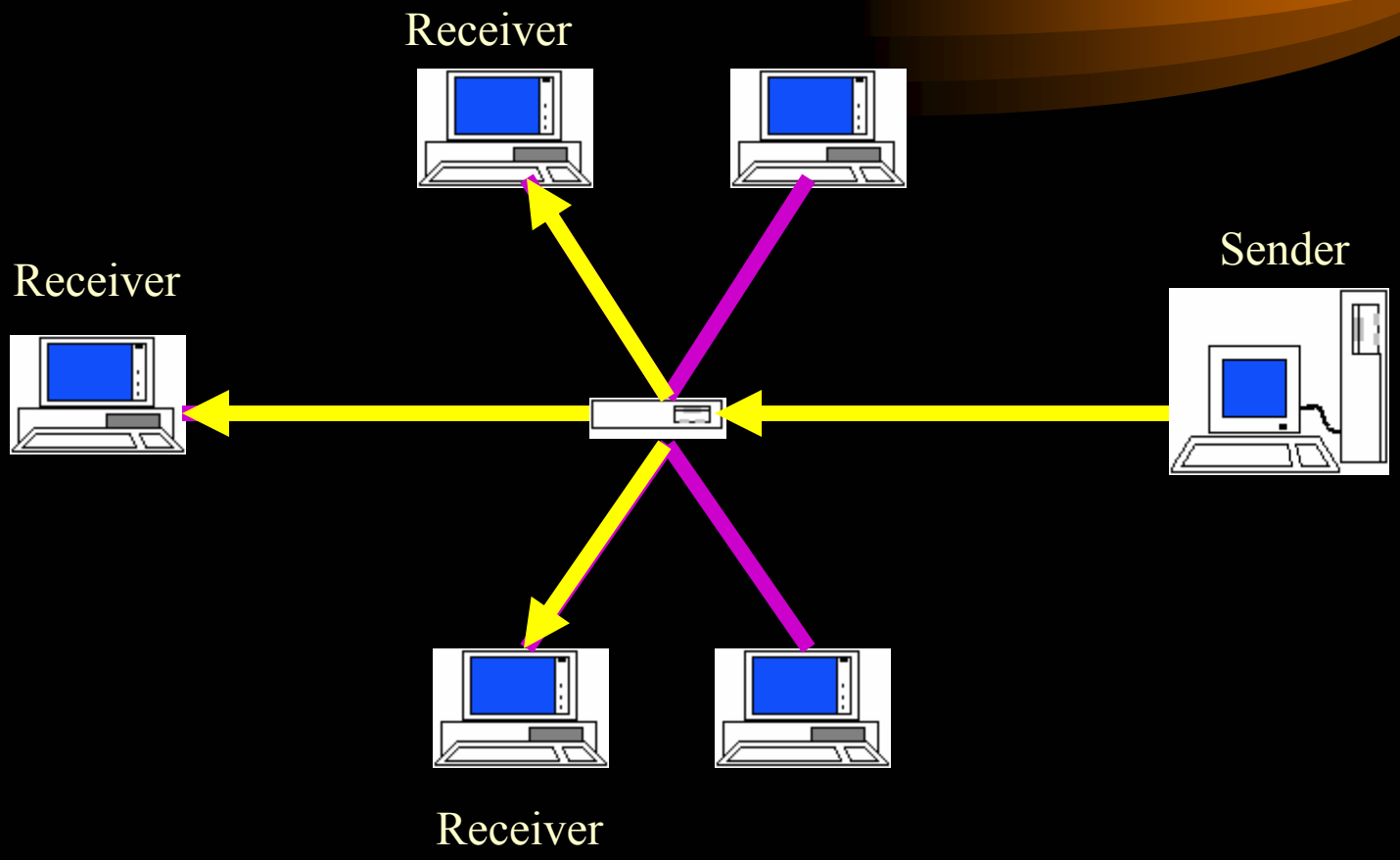
Unicast

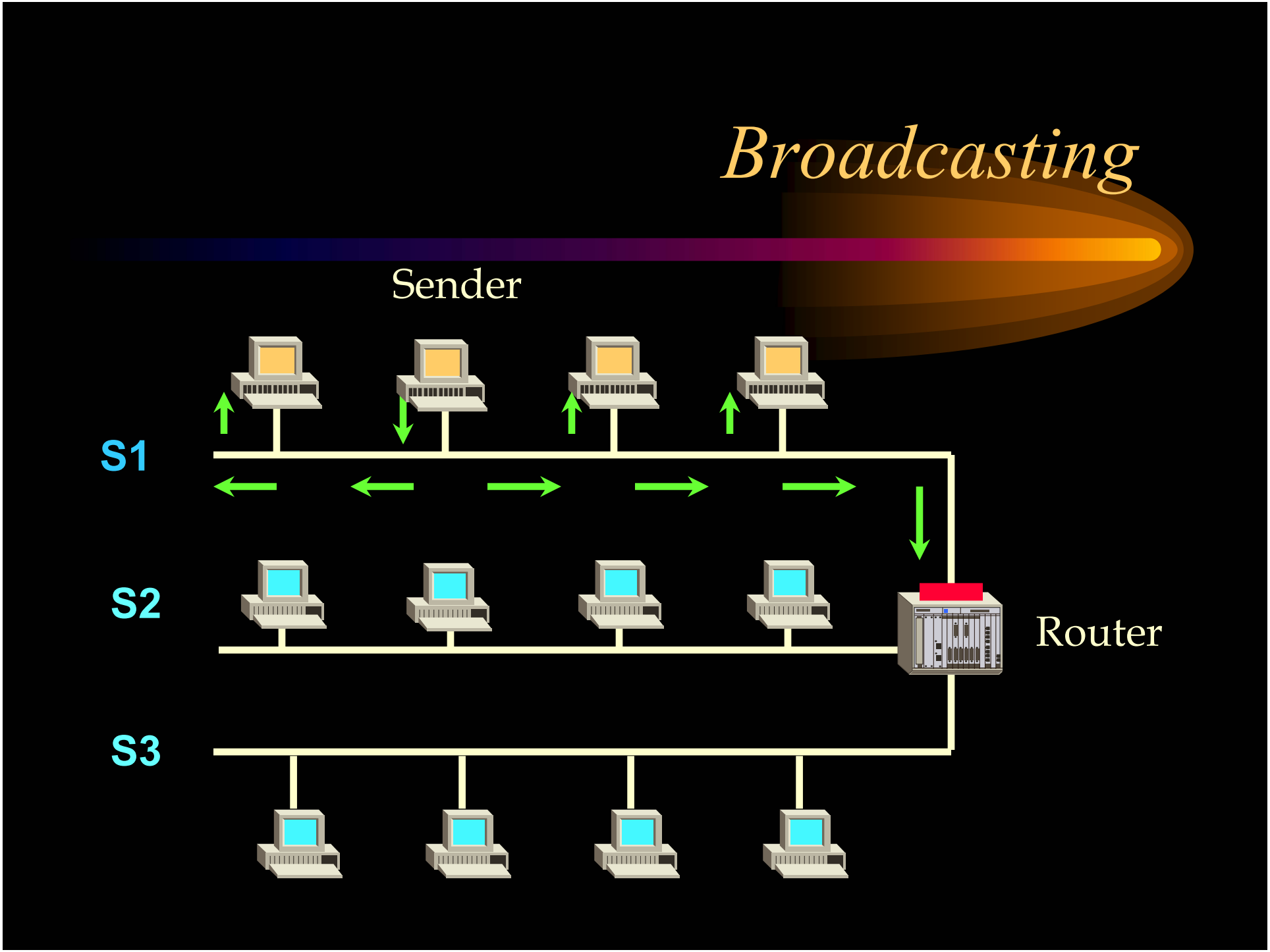


Broadcasting

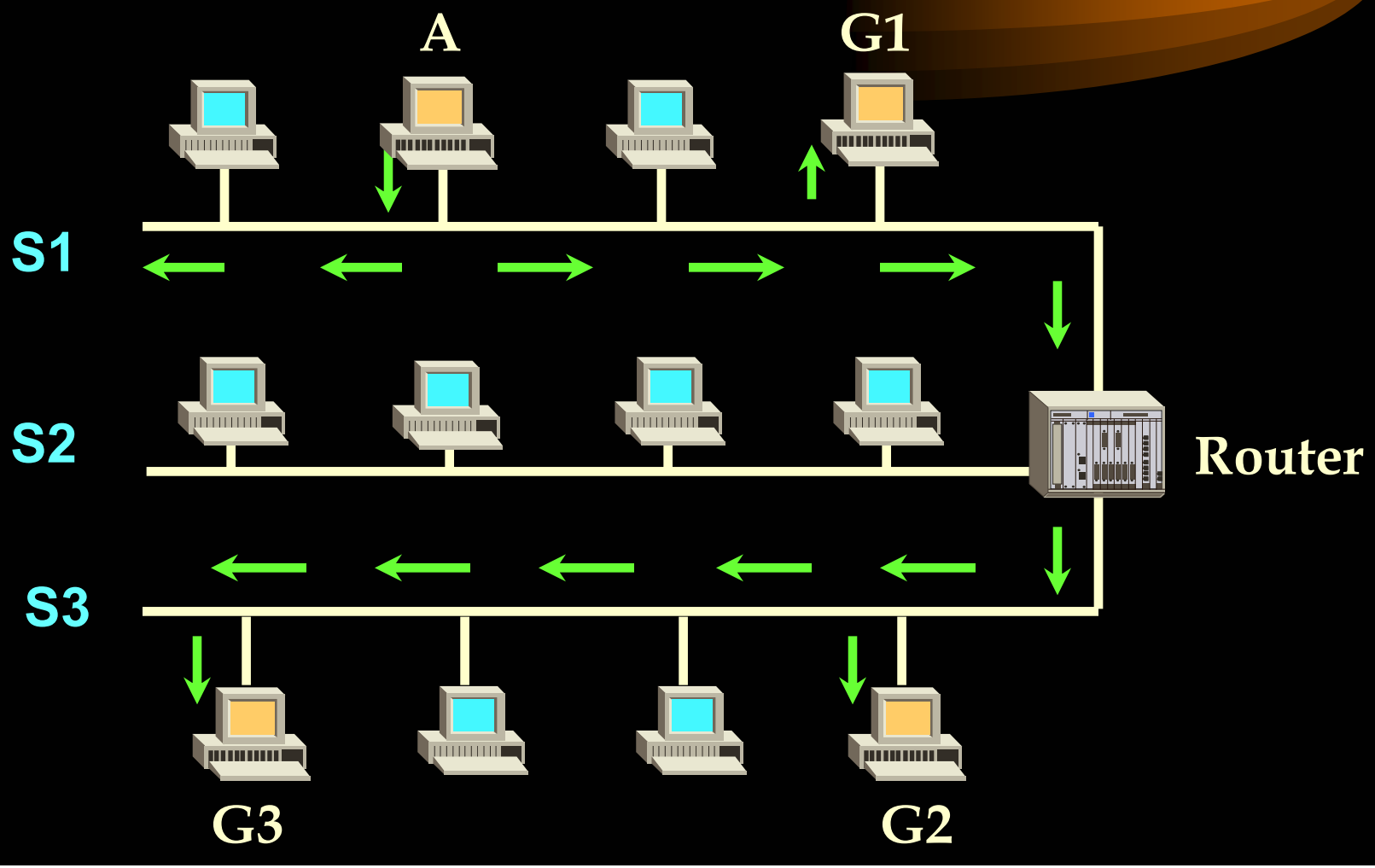


Multicast

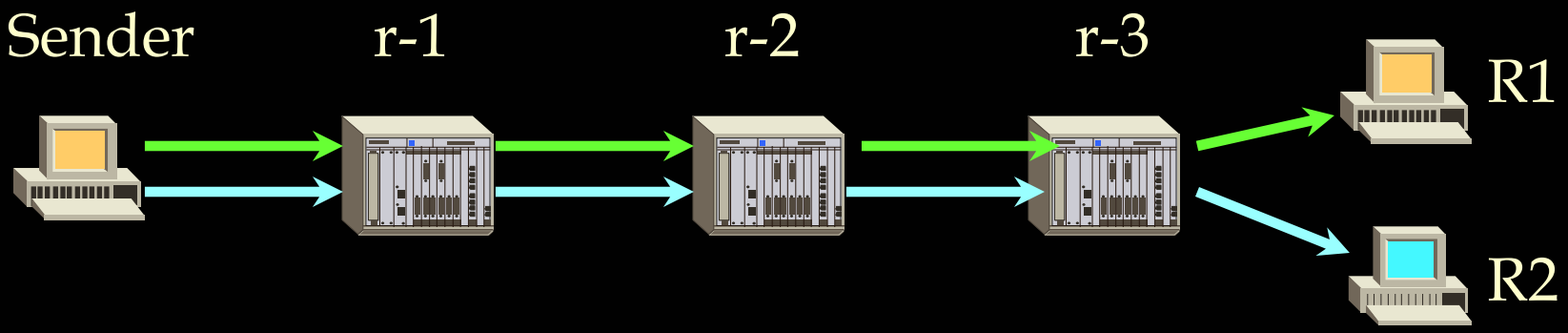



Broadcasting
Sender
S1
S2
S3
Router

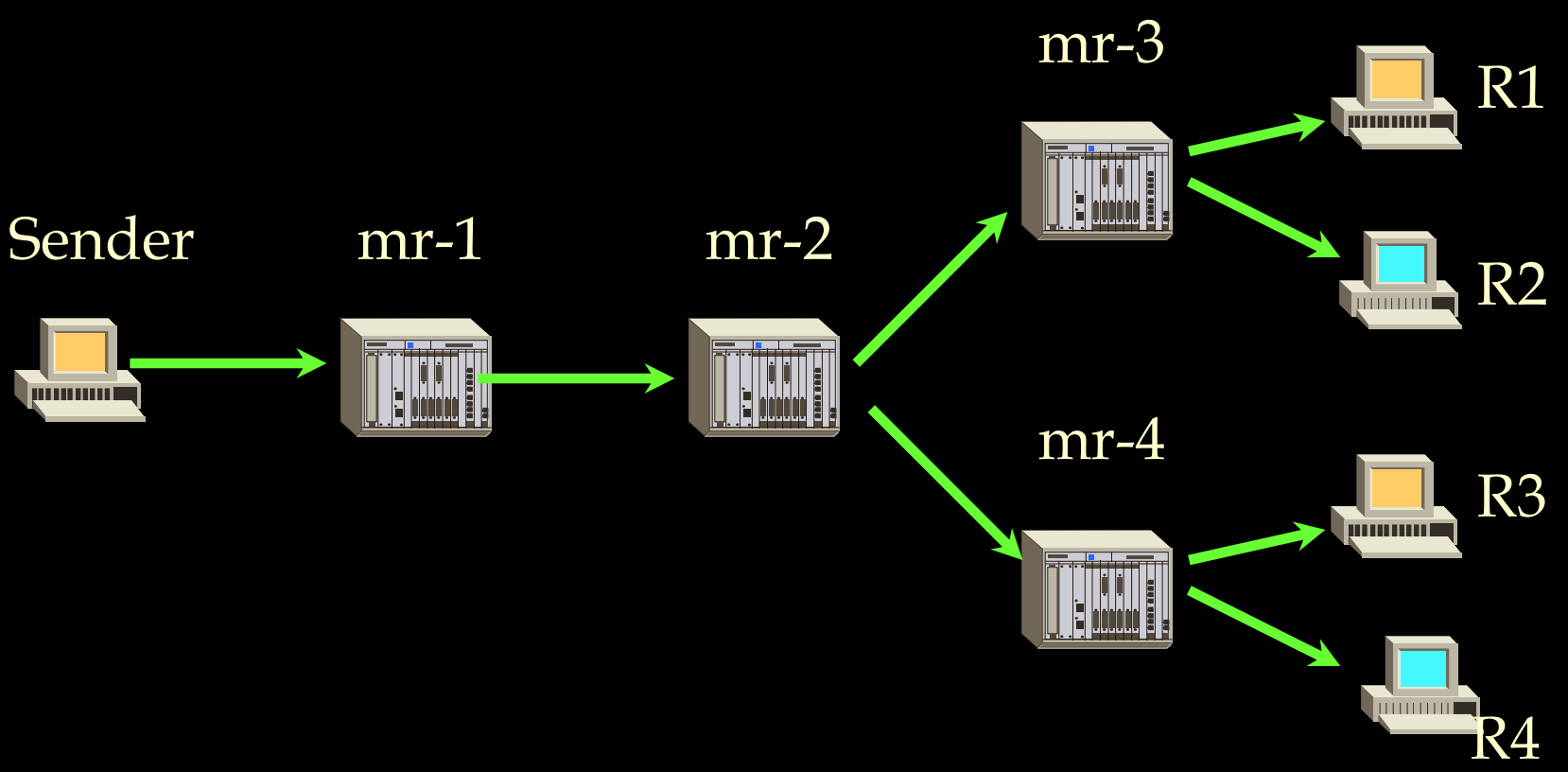
Multicasting



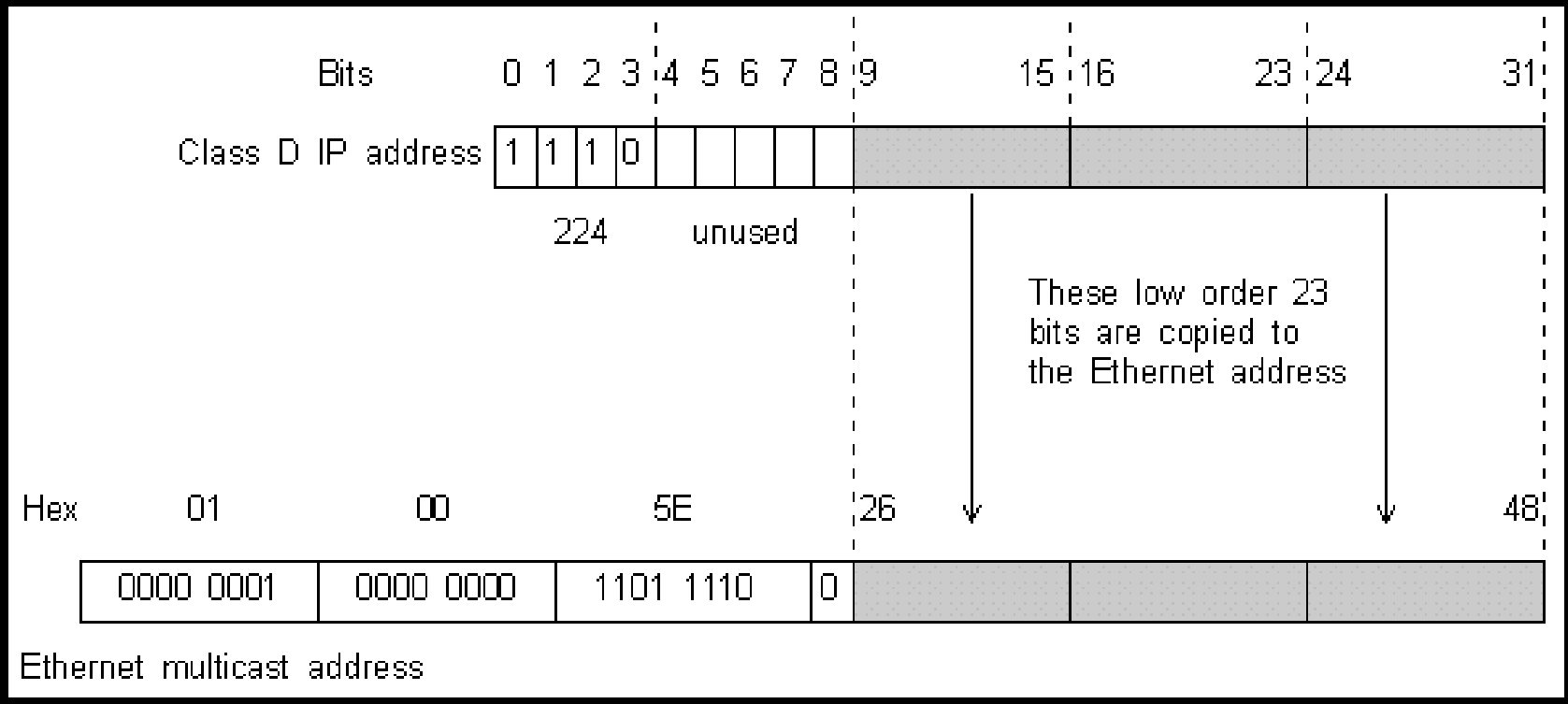
IP unicast routing



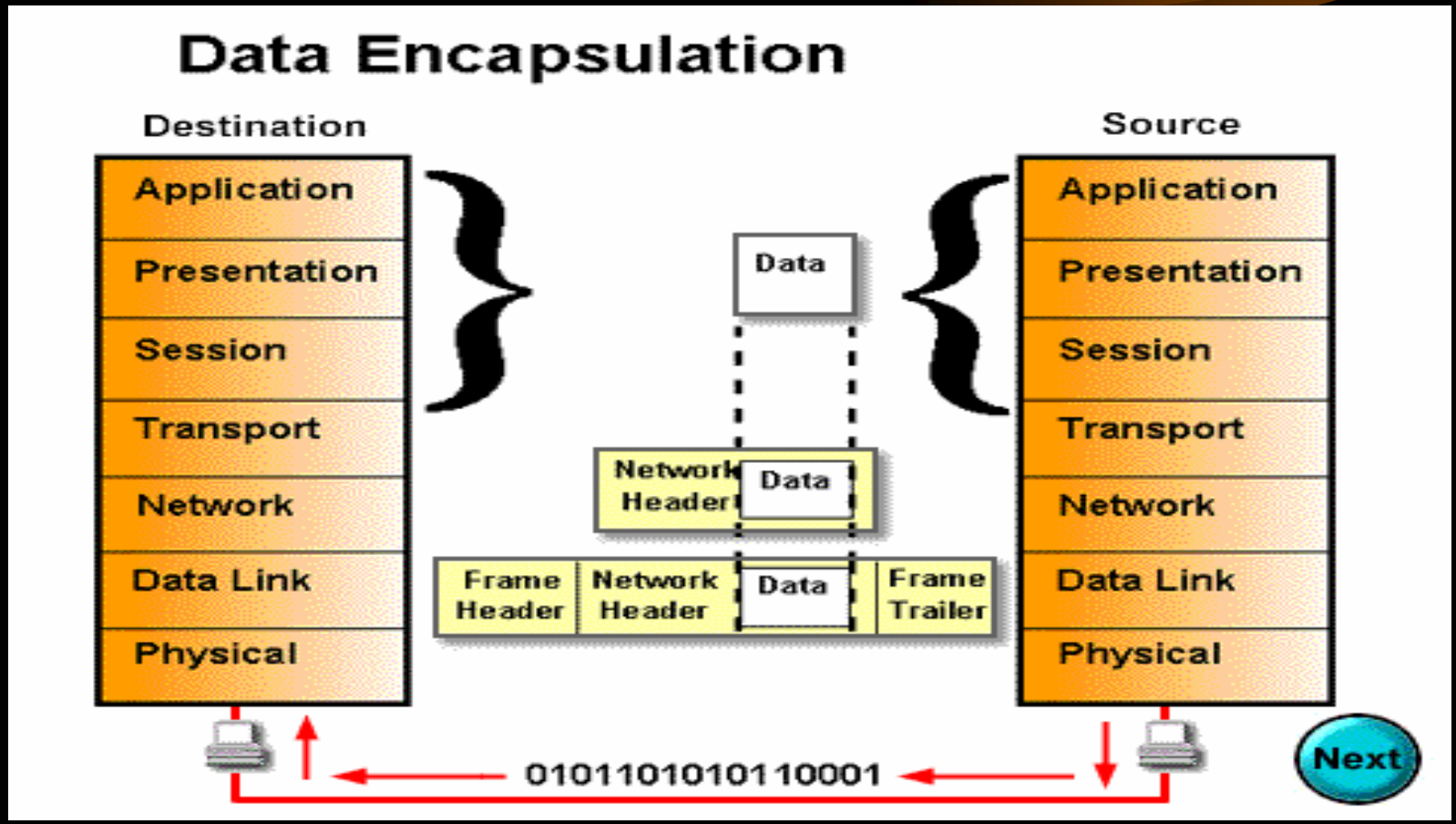
IP multicast routing



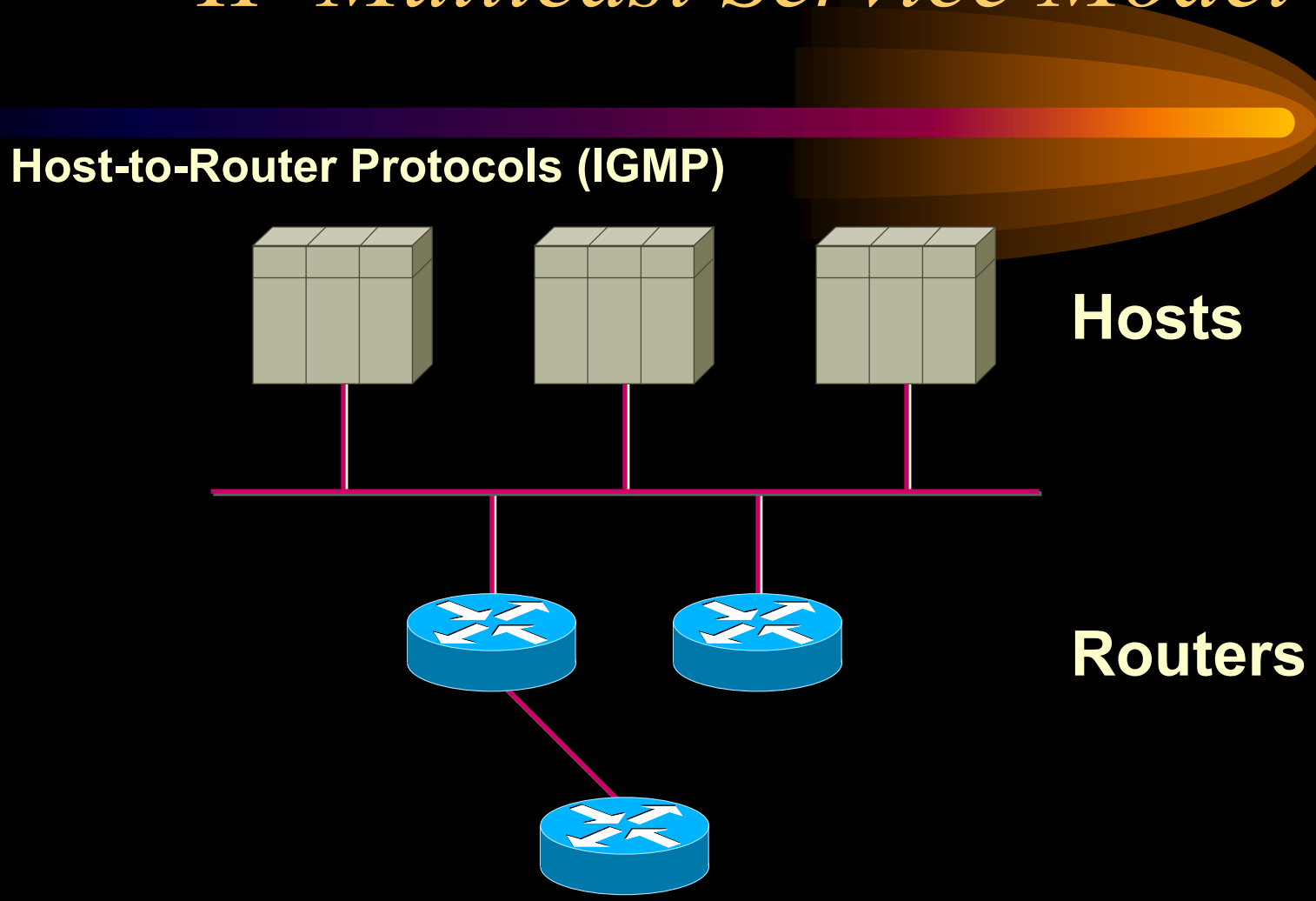
Ethernet Address Mapping



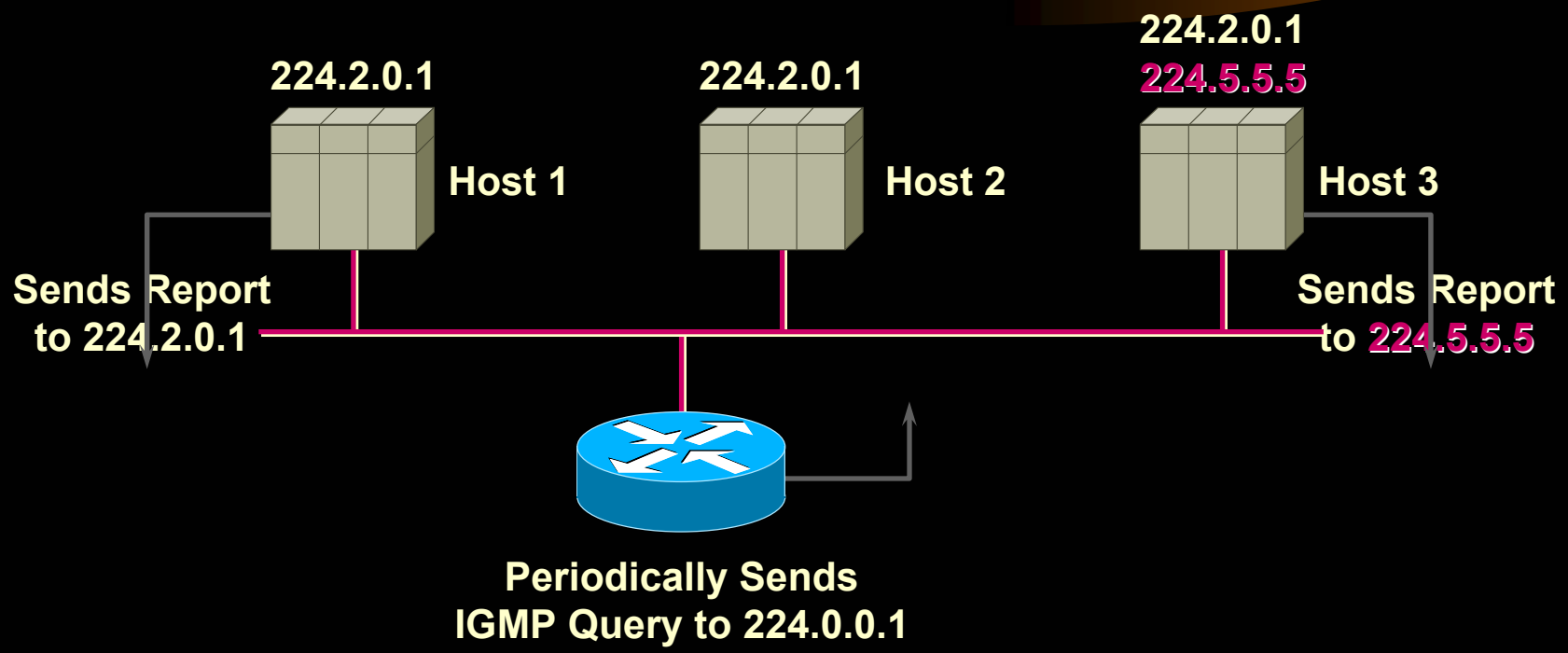
The OSI Model



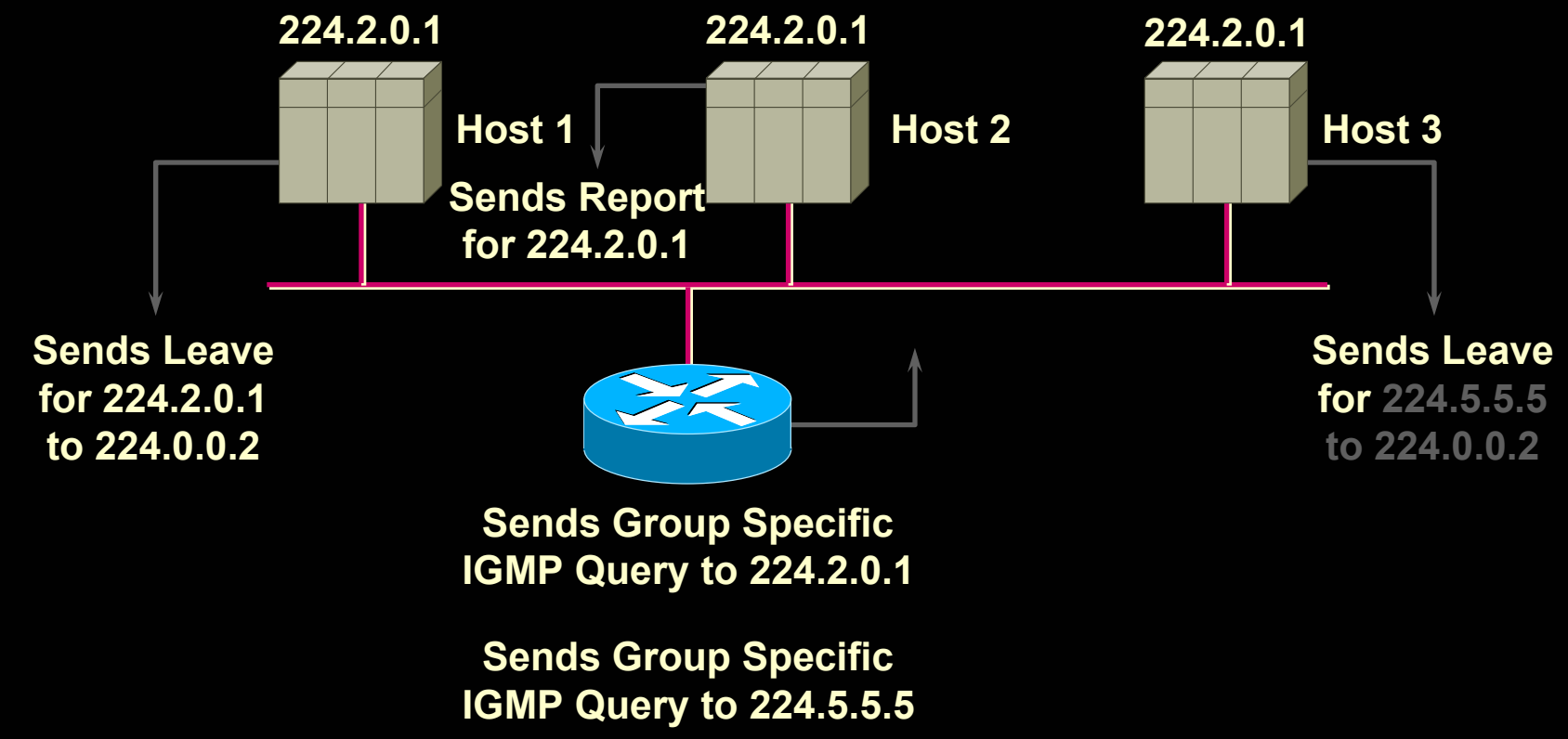
IP Multicast Service Model



IGMP—Joining a Group



IGMP—Leaving a Group



Router To Network

- **Dense Mode Routing Protocols**

- **1. Distance Vector Multicast Routing (DVMRP)**
- **2. Multicast Open Shortest Path First (MOSPF)**
- **3. Protocol Independent Multicast Dense Mode (PIM DM)**

Router To Network (contd.)

- **Sparse Mode Routing Protocols**

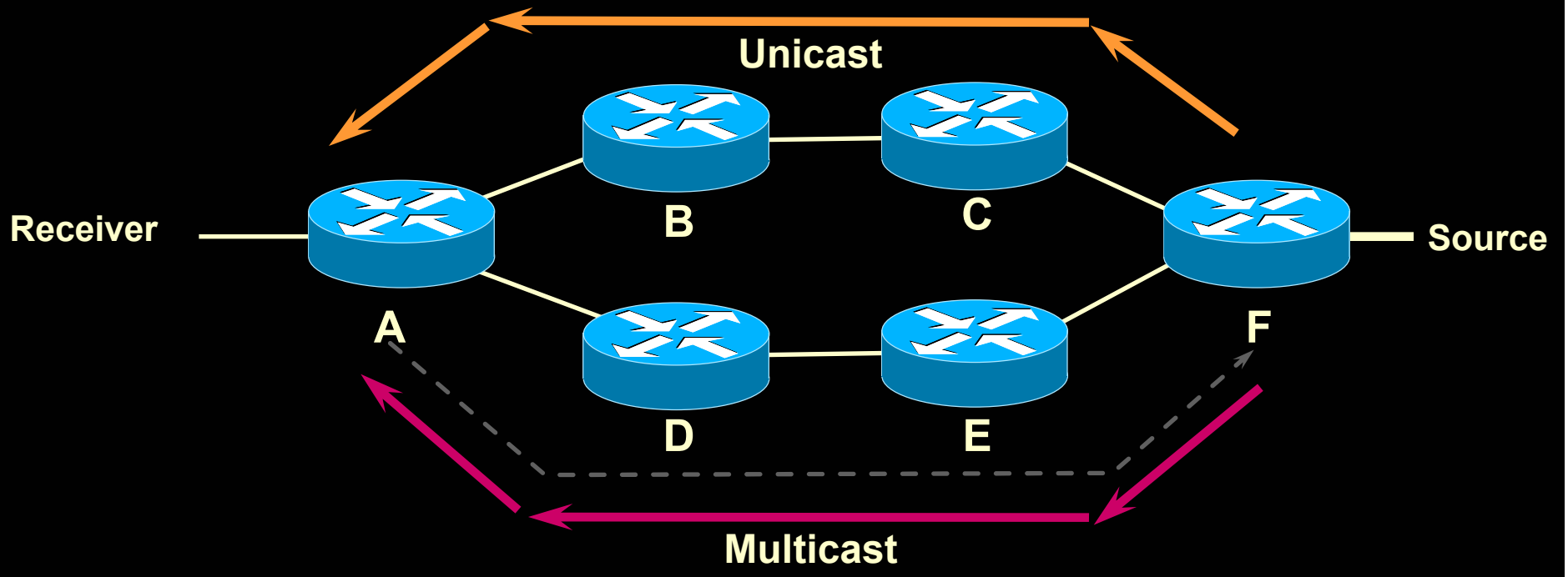
- **1. Core-Based Tree (CBT)**
- **2. Protocol Independent Multicast Sparse Mode (PIM SM)**

PIM DM

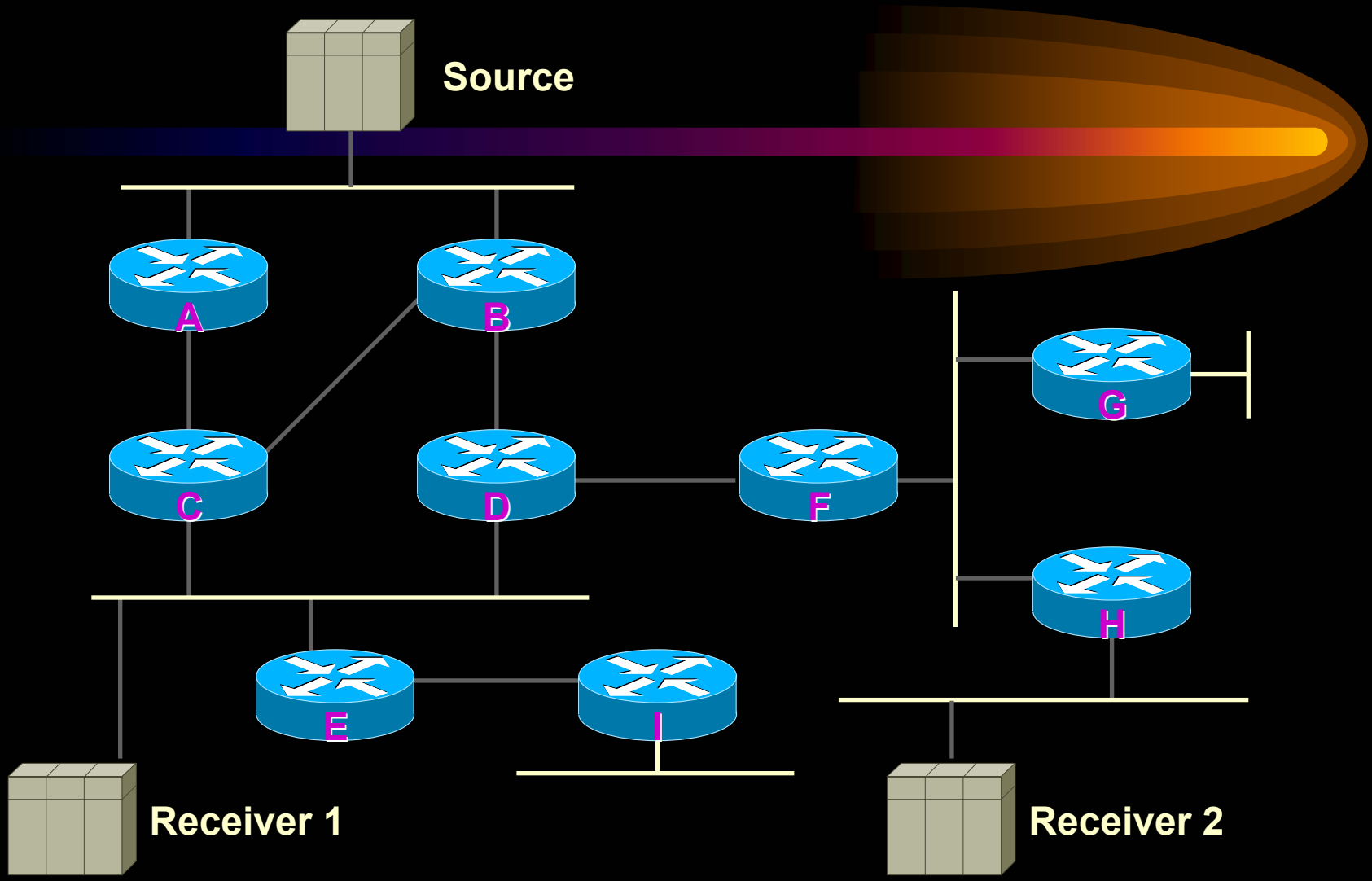
- Protocol Independent Mode – Dense Mode
  - Most widely used type of Multicast
  - Designed to be used with large numbers of recipients
  - Flooding Design
  - Operation has a high initial network overhead
    - Though still less than Unicasting the packets
    - Every router gets every packet unless
      - A Prune message is sent for a particular route
      - These Prune messages have to be resent regularly
  - Used for the broadcast of the Hubble Telescope

Multicast Routing Protocols (Reverse Path Forwarding)

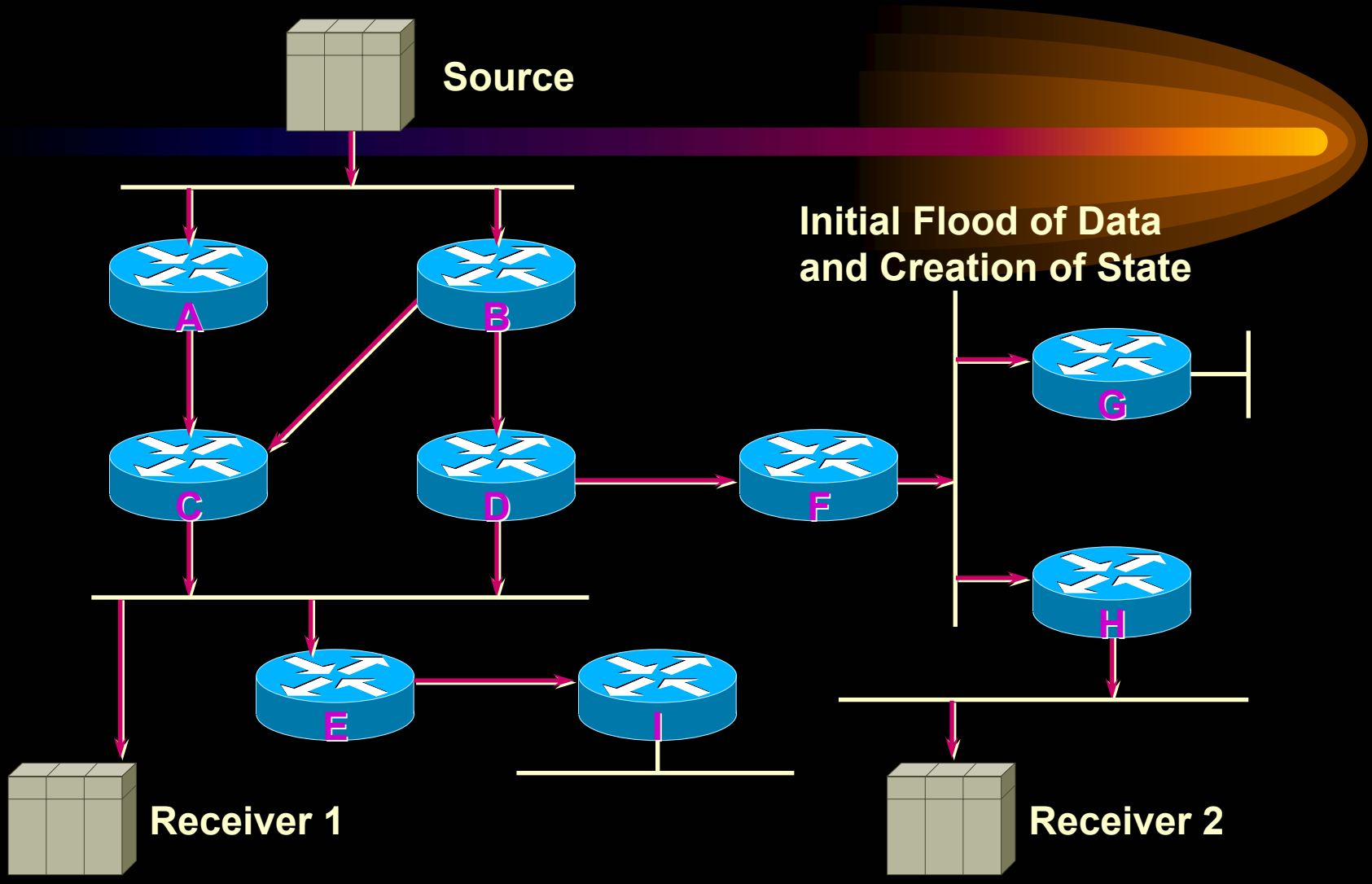
- What is RPF?
  - –A router forwards a multicast datagram if received on the interface used to send unicast datagrams to the source



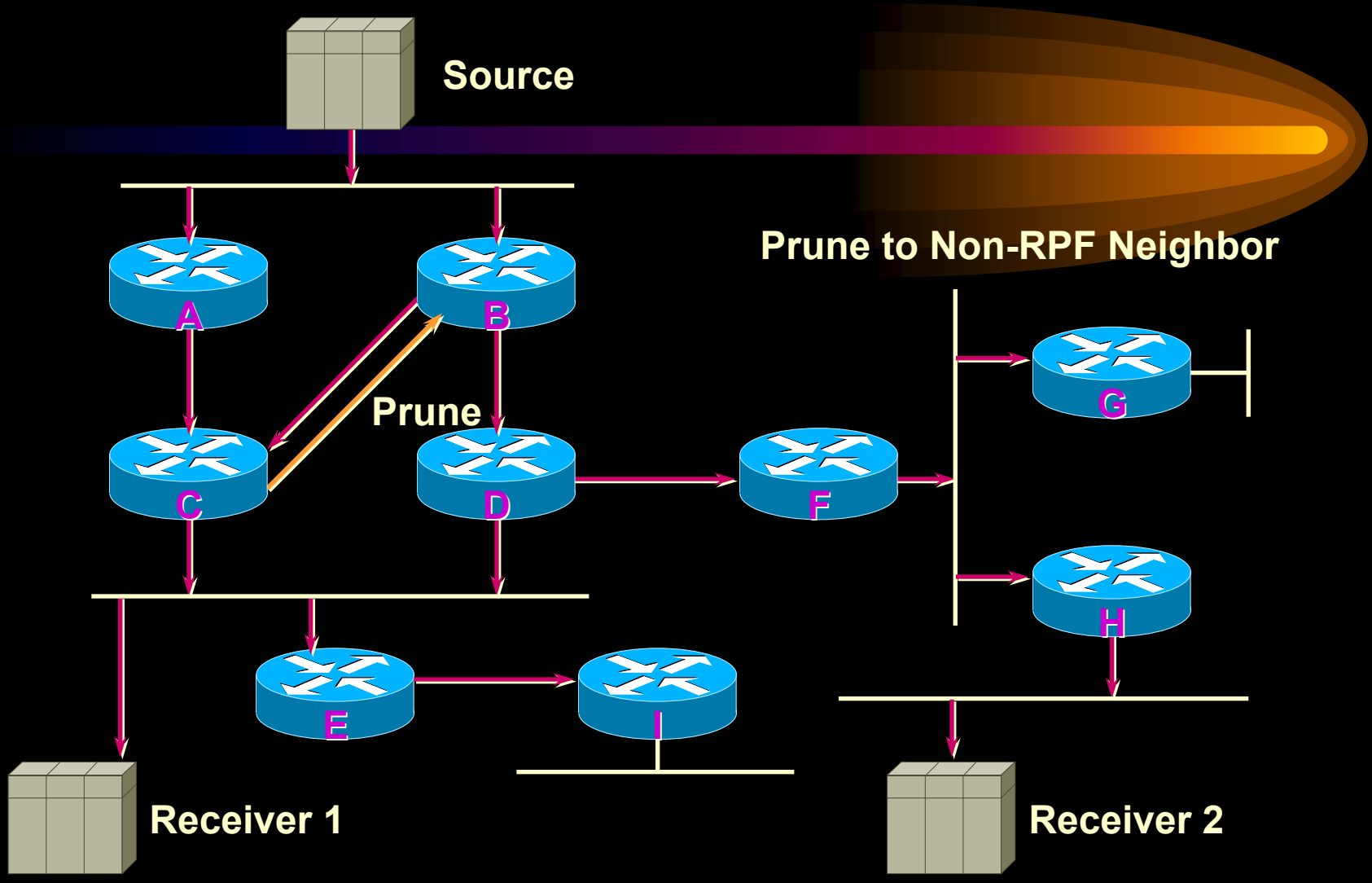
Dense Mode PIM Example



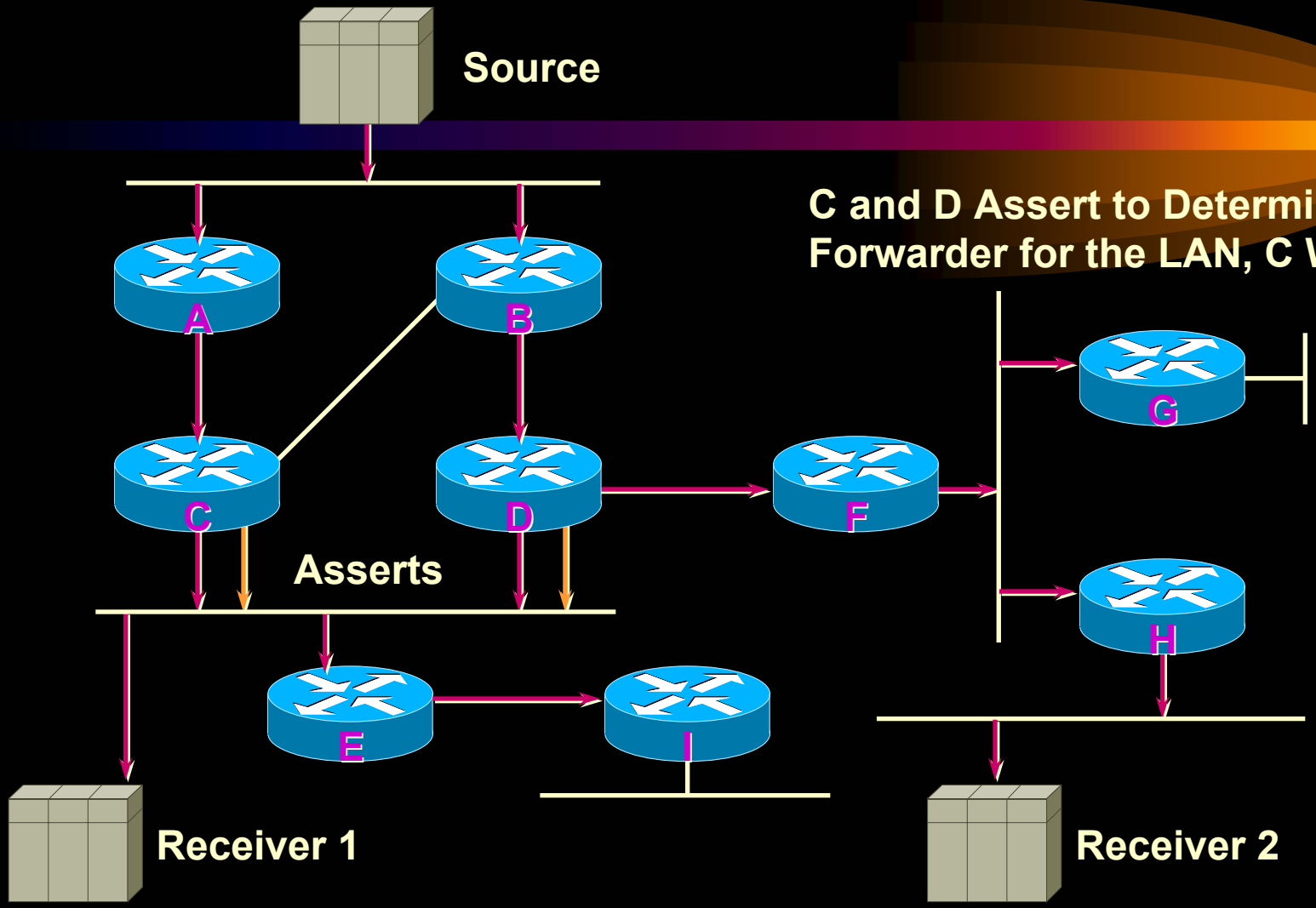
Dense Mode PIM Example



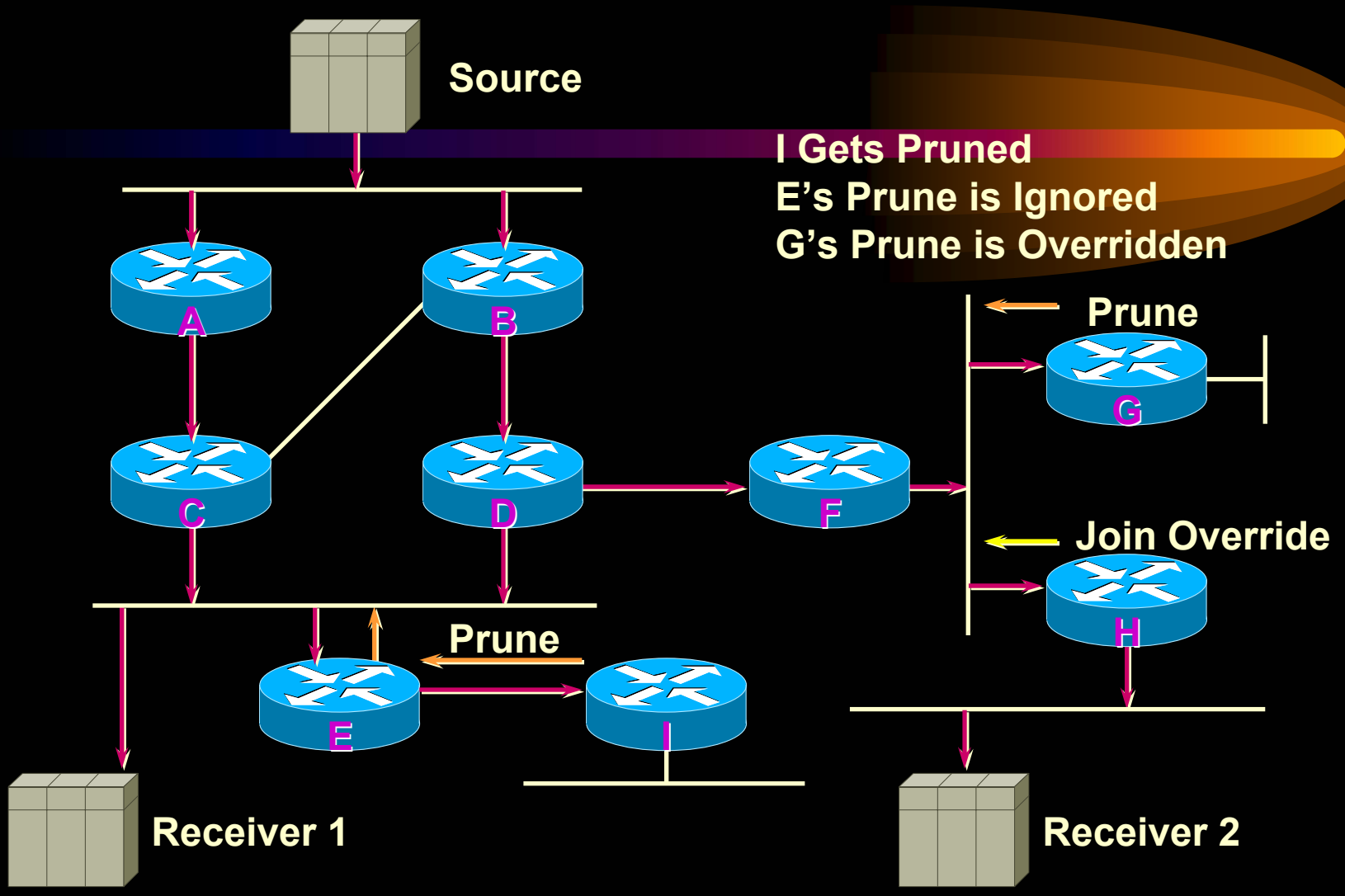
Dense Mode PIM Example



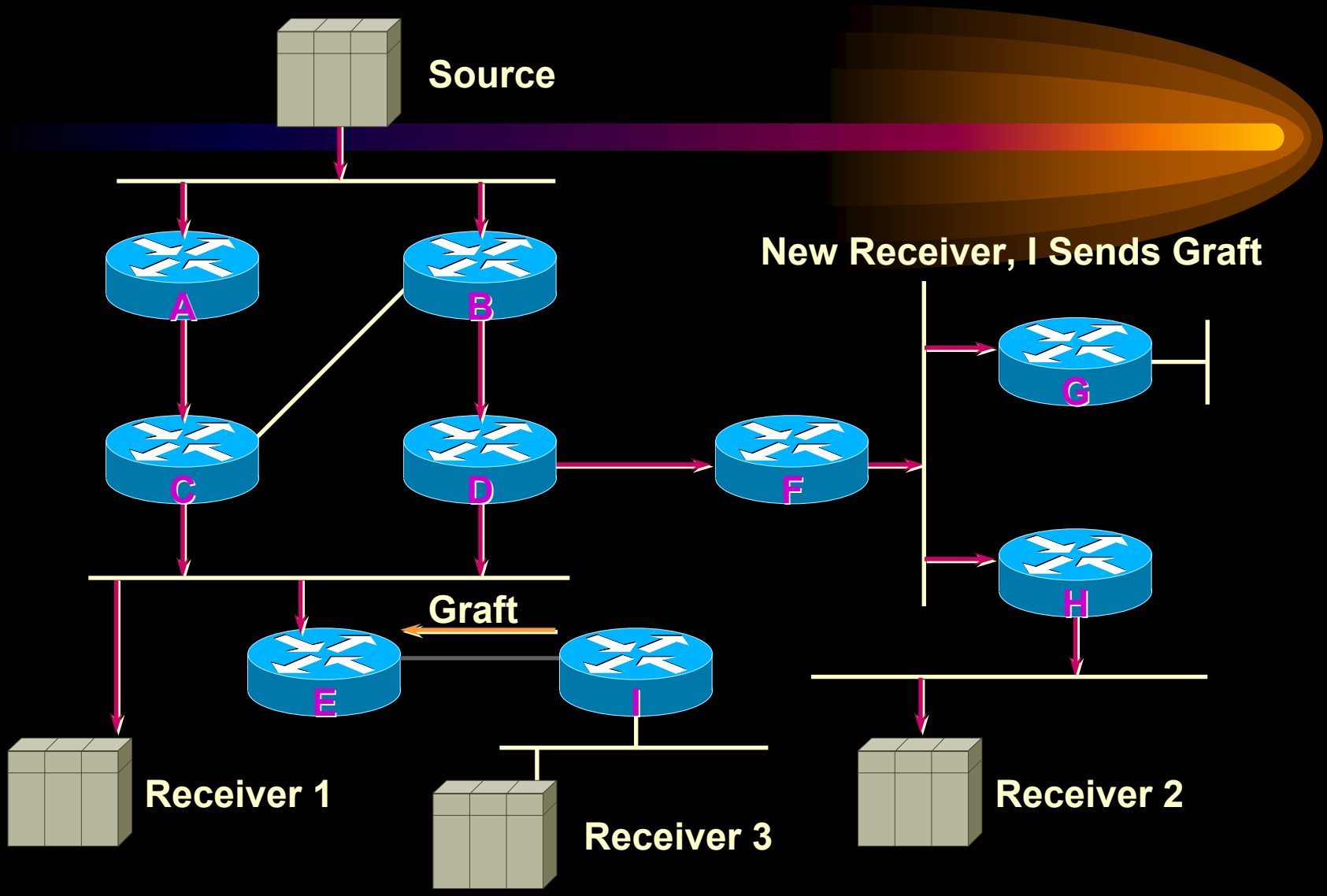
Dense Mode PIM Example



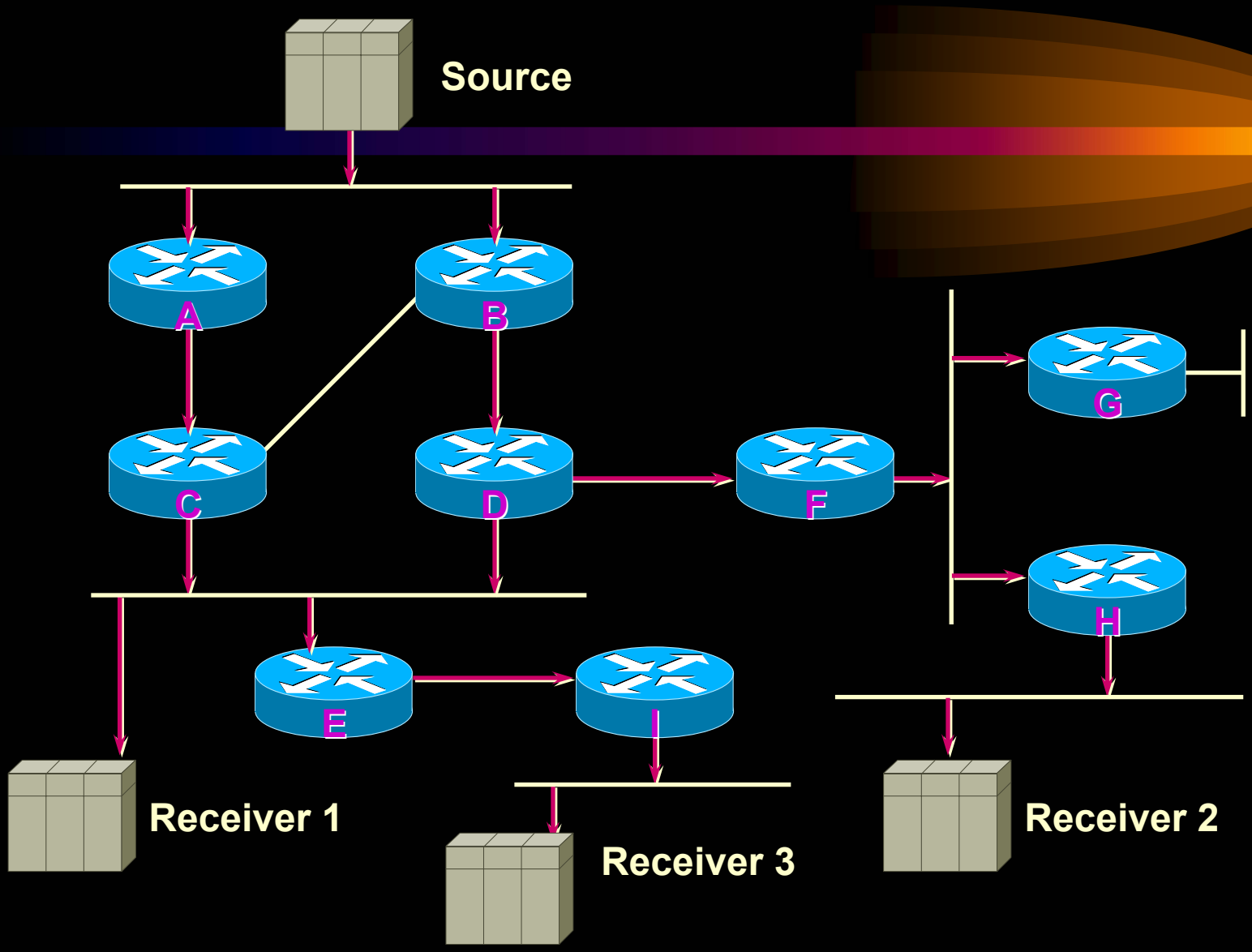
Dense Mode PIM Example



Dense Mode PIM Example



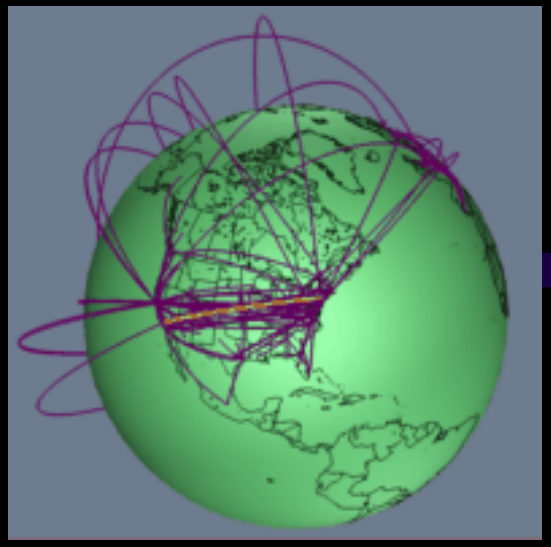
Dense Mode PIM Example

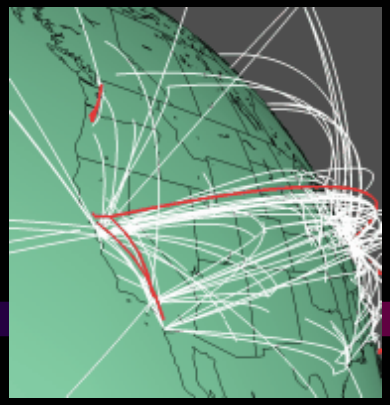


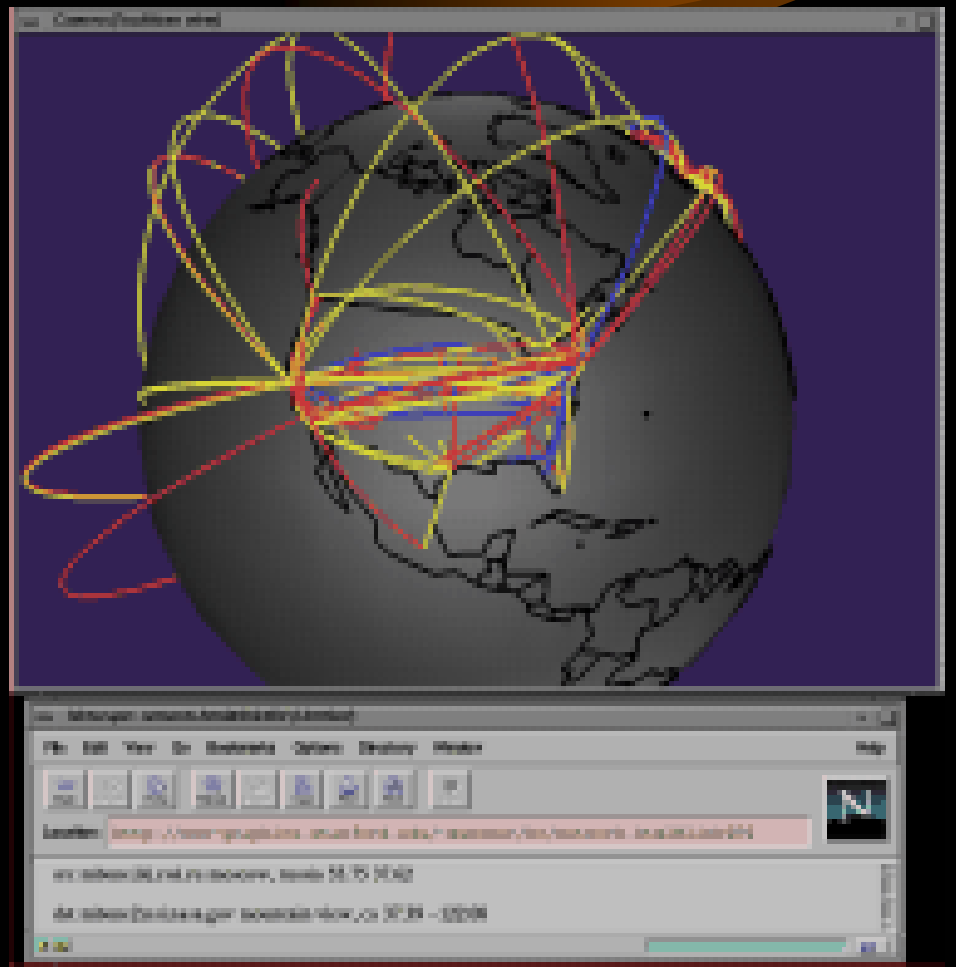
Multicast - Mbone

- Multicast requires Multicast aware routers
  - When first considered these were not available so the Mbone was developed by the IETF.
- Multicast across the Internet requires the Mbone
- Mbone (Multicast Back-Bone)
  - Is a virtual network on the Internet
  - First used in March 1992 with a audio transmission by the IETF
  - Works by encapsulating the Multicast packets inside of Unicast IP Packets
    - Sends these packets to and from Multicast aware routers
    - These routers are supplied by key universities and companies on the Internet

MBONE







Multicast – Issues

- If it so good why do few people know of it?
  - Use of UDP
    - UDP is a non reliable transport method
      - No acknowledgements are given
      - Corrupt packets are just thrown away
      - ‘Windowing’ is not supported by UDP
      - The original server is unaware who is actually receiving these packets
      - If a route is agreed to a host, then a router fails this route does NOT update
  - Packets are sent in a uniform manner and rate
    - The quality of the contents is standard even if the machine can not cope with it
    - The sending rate can not adjust for people on slow connections

Multicast – Issues

- Why use UDP if it is so bad?
  - Consider the environment with a large number of users
    - Packet acknowledgments could block the system
    - Lost/corrupt packets can not be resent by the server
    - Small overhead on the network with UDP packets
    - Features which other protocols support would be of no use with Multicast
      - Windowing
      - Acknowledgment

Security Overview

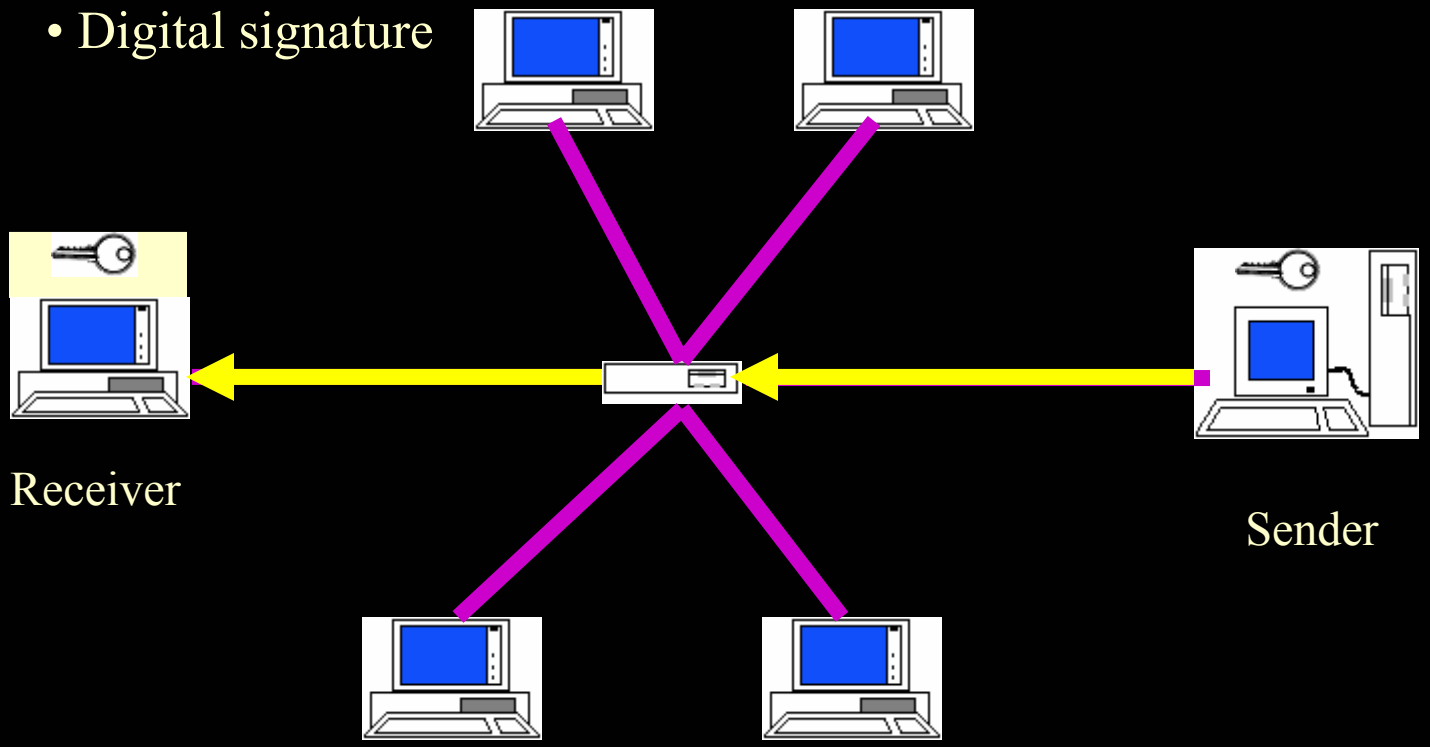
- How does multicast security differ from unicast security?
- What are the vulnerabilities of multicast?
- Different methods of multicast security.

Vulnerabilities of Multicast

- Multicast suffers from increased vulnerability due to:
  - Sessions are frequently advertised
  - Greater number of points of vulnerability
  - Attack affects a broader base of people
  - Attacker can pose as a legitimate user easier (larger “crowd” of principals)

Security in Unicast

- Pre shared keys
- Public key cryptography
- Digital signature



Receiver

Sender

Multicast Group characteristics

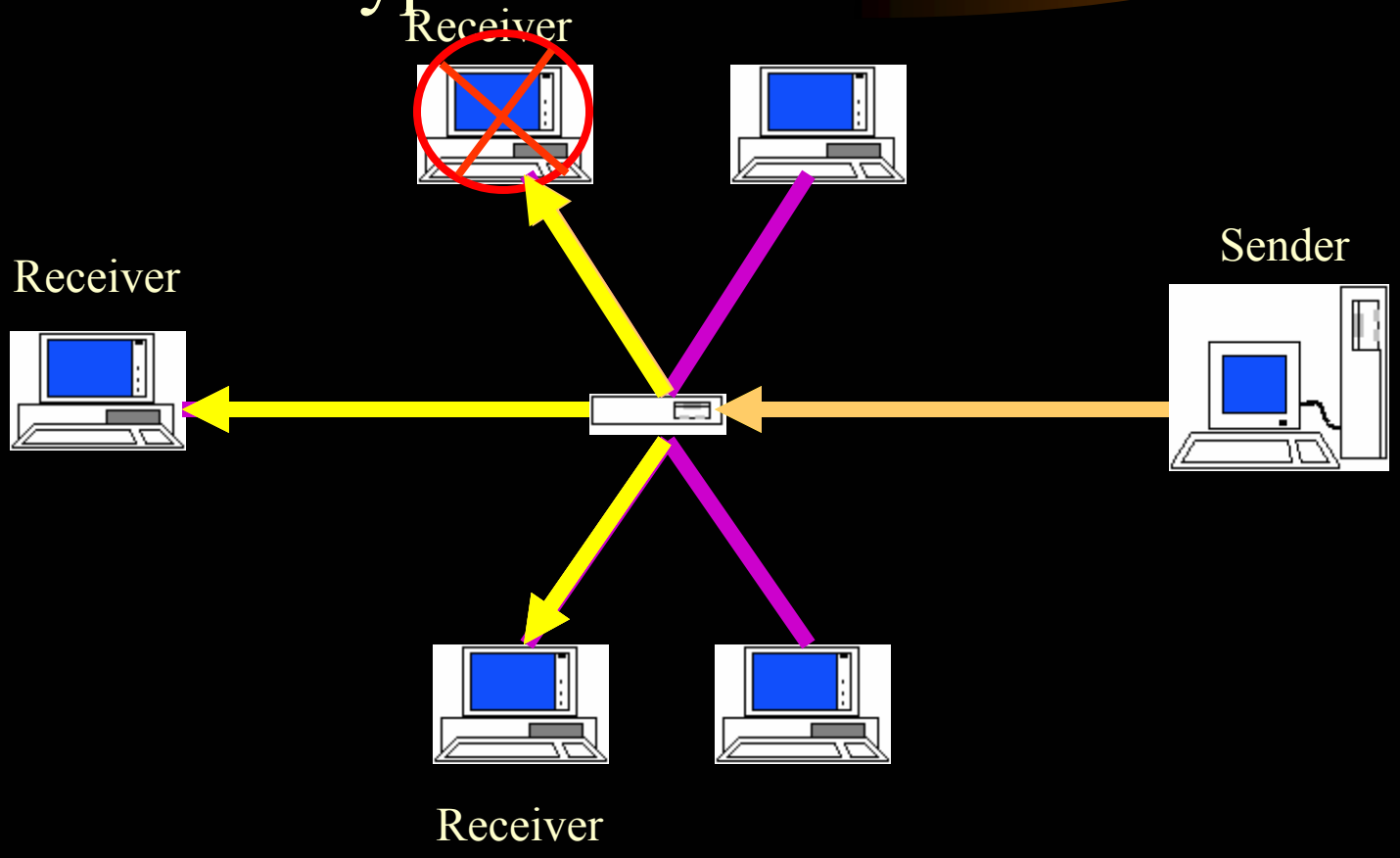
- Group Size
- Dynamic Membership
- Number and types of sender
- Expected life time
- Member characteristics

"1 affects n" Join

- If the entire group shares a single group key (K_{grp}), a new key must be generated ($K`_{grp}$) and distributed (may use $K_{grp}$ to distribute $K`_{grp}$) when a new user joins the group
- Joins exhibit a "1 affects n" scalability failure because they require all members to process the change in K_{grp} when one new member joins

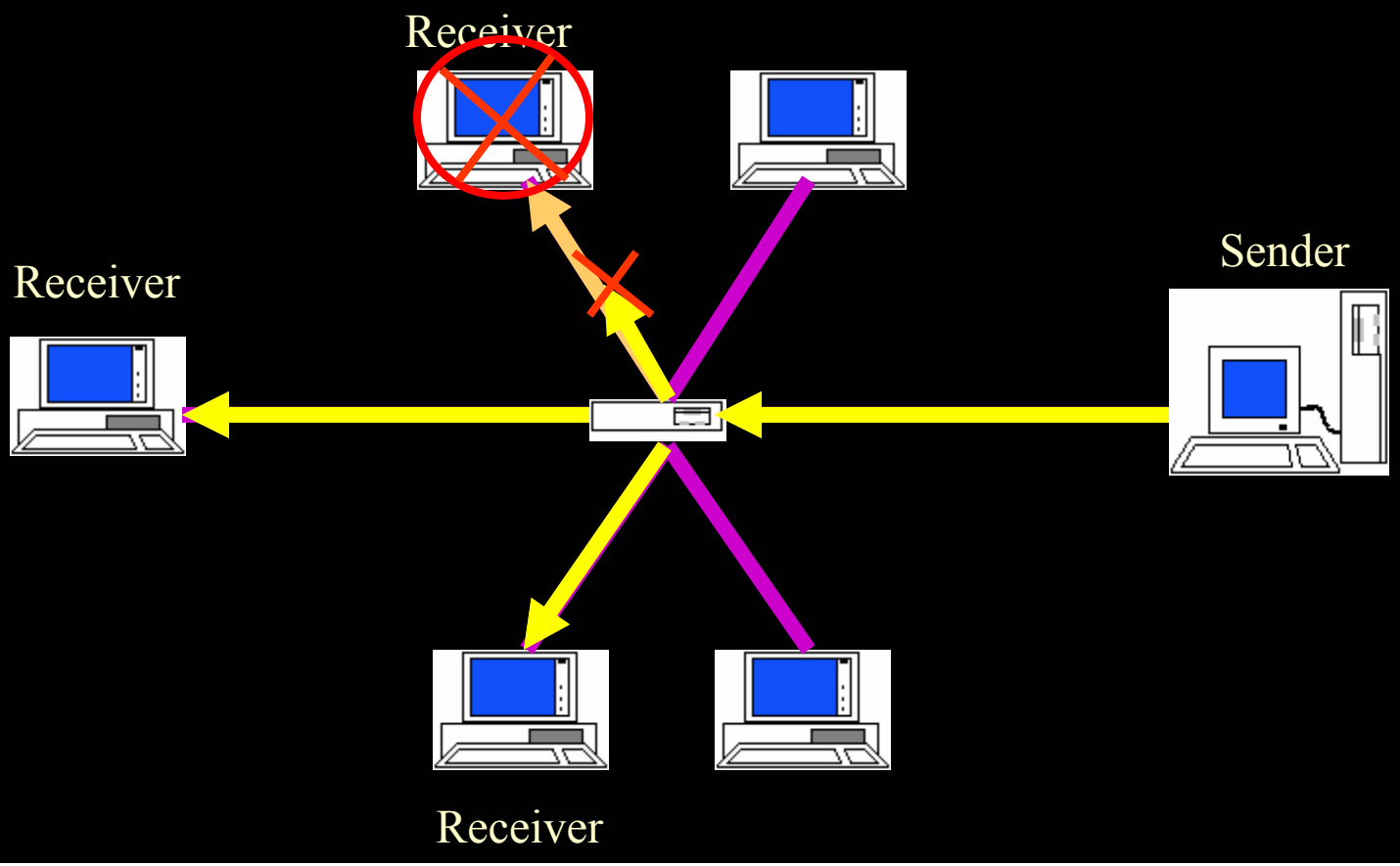
Scalability Problem (Join)

1. 1 affects n type failure



Scalability Problem (Leave)

- ✓ 1 affects n type failure

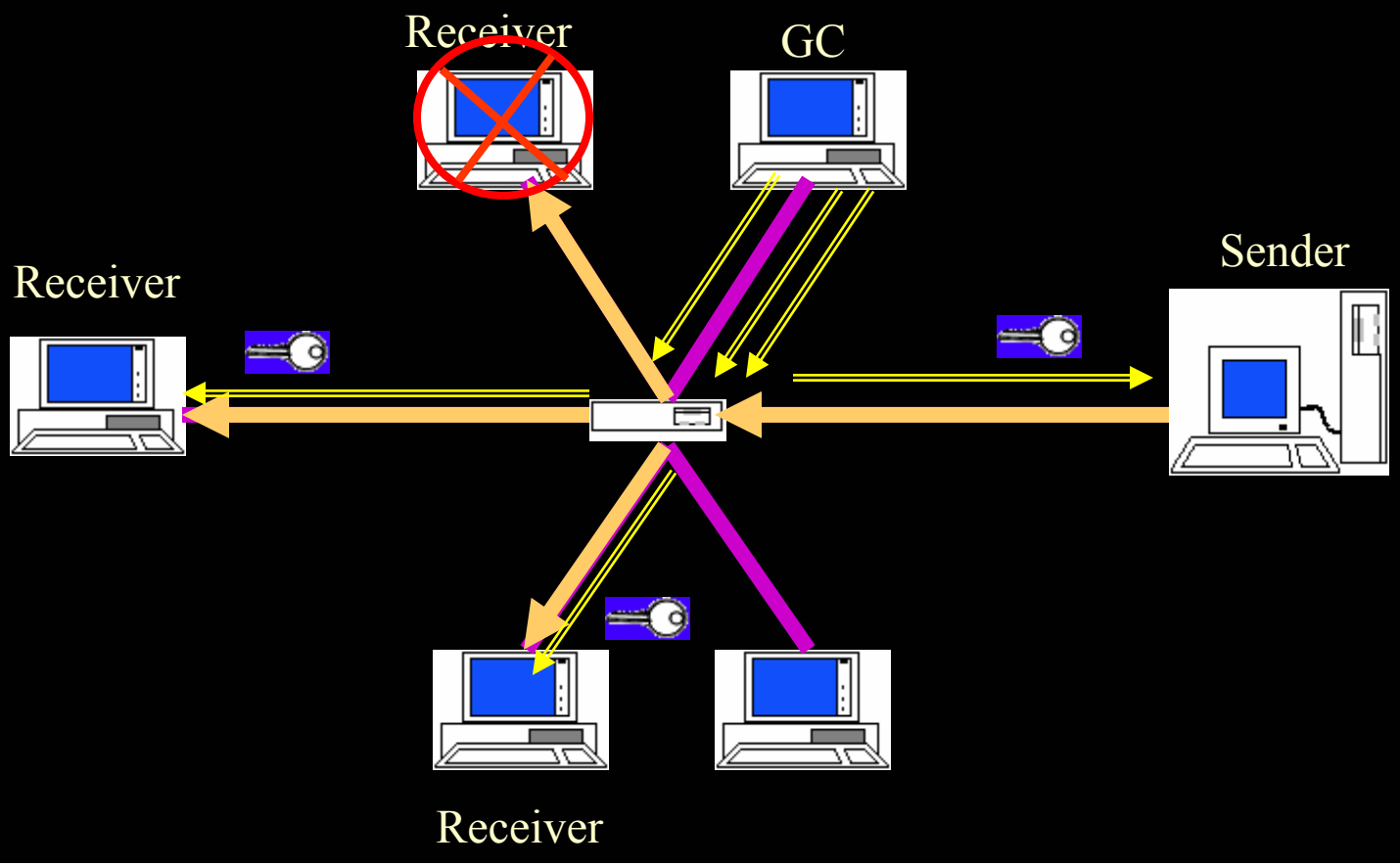


"1 does not equal n" Example

- On leaves, we need to replace K_{grp} with $K`_{grp}$, but we cannot distribute using K_{grp}
- Under basic scheme, we need to unicast the new key to each user individually
- Extremely inefficient in groups with large memberships or highly dynamic memberships

Scalability Problem (Leave)

- ✓ 1 does not affect n type failure



Solution -- The Iolus Approach

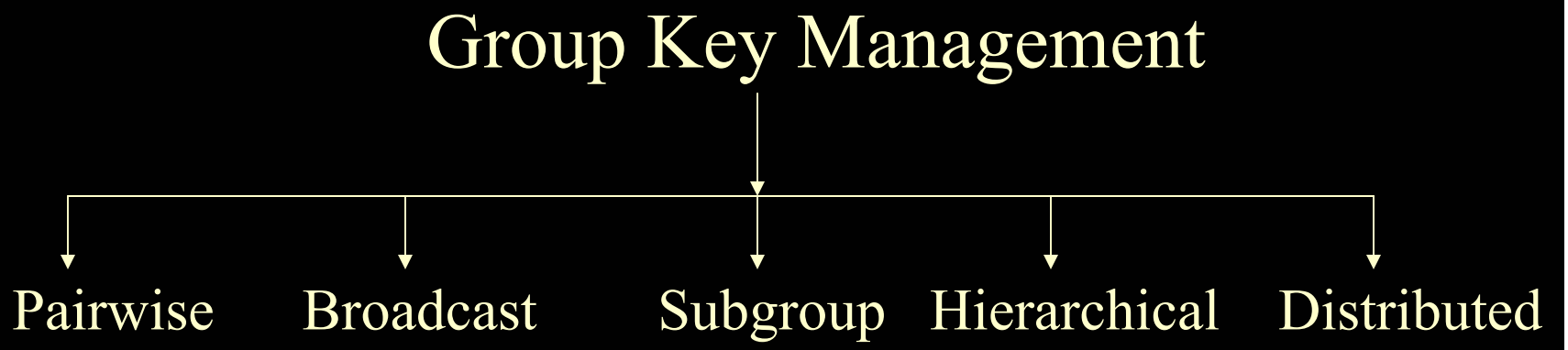
- A hierarchical approach to key distribution
- Uses ‘Secure Agents’ to administer security
- Users join separate local multicast groups

Security Issues

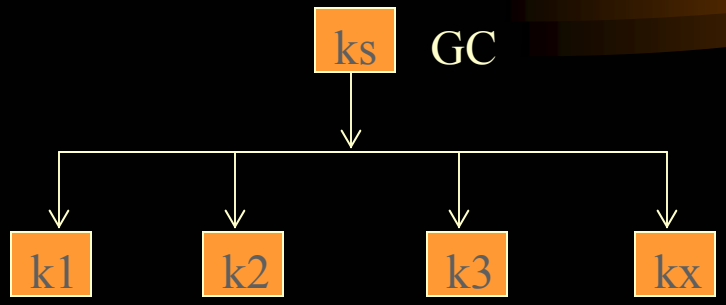
Group Management & Access Control

- Authentication, Integrity and Confidentiality
- Group key distribution
- Joining Members
- Revoking Membership
- Refreshing group key
- Allowing external auditing

Security Considerations



Pairwise



- Simple and straight forward
- GC authenticates the member
- GC sends the group key, encrypted using key mutually shared, to each member
- Not scalable
- e.g. GKMP

Multicast – Future

- Xcast
  - Formerly known as Small Group Multicasting Protocol
  - Developed by IBM research among others
  - Good method of sparse group communication
    - Like a video conference between 10 people
    - Group must be known at the start of the communication
  - Reduces the storage overhead on the routers
  - Stores all of the recipient IP addresses in the packet header
  - Currently being trialled on the Internet2

Demo Programs

- Multicast Chat Program.
- Multicast Audio Transmitter/Receiver.
- Port & IP Scanner (Non Stealth) .
- Ethernet Sniffer .
- Syn Flooder with IP Spoofing .
- Encryption using an PRBS seq. as key

REFERENCES

- RFC – 988 , 1112 , 2365 ,2201 , 1584 , 1075, 2236 .
- Unix Network Programming – Richard Stevans
- Multicast Communication – Ralph Wittman
- Computer Networks – Tenenbhaum
- Websites – www.cisco.com , www.mbone.org , www.ietf.org , www.linuxsecurity.org , www.redhat.com

Multicast – Multicast

Any Questions