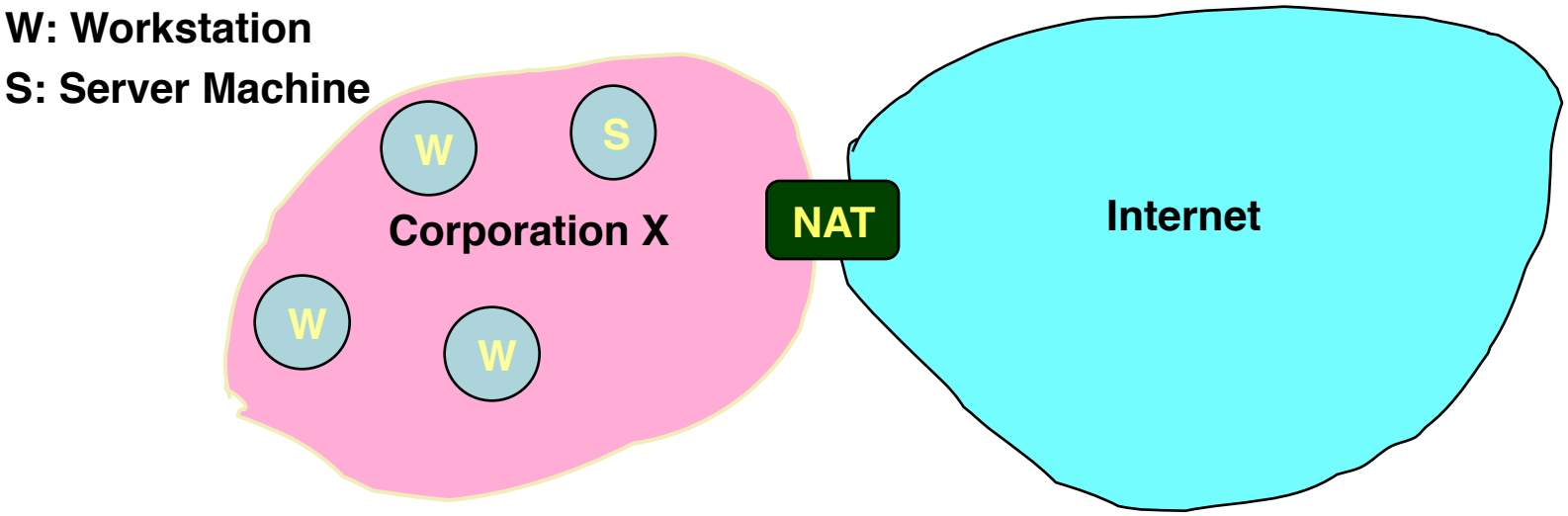
Networks and Distributed Systems

Lecture 12 – NAT and Multicast

Altering the Addressing Model

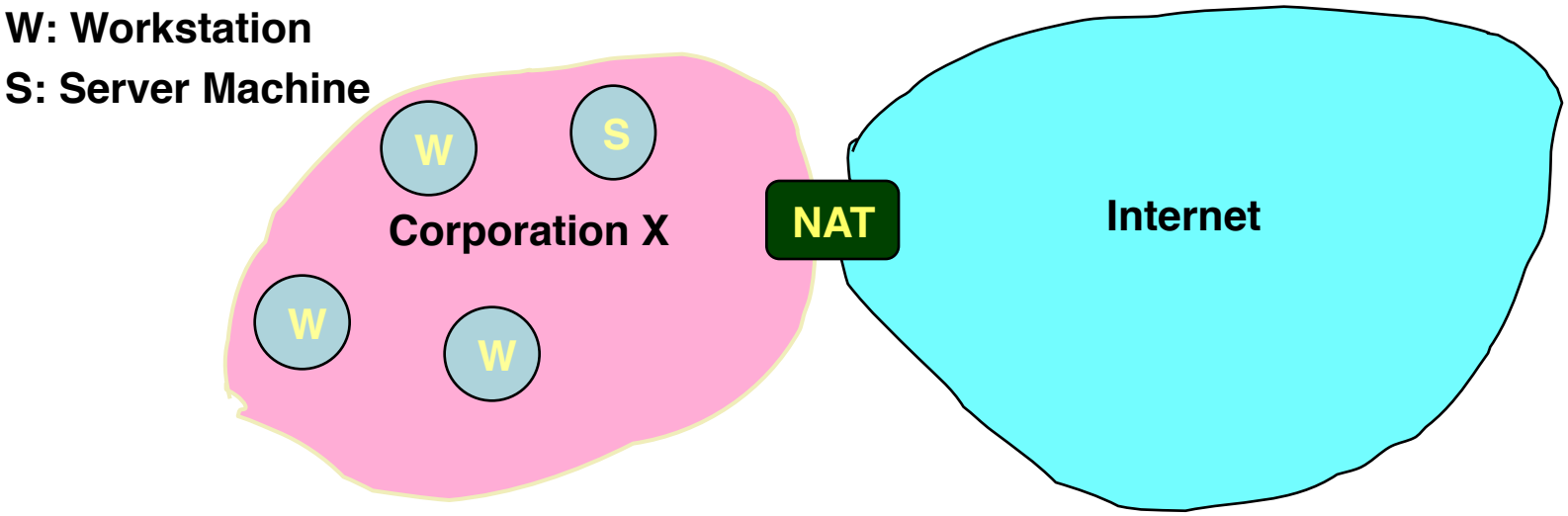
- Original IP Model
  - Every host has a unique IP address
- Implications
  - Any host can find any other host
  - Any host can communicate with any other host
  - Any host can act as a server
    - Just need to know host ID and port number
- No Secrecy or Authentication
  - Packet traffic observable by routers and by LAN-connected hosts
  - Possible to forge packets
    - Use invalid source address

Private Network Accessing - Public Internet



- Don’t have enough IP addresses for every host in organization
- Security
  - Don’t want every machine in organization known to outside world
  - Want to control or monitor traffic in / out of organization

Reducing IP Addresses

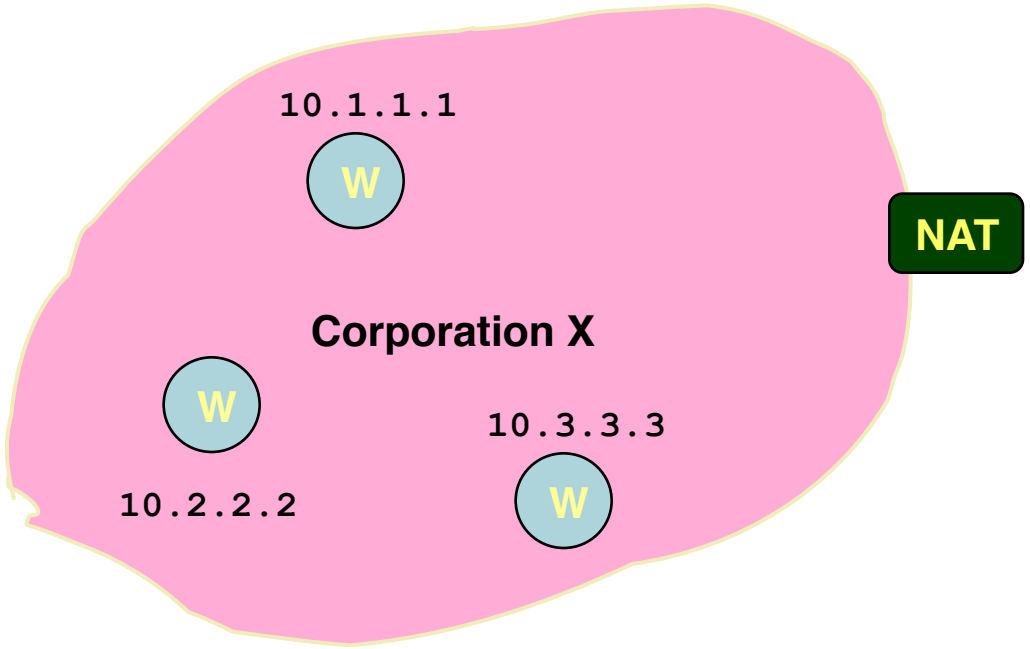


- Most machines within organization are used by individuals
  - "Workstations"
  - For most applications, act as clients
- Small number of machines act as servers for entire organization
  - E.g., mail server
  - All traffic to outside passes through firewall

(Most) machines within organization don't need actual IP addresses!

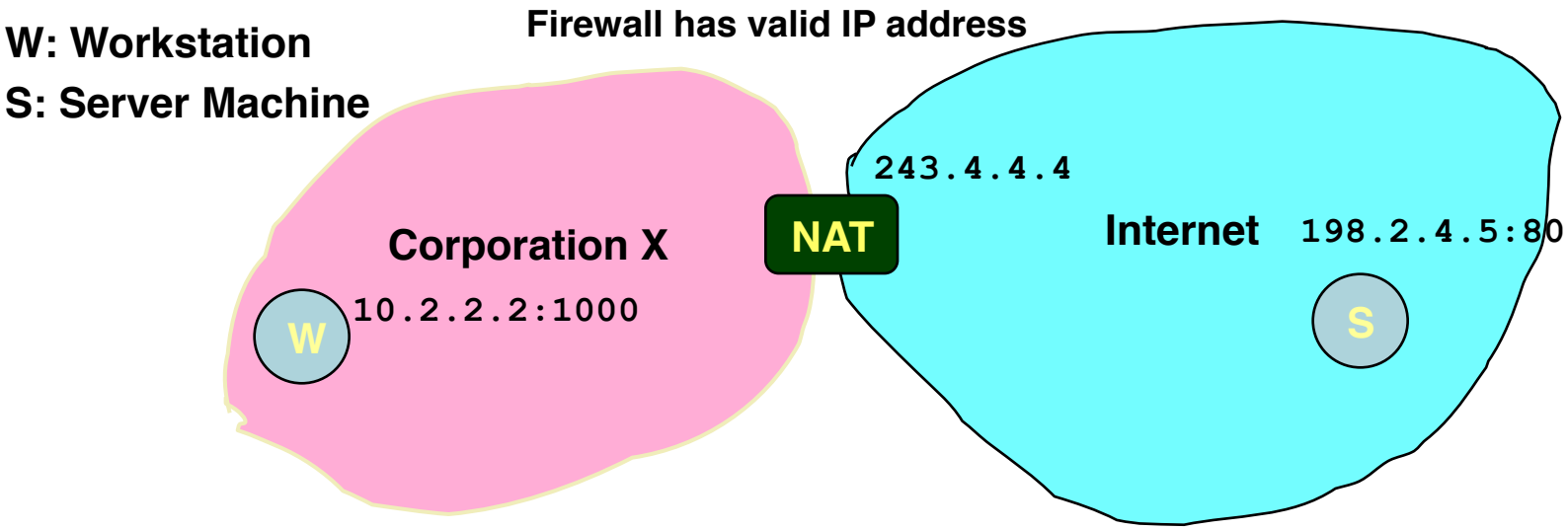
Network Address Translation (NAT)

W: Workstation



- Within Organization
  - Assign every host an unregistered IP address
    - IP addresses 10/8 & 192.168/16 unassigned
  - Route within organization by IP protocol
- Firewall
  - Doesn't let any packets from internal node escape
  - Outside world doesn't need to know about internal addresses

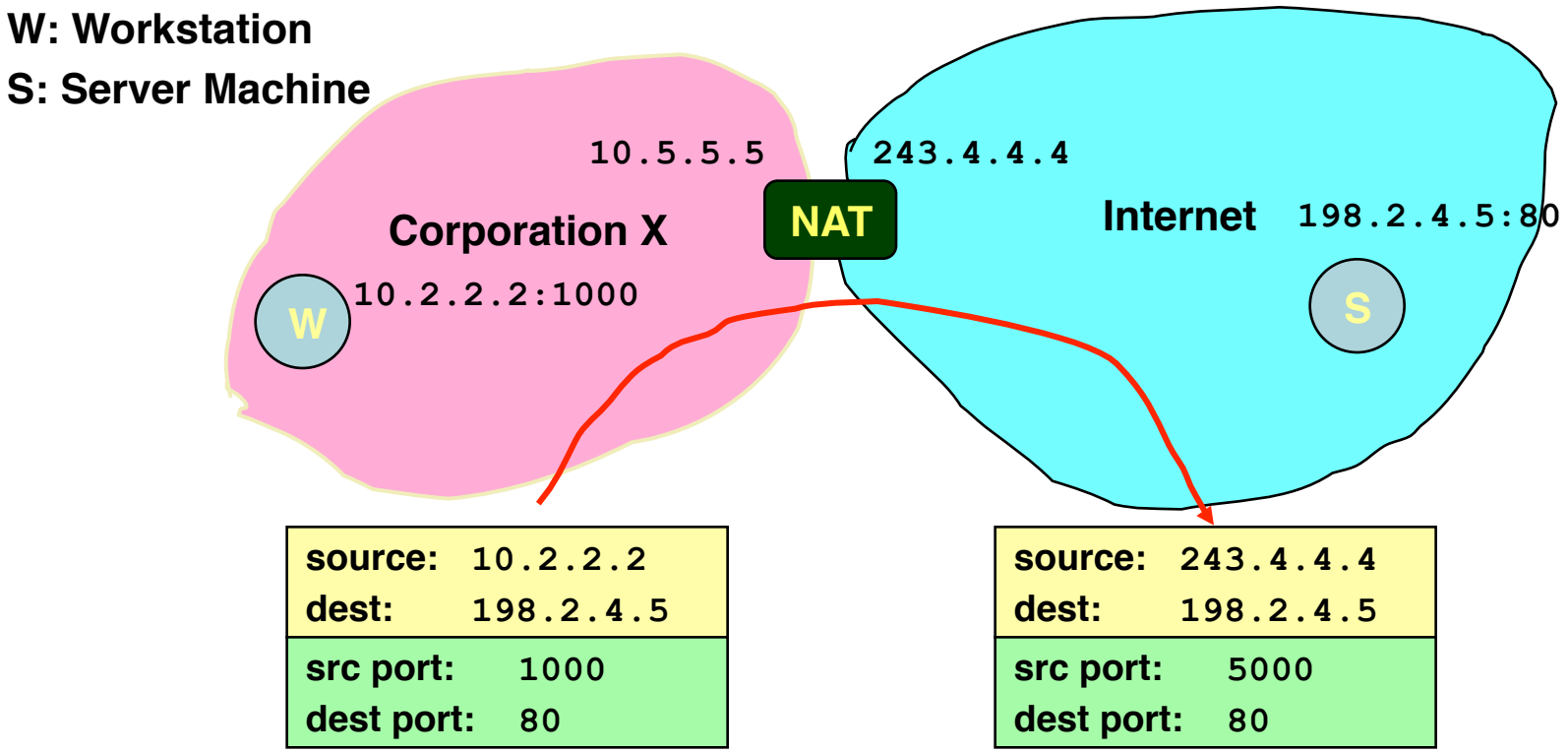
NAT: Opening Client Connection



- Client 10.2.2.2 wants to connect to server 198.2.4.5:80
  - OS assigns ephemeral port (1000)
- Connection request intercepted by firewall
  - Maps client to port of firewall (5000)
  - Creates NAT table entry

Int Addr	Int Port	NAT Port
10.2.2.2	1000	5000

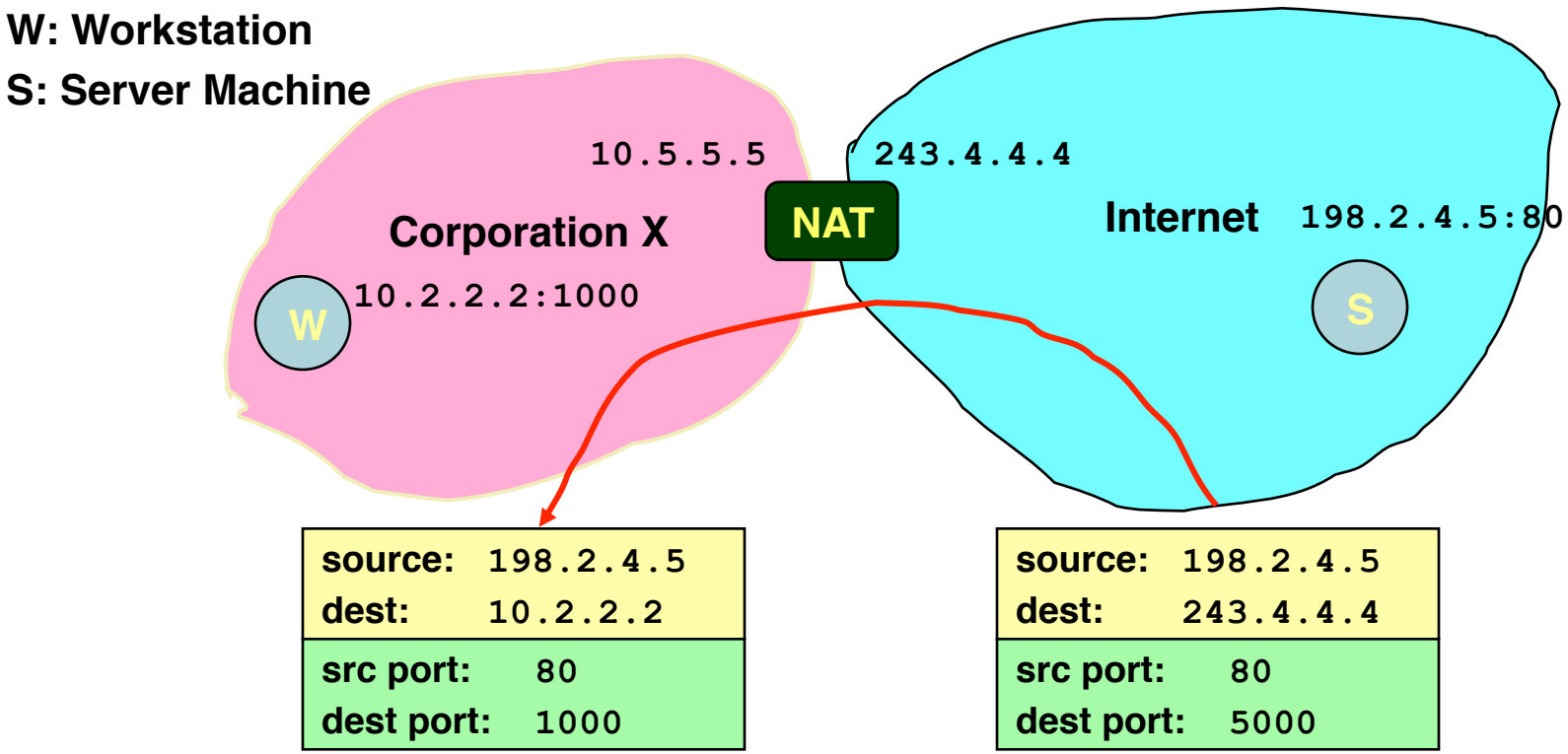
NAT: Client Request



Int Addr	Int Port	NAT Port
10.2.2.2	1000	5000

- Firewall acts as proxy for client
  - Intercepts message from client and marks itself as sender

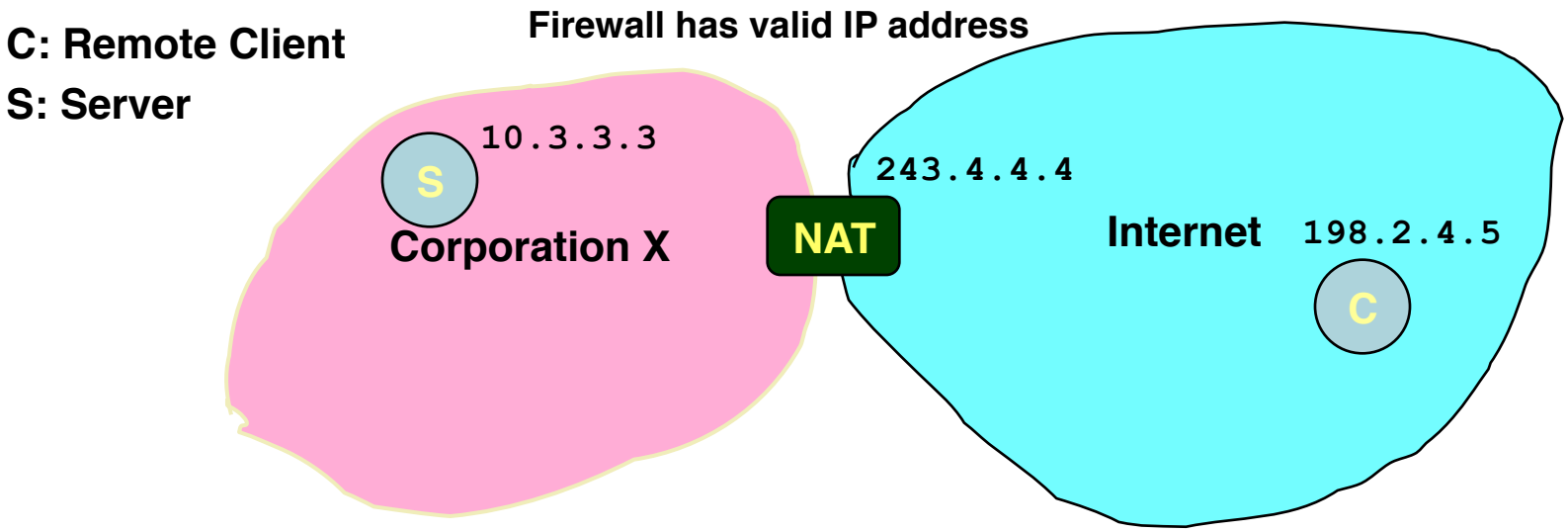
NAT: Server Response



Int Addr	Int Port	NAT Port
10.2.2.2	1000	5000

- Firewall acts as proxy for client
  - Acts as destination for server messages
  - Relabels destination to local addresses

NAT: Enabling Servers



- Use port mapping to make servers available

Int Addr	Int Port	NAT Port
10.3.3.3	80	80

  - Manually configure NAT table to include entry for well-known port
  - External users give address 243.4.4.4:80
  - Requests forwarded to server

Properties of Firewalls with NAT

- Advantages
  - Hides IP addresses used in internal network
    - Easy to change ISP: only NAT box needs to have IP address
    - Fewer registered IP addresses required
  - Basic protection against remote attack
    - Does not expose internal structure to outside world
    - Can control what packets come in and out of system
    - Can reliably determine whether packet from inside or outside
- Disadvantages
  - Contrary to the “open addressing” scheme envisioned for IP addressing
  - Hard to support peer-to-peer applications

NAT Considerations

- NAT has to be consistent during a session.
  - Set up mapping at the beginning of a session and maintain it during the session
    - Recall 2nd level goal 1 of Internet: Continue despite loss of networks or gateways
    - What happens if your NAT reboots?
  - Recycle the mapping at the end of the session
    - May be hard to detect

- NAT only works for certain applications.
  - Some applications (e.g. ftp) pass IP information in payload
  - Need application level gateways to do a matching translation
  - Breaks a lot of applications.

- NAT is loved and hated
  - Breaks many apps (FTP)
  - Inhibits deployment of new applications like p2p (but so do firewalls!)
  + Little NAT boxes make home networking simple.
  + Saves addresses. Makes allocation simple.

Internet Multicast

Overview

- IPv4
  - class D addresses
  - uses tunneling
- Integral part of IPv6
  - problem is making it scale

Overview

- One-to-many
  - Radio station broadcast
  - Transmitting news, stock-price
  - Software updates to multiple hosts
- Many-to-many
  - Multimedia teleconferencing
  - Online multi-player games
  - Distributed simulations

Overview

- Without support for multicast
  - A source needs to send a separate packet with the identical data to each member of the group
    - This redundancy consumes more bandwidth
    - Redundant traffic is not evenly distributed, concentrated near the sending host
  - Source needs to keep track of the IP address of each member in the group
    - Group may be dynamic
- To support many-to-many and one-to-many IP provides an IP-level multicast

Overview

- Basic IP multicast model is many-to-many based on multicast groups
  - Each group has its own IP multicast address
  - Hosts that are members of a group receive copies of any packets sent to that group's multicast address
  - A host can be in multiple groups
  - A host can join and leave groups

Overview

- Using IP multicast to send the identical packet to each member of the group
  - A host sends a single copy of the packet addressed to the group's multicast address
  - The sending host does not need to know the individual unicast IP address of each member
  - Sending host does not send multiple copies of the packet

Overview

- IP's original many-to-many multicast has been supplemented with support for a form of one-to-many multicast
- One-to-many multicast
  - Source specific multicast (SSM)
  - A receiving host specifies both a multicast group and a specific sending host
- Many-to-many model
  - Any source multicast (ASM)

Overview

- A host signals its desire to join or leave a multicast group by communicating with its local router using a special protocol
  - In IPv4, the protocol is Internet Group Management Protocol (IGMP)
  - In IPv6, the protocol is Multicast Listener Discovery (MLD)
- The router has the responsibility for making multicast behave correctly with regard to the host

Multicast Routing

- A router's unicast forwarding tables indicate for any IP address, which link to use to forward the unicast packet
- To support multicast, a router must additionally have multicast forwarding tables that indicate, based on multicast address, which links to use to forward the multicast packet
  - Unicast forwarding tables collectively specify a set of paths
  - Multicast forwarding tables collectively specify a set of trees
    - Multicast distribution trees

Multicast Routing

- To support source specific multicast, the multicast forwarding tables must indicate which links to use based on the combination of multicast address and the unicast IP address of the source

- Multicast routing is the process by which multicast distribution trees are determined

Distance-Vector Multicast

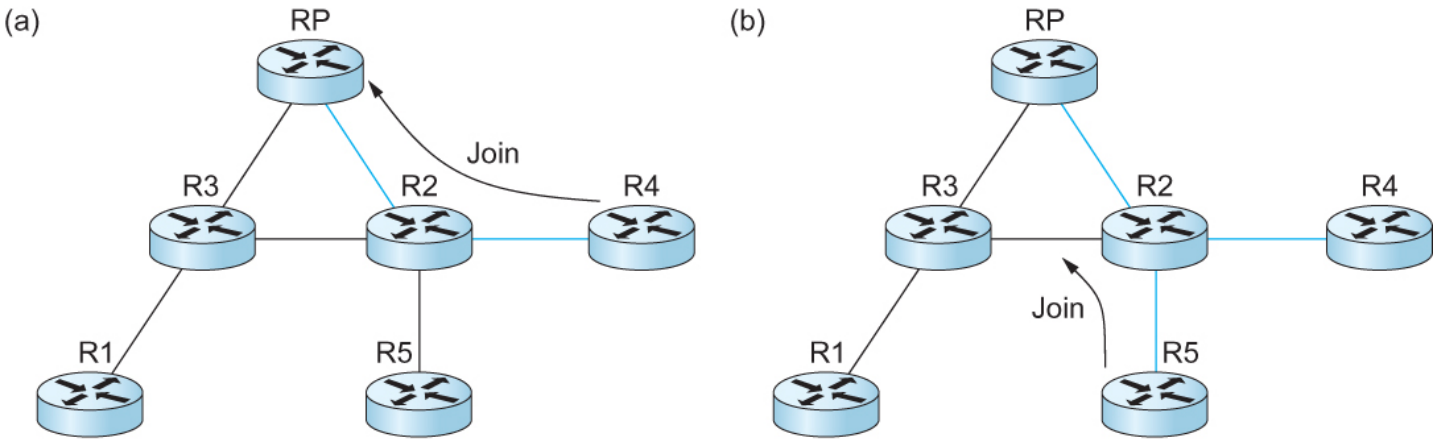
- Each router already knows that shortest path to source S goes through router N.
- When receive multicast packet from S, forward on all outgoing links (except the one on which the packet arrived), iff packet arrived from N.
- Eliminate duplicate broadcast packets by only letting
  - "parent" for LAN (relative to S) forward
    - shortest path to S (learn via distance vector)
    - smallest address to break ties

Distance-Vector Multicast

Reverse Path Broadcast (RPB)

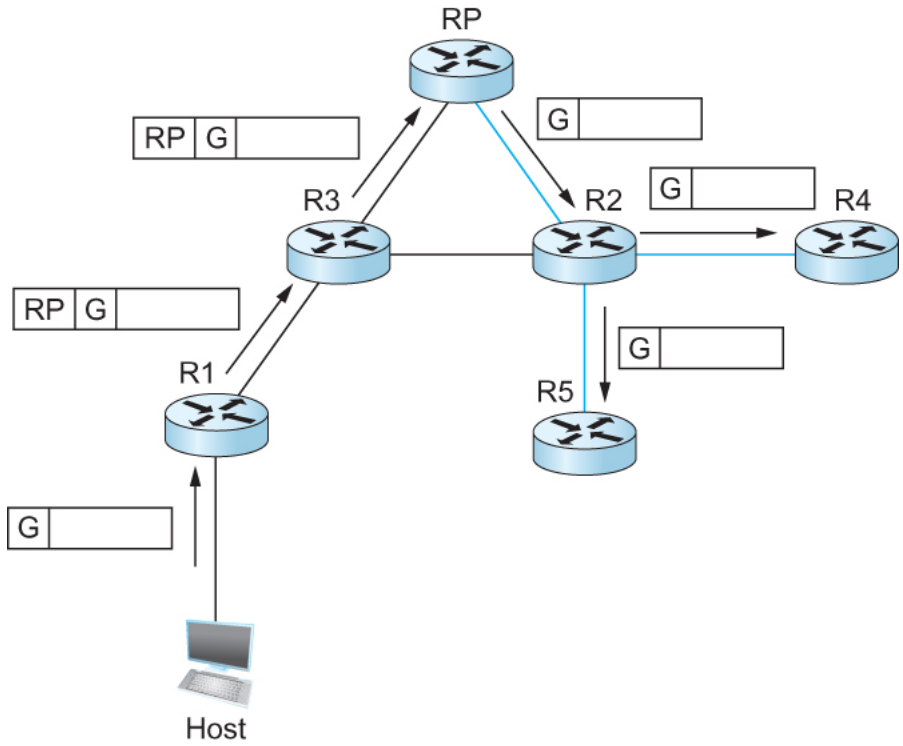
- Goal: Prune networks that have no hosts in group G
- Step 1: Determine if LAN is a *leaf* with no members in G
  - leaf if parent is only router on the LAN
  - determine if any hosts are members of G using IGMP
- Step 2: Propagate "no members of G here" information
  - augment `<Destination, Cost>` update sent to neighbors with set of groups for which this network is interested in receiving multicast packets.
  - only happens when multicast address becomes active.

Protocol Independent Multicast (PIM)



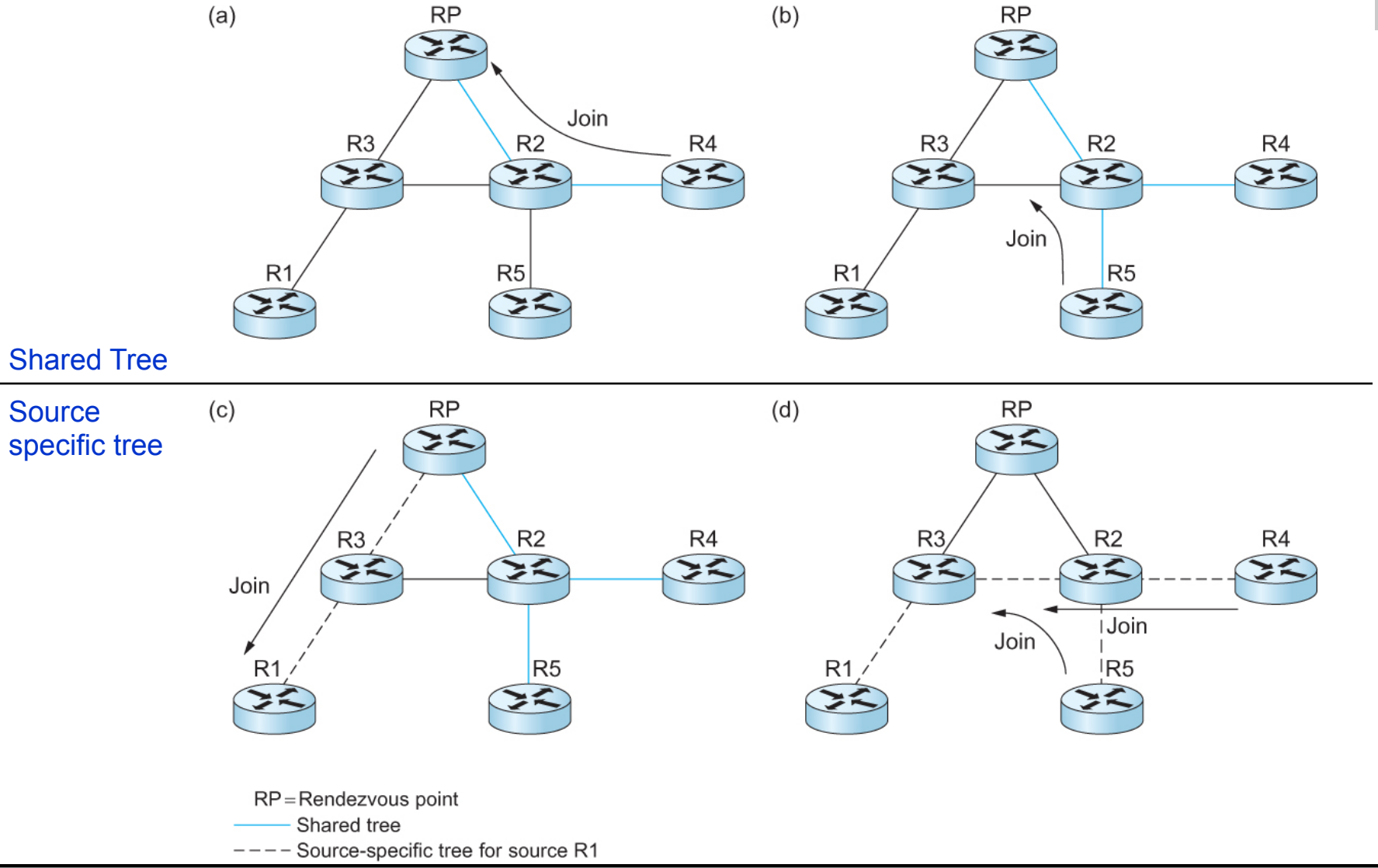
Shared Tree

Protocol Independent Multicast (PIM)



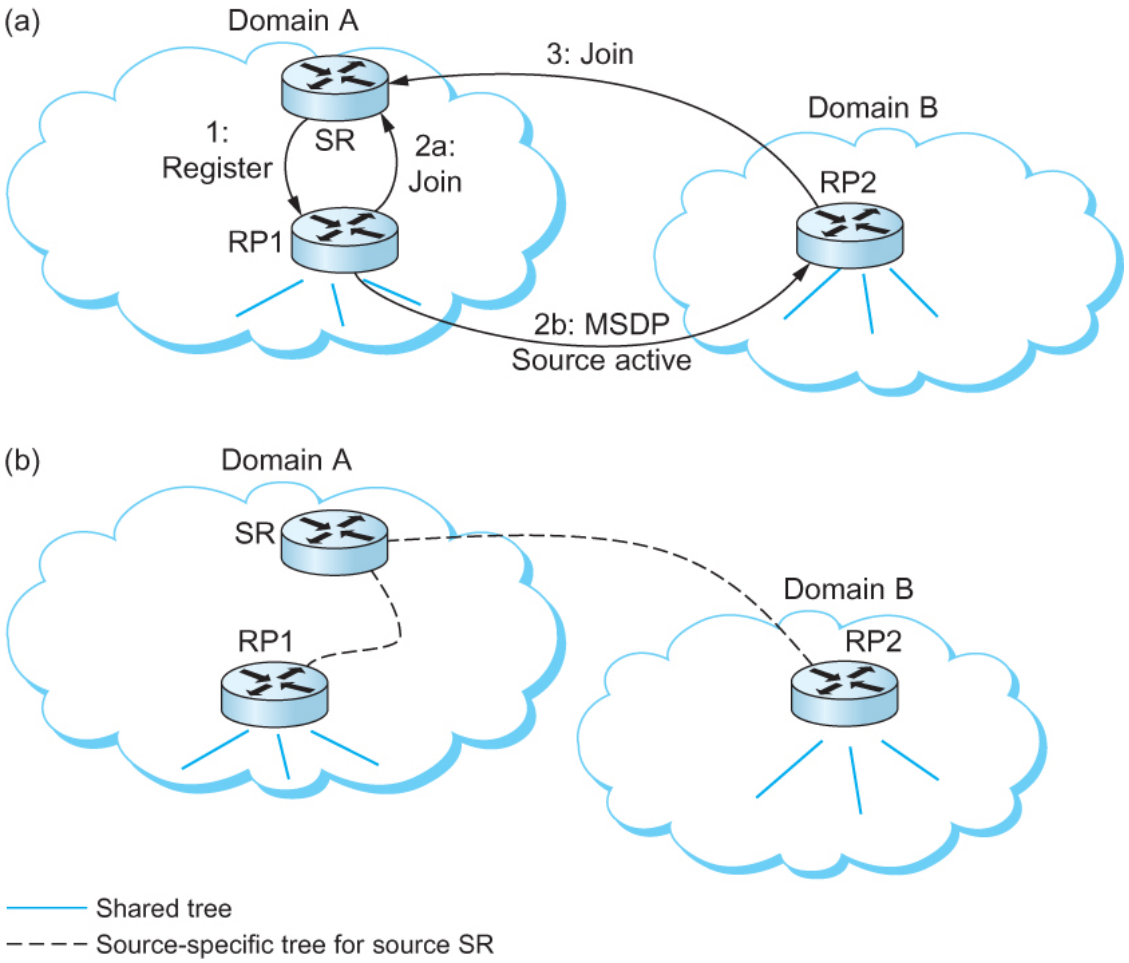
Delivery of a packet along a shared tree. R1 tunnels the packet to the RP, which forwards it along the shared tree to R4 and R5.

Protocol Independent Multicast (PIM)



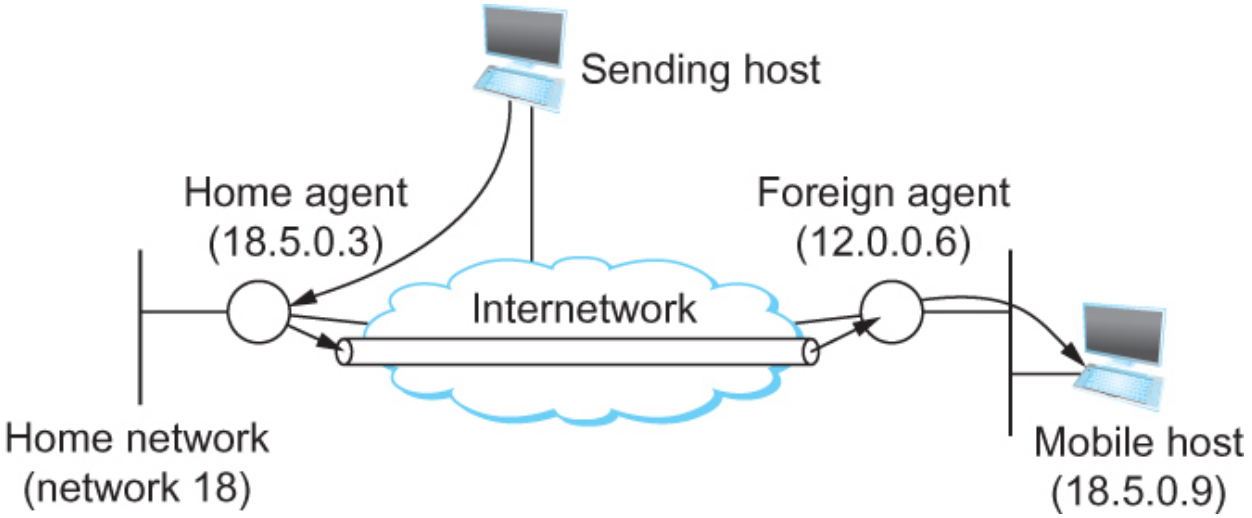
Inter-domain Multicast

Multicast Source Discovery Protocol (MSDP)



Routing for Mobile Hosts

- Mobile IP
  - *home agent*
    - Router located on the home network of the mobile hosts
  - *home address*
    - The permanent IP address of the mobile host.
    - Has a network number equal to that of the home network and thus of the home agent
  - *foreign agent*
    - Router located on a network to which the mobile node attaches itself when it is away from its home network



Routing for Mobile Hosts

- Problem of delivering a packet to the mobile node
  - How does the home agent intercept a packet that is destined for the mobile node?
    - Proxy ARP
  - How does the home agent then deliver the packet to the foreign agent?
    - IP tunnel
    - Care-of-address
  - How does the foreign agent deliver the packet to the mobile node?

Routing for Mobile Hosts

- Route optimization in Mobile IP
  - The route from the sending node to mobile node can be significantly sub-optimal
  - One extreme example
    - The mobile node and the sending node are on the same network, but the home network for the mobile node is on the far side of the Internet
      - Triangle Routing Problem
  - Solution
    - Let the sending node know the care-of-address of the mobile node. The sending node can create its own tunnel to the foreign agent
    - Home agent sends binding update message
    - The sending node creates an entry in the binding cache
    - The binding cache may become out-of-date
      - The mobile node moved to a different network
      - Foreign agent sends a binding warning message