CS 640 Introduction to Computer Networks

Lecture 24

Today's lecture

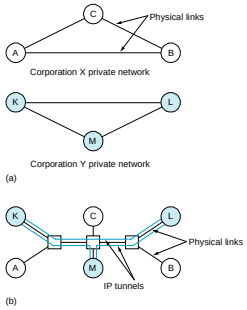
- VPNs
- Mobile IP

Why restrict reachability?

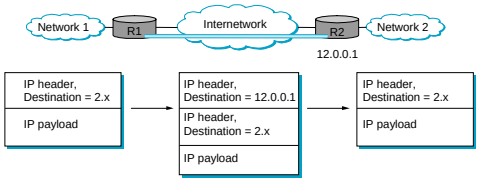
- Security – multiple defenses
  - Sometimes you don't want some computers to communicate with the outside world
- Performance
  - Protect the performance of virtual networks from the effects of the rest of the traffic
  - VLANs cut down on broadcast traffic
- But sharing infrastructure reduces costs!!!

VPNs

- Internal traffic between offices needs “more security” than traffic to the Internet
- Using same physical links cheaper because of statistical multiplexing



Tunneling



Forwarding table for R1

Network	Next hop
Network 1	Interface 1
Network 2	Virtual interface 2
Default	Interface 3

MPLS (MultiProtocol Label Switching)

- Circuit switching technology developed to work with IP
  - Can use IP control plane (routing)
  - Can control paths explicitly
  - Convert ATM switches with software update
- Uses 32 bit “shim header” between layer 2 and 3 headers
  - 20 bit link-local labels

MPLS (contd.)

- Label Switching Routers (LSRs) inside the network forward packets based on exact lookups of MPLS labels
- Label Edge Routers (LERs) still need to perform longest matching prefix lookup to determine first label
- MPLS used for
  - VPNs
  - Traffic engineering

Today's lecture

- VPNs
- Mobile IP

Portable Networking Technology

- Cellular systems
  - Cellular Digital Packet Data (CDPD)
  - 3G
- Bluetooth
  - Cheap, short range radio links for mobile devices
- Wireless Ethernet (802.11)
  - Widely used wireless MAC layer technology

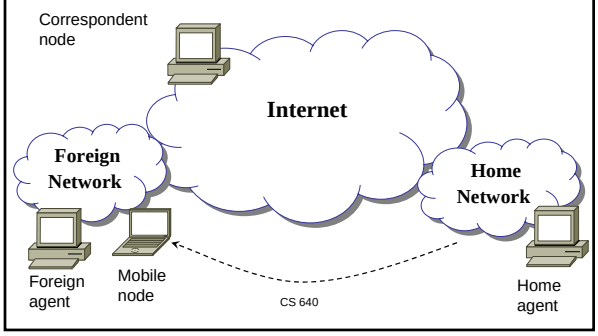
Mobility and IP Routing

- IP assumes end hosts in fixed physical locations
  - What happens if we move a host between networks?
- IP addresses allow IP routing algorithms to get packets to the correct network
  - Each IP address has network part and host part
    - This keeps host specific information out of routers
  - DHCP is used to give IP addresses to hosts
    - This still assumes a fixed end host
- What if a user wants to roam between networks?
  - Users don't want to notice moving between networks
  - Why can't mobile users change IP when running an application?

Mobile IP

- Mobile IP was developed for transparently dealing with problems of mobile users
  - Hosts can connect to Internet regardless of location
  - Hosts can accept connections w/o changing IP addr.
  - Requires no changes for non-mobile hosts/routers
  - Requires addition of some infrastructure
  - Has no geographical limitations
  - Requires no modifications to IP address format
  - Supports security
    - Could be even more important than physically connected routing
- IETF standardization process is still underway

Mobile IP – the big picture



Mobile IP Entities

- Mobile Node (MN)
  - The entity that may change its point of attachment from network to network in the Internet
    - Detects it has moved and registers with "best" FA
  - Assigned a permanent IP called its *home address* to which other hosts send packets regardless of MN's location
    - Can be used by long-lived applications as MN's location changes
- Home Agent (HA)
  - This is router with additional functionality
  - Located on home network of MN
  - Does mobility binding of MN's IP with its COA
  - Forwards packets to appropriate network when MN is away

Mobile IP Entities contd.

- Foreign Agent (FA)
  - Another router with enhanced functionality
  - If MN is away it uses an FA to send/receive data to/from HA
  - Advertises itself periodically
  - Forward's MN's registration request
- Care-of-address (COA)
  - Address which identifies MN's current location
  - Sent by FA to HA when MN attaches
  - Usually the IP address of the FA
- Correspondent Node (CN)
  - End host to which MN is corresponding (eg. a web server)

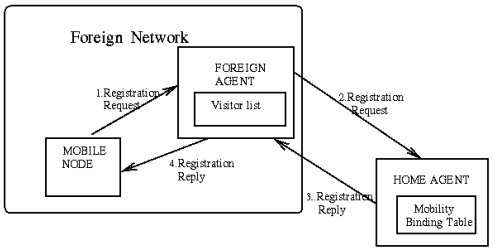
Mobile IP Support Services

- Agent Discovery
  - HAs and FAs broadcast their presence on their networks
    - Beacon messages via ICMP Router Discovery Protocol (IRDP)
  - MN's listen for advertisement and then initiate registration
- Registration
  - When MN is away, it registers its COA with its HA
    - Typically through the FA with strongest signal
  - Registration control messages are sent to well known UDP port
- Tunneling between HA and FA

Mobile IP Operation

- MN listens for agent advertisement and initiates registration
  - If responding agent is the HA, mobile IP is not necessary
- After receiving the registration request from a MN, the HA acknowledges and registration is complete
  - Registration happens as often as MN changes networks
- HA intercepts all packets destined for MN
  - Simple unless sender is on same network as HA
  - HA masquerades as MN
  - After some time, MN must re-register

Registration Process



Tables maintained on routers

- Mobility Binding Table
  - Maintained on HA of MN
  - Maps MN's home address with its current COA

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

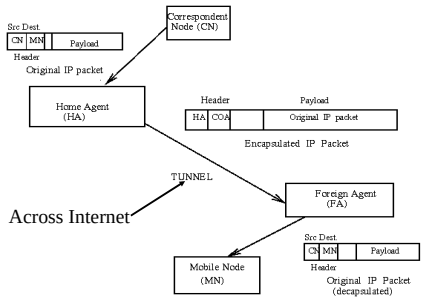
- Visitor List
  - Maintained on FA
  - Maps MN's home address to its MAC address and HA

Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

Mobile IP Operation contd.

- HA encapsulates all packets addressed to MN and forwards them to FA
  - IP tunneling
- FA decapsulates all packets addressed to MN and forwards them via hardware address (learned as part of registration process)
  - MN can perform FA functions if it acquires an IP address eg. via DHCP
- Bidirectional communications require tunneling in each direction

Mobile IP Tunneling



Security in Mobile IP

- Authentication can be performed by all parties
  - Only authentication between MN and HA required
- Replay protection
  - Timestamps are mandatory
  - Random numbers on request reply packets are optional
- HA and FA do not have to share any security information.

Problems with Mobile IP

- Suboptimal "triangle" routing
  - What if MN is in same subnet as the CN and HA is on the other side of the world?
    - Would be nice if we could directly route packets
  - Solution: Let the CN know the COA of MN
    - CN can create its own tunnel to MN
    - CN must have software to enable it to learn the COA
    - Initiated by HA who notifies CN via "binding update"
    - Binding table can become stale
- Alternatives handle mobility at session layer

Other Mobile IP Problems

- Single HA model is fragile
  - Possible solution – have multiple HA
- Security
  - Connection hijacking, snooping…
- What if MN moves out of reach
  - Applications must handle disconnection
- Many open research questions