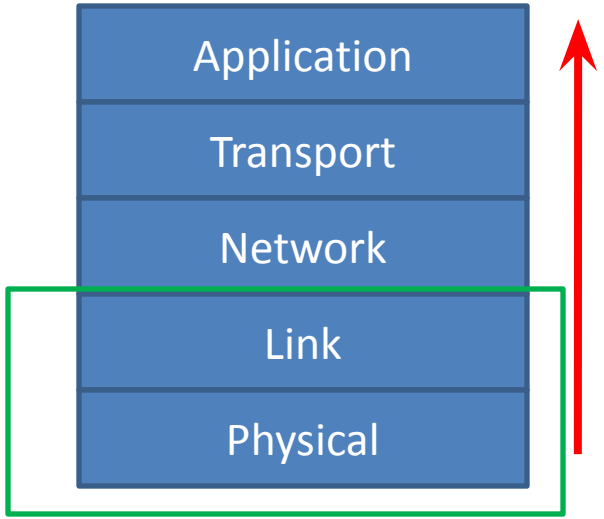
Computer and Network Security: Physical/Link Layer Attacks and Solutions

Kameswari Chebrolu

Outline

- Attacks at different layers of the protocol stack
  - Background Material
  - Various Attacks
  - Solutions to the same

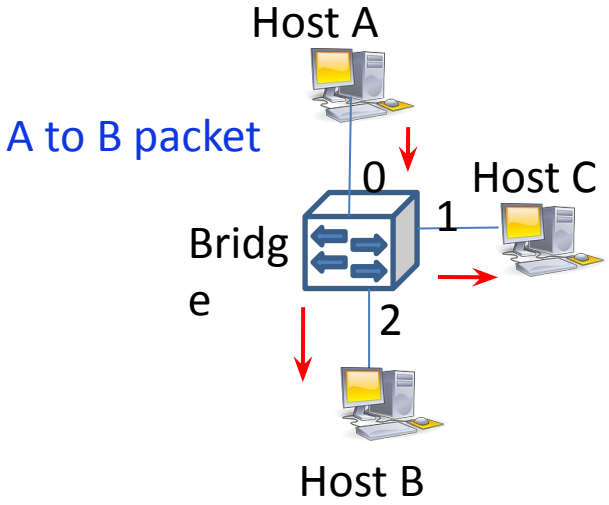


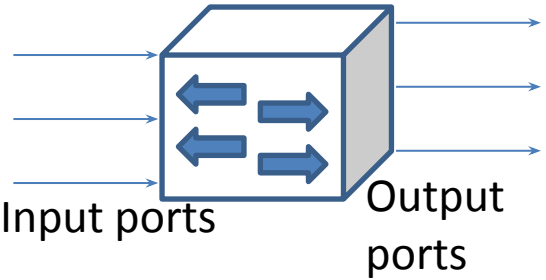
Physical/Link Layer Roles

- What is the role of physical layer?
  - Encode bits into signals (e.g. voltage levels)
- What is the role of link layer?
  - Next hop delivery (framing, error-control, media access and switching)
- Link-layer Switching: Star topology and learning bridges
  - Bus topology outdated, no role for CSMA/CD

Forwarding

- MAC Address: identifies source and destination nodes
- How to forward?
  - Host A sending packet to Host B
  - Host A sending packet to Host C
- Manual configuration: Tedious
- Automatic simple strategy: Forward on all interfaces except the one on which received





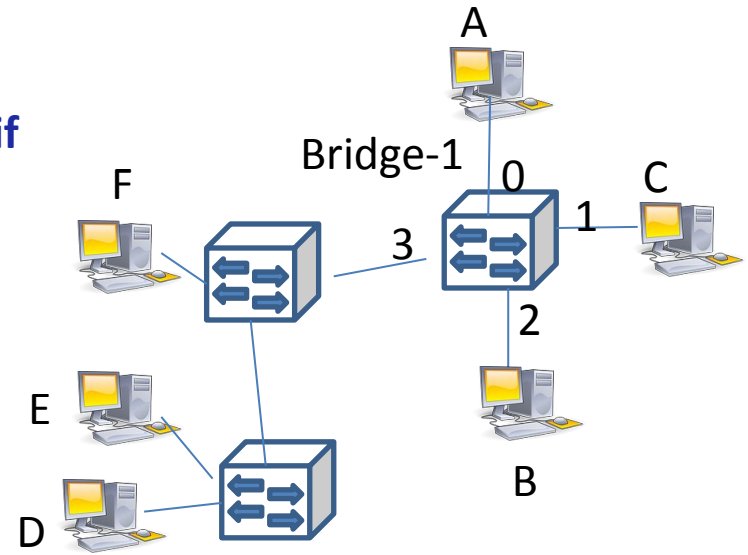
Learning Bridges

- Idea: Inspect source address and map it to port on which the frame was received
  - Each entry purged after some period unless refreshed

Host	Port
A	0
B	2
C	1
D	3
E	3
F	3

Bridge-1's table

Extended LAN (A to F are all neighbours as if connected to a single bus **)

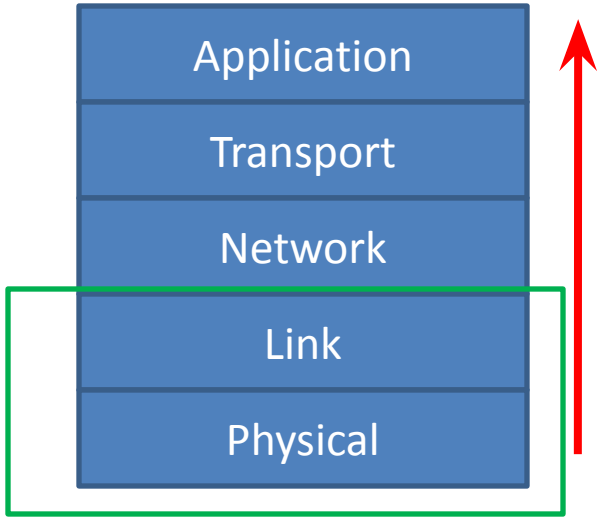


Algorithm

- If a frame received at bridge for destination D on port p
  - No entry for D in the table, forward on all ports except port p
  - If entry for D in forwarding table corresponds to p, drop frame
  - If entry for D in forwarding table corresponds to i != p, then forward on i

Outline

- Attacks at different layers of the protocol stack
  - ~~Background Material~~
  - **Various Attacks**
  - Solutions to the same



Attacks and Defenses (Outline)

- Eavesdropping
- Disruption
- Spoofing
- Protocol specific attacks

Eavesdropping

- Communication media and topology matters
  - Fiber, Wireless, Ethernet star
- Can splice a cable and sniff
- Eavesdropping without piercing cable also possible (based on electromagnetic radiation)
  - See Operation Ivy Bells: https://en.wikipedia.org/wiki/Operation_Ivy_Bells

Eavesdropping

- Wireless media
  - Put interface in monitor/promiscuous mode; sniff media using tcpdump/wireshark tools
  - Can sniff network/transport/app layer headers/data
- Ethernet switching based on star topology
  - Learning bridges make it hard to sniff (frame is forwarded only on the relevant port)
  - Possible to work around. How?

Eavesdropping in Ethernet

- **MAC flooding:** Forces a switch to flood unicast traffic instead of route along right path
- How achieved?
  - Bridges set aside limited memory to store forwarding table (MAC address to port)
  - Feed switch many Ethernet frames with different source addresses □ evict valid entries
  - No entry for a destination □ forward on all ports (other than one received) □ scope for eavesdropping

Defense

- MAC Limiting: Limit the number of MAC addresses learnt from a port.
  - Ports connected to end-hosts (low limit) vs other switches (high limit)
- Encryption of link layer payload (or at higher layers, e.g. HTTPS)

Attacks and Defenses (Outline)

- ~~Eavesdropping~~
- **Disruption**
- **Spoofing**
- Protocol specific attacks

Disruption

- Jam ongoing communication
  - Easier in wireless environment; Transmit at same time with high signal strength
    - Packet discarded due to bit corruption (checksum fail)
  - Cut cables (especially ones that serve many customers)
- **Defence:** No easy solution
  - Localizing jammers; Redundancy in the system

Spoofing

- Impersonate some one else (take their address)
  - Blind spoofing: spoofing without eavesdropping
- Used to cover track or access unauthorized resource
- Inject packets with fake source MAC address
  - In linux, can be done via “ifconfig” (e.g. ifconfig eth0 hw ether 00:84:48:AA:D3:61) with root permission

Attacks and Defenses (Outline)

- ~~Eavesdropping~~
- ~~Disruption~~
- ~~Spoofing~~
- **Protocol specific attacks: Address Resolution Protocol (ARP)**

ARP Spoofing

- **ARP Spoofing** can allow eavesdropping, denial of service and MITM attacks
- But what is ARP?

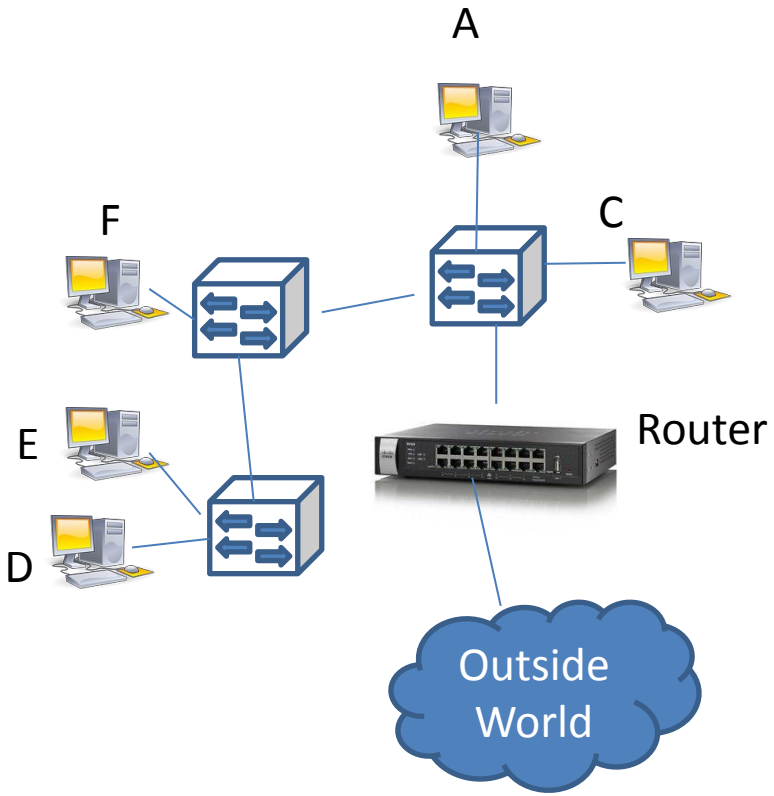
ARP (Address Resolution Protocol)

- At network layer: Routing module at a node decides who the next hop node is (its IP address)
- At link layer: transfer over the next-hop link needs next hop's MAC address
  - Link here can refer to extended LAN

ARP (Address Resolution Protocol)

- ARP helps determine MAC address corresponding to given IP address (Request is broadcast)
  - Host with matching IP address replies (Reply is unicast)
- Each host maintains a cache with IP to MAC translations
  - Entries in cache timed out periodically (say 15 min)

Example



Address Resolution Protocol (ARP)

- When forwarding a datagram, check cache, if no mapping, invoke ARP
- Originator: Add entry to cache corresponding to target (obtained from ARP reply)
- Target: Add entry to cache corresponding to the originator (obtained from ARP request)
- Intermediate hosts: Refresh existing entries (obtained from ARP request)

Gratuitous ARPs

- Generated by a host to inform others of its IP to MAC mapping
- Could be a request or reply
  - If request, no reply will occur
  - If reply, there was no preceding request

Uses of Gratuitous ARPs

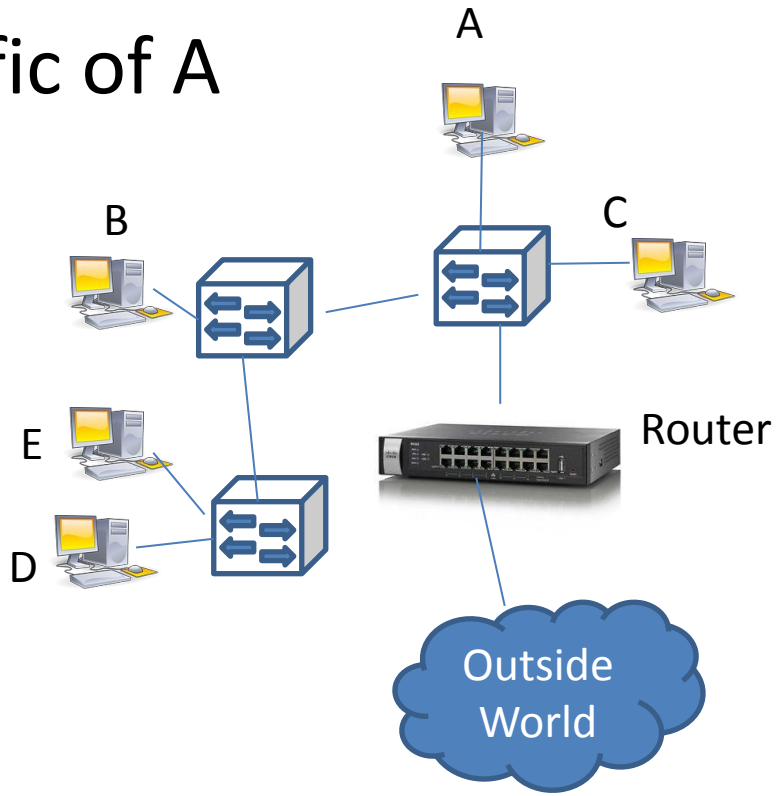
- Issued whenever IP or MAC address of an interface changes or brought up from down state
  - Help rectify cached ARP entries
  - Report IP address conflicts (duplicate IP)
  - Inform bridges of the location of new host

Vulnerability

- ARP is a stateless protocol
  - A host will act on a reply regardless of whether a request precedes it
- ARP has no authentication mechanism to verify identity of sender

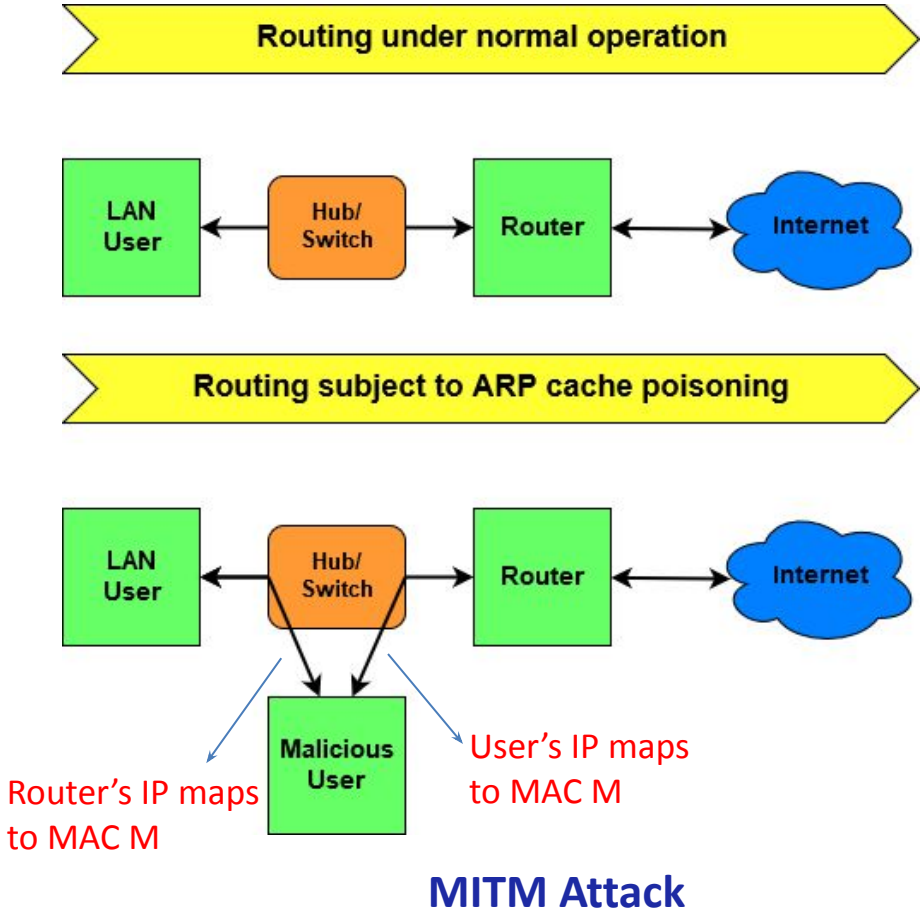
ARP Cache Poisoning

- Eve E wants to examine traffic of A



ARP Cache Poisoning

- Associate IP address of target host with Attacker's MAC
  - Traffic meant for target received by attacker
  - Inspect, modify, drop (denial of service) traffic
  - Can also do MITM, where both parties unaware of the attack
- Legitimate uses: backup-servers; debug traffic



Solutions

- Hosts maintain ‘static read-only’ ARP tables for critical services
  - Not very convenient; not scalable
- Ethernet switches can check for same IP address mapped to many MACs and alert sys-ads via email
  - Can also verify mapping from DHCP servers
- OS level: Ignore unsolicited replies (but attacker can work around it)
- Tools: Arpwatch, xARP, ArpStar
  - Analyze all observed ARP traffic and determine spoofing attacks

Summary

- Covered some Link layer background (switching, learning bridges, ARP)
- Different types of attacks: Eavesdropping, Disruption, Spoofing and ARP spoofing
- Each attack has a solution that works in practice