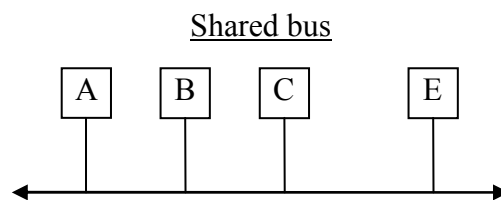


“Network attack” types:

- “Uses the network” – some guy in Asia can attack your PC because the network is there.
- “Exploits the network” – exploit the protocols, etc. used by the network. This is our focus.

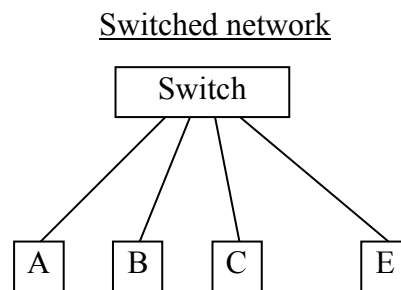
Small Scale (LAN)

- Little publicity due to small scale



Attack methods:

- Eavesdrop
- Insert spoofed packets
- Delete packets via jamming - collision or checksum corruption triggered by header/data
- ARP spoofing for man-in-the-middle (MITM)
 - ARP is the IP-to -Ethernet address protocol. Procedure:
 1. Sender broadcasts ARP request: “who is W.X.Y.Z?”
 2. Host with that IP responds
 - Spoofing is thus a race between valid and spoofed responses



ARP spoofing changes due to the presence of the switch. Switch has an ARP cache, filled by snooping. ARP request and reply are broadcast.

Switch has a CAM table matching Ethernet address to physical connection. Subversions:

- Port stealing – spoof a message from target to self
- Flood cache with bogus entries, force broadcast fallback

Large Scale (network of nodes)

Packet format:

Source	Destination	Rest of header	Data
--------	-------------	----------------	------

Routing table present at each node; node looks only at destination address when routing

Attacks:

- Inject spoofed packets – mostly defeatable by ingress/egress filtering, but little incentive for ISPs to filter. If anything, there will probably be ingress filtering.
 - Ingress – block packets from entering that claim to be from inside
 - Egress – block packets from exiting that claim to be from outside
- Eavesdrop – must be in the path from source to destination; generally unlikely
- Modify packets (MITM) – must be in the source-destination path; again, unlikely in the general case

Internet security threat model: Attackers exist, but not on the source-destination path. If they are on the path, assume we're doomed due to easy MITM.

(Compare to crypto threat model: Everyone else is an attacker.)

Criticisms:

- Wireless vulnerabilities – access point spoofing, etc.
- DNS attacks
- BGP attacks (router protocol, little security; attack by announcing an excellent route to a target)

Salient BGP (border gateway protocol) info:

Routing tables contain IP prefixes, route direction/quality, AS-PATH (the path of nodes that the route announcement took to get to the current router; prevents loops)

(AS is autonomous systems)

To MITM with BGP, hijack all traffic except one route – set AS-PATH of fraudulent route announcement to include the routers on that route. Otherwise all nodes will incorporate your path and prevent you from sending your MITMed packets to the destination as the packets will be routed back to you.