Computer and Network Security: Network Security Overview

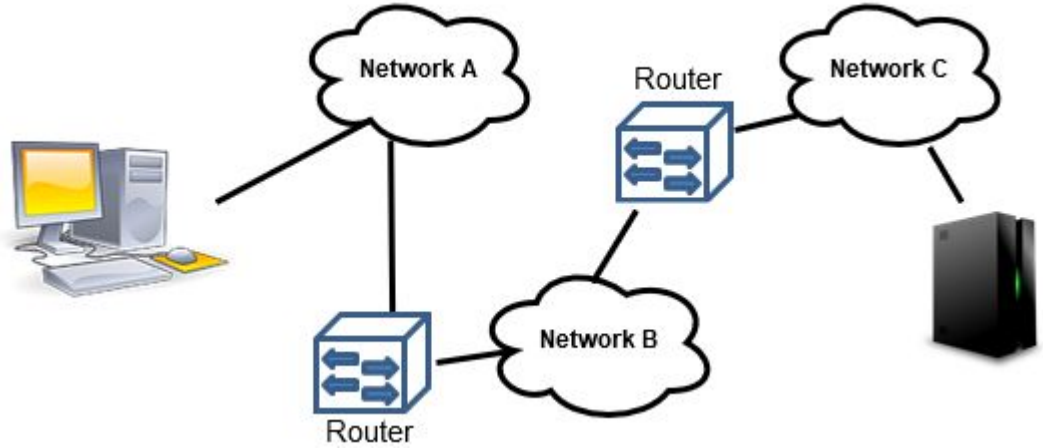
Kameswari Chebrolu

Outline

- Networks Background (high-level)
  - Relevant topic related details covered later
- Network Security Overview
  - Why are they vulnerable?
  - Composition of an attack
  - Defense Mechanisms

Internet

- Inter-net(works): interconnecting heterogeneous networks at global scale
  - Ethernet, Fiber, Wireless etc
- Network: An interconnection of computing devices over links to exchange data



Very simplistic view of Internet

Implementation

- A very complex task handled via layering Internet Protocol Stack
  - Modular Design; distributed implementation
  - Each layer made up of protocols
- Protocol: agreement on how to communicate
  - Format, Rules, Actions

Internet Protocol Stack

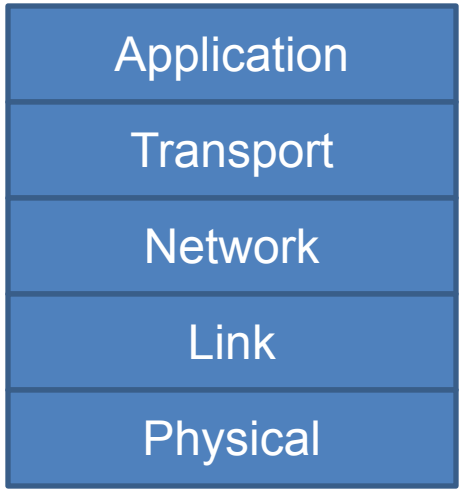
Application
- Supports application processes which generate messages
- E.g. Email, Web, File-transfer

Transport
- Supervises process to process communication (multiplexing/demultiplexing messages, reliability)
- E.g. TCP, UDP

Network
- Enables end-to-end routing of messages (from source to destination hosts)
- E.g. IP

Link
- Enables hop-to-hop message transfer (between neighbors)
- E.g. Ethernet, 802.11

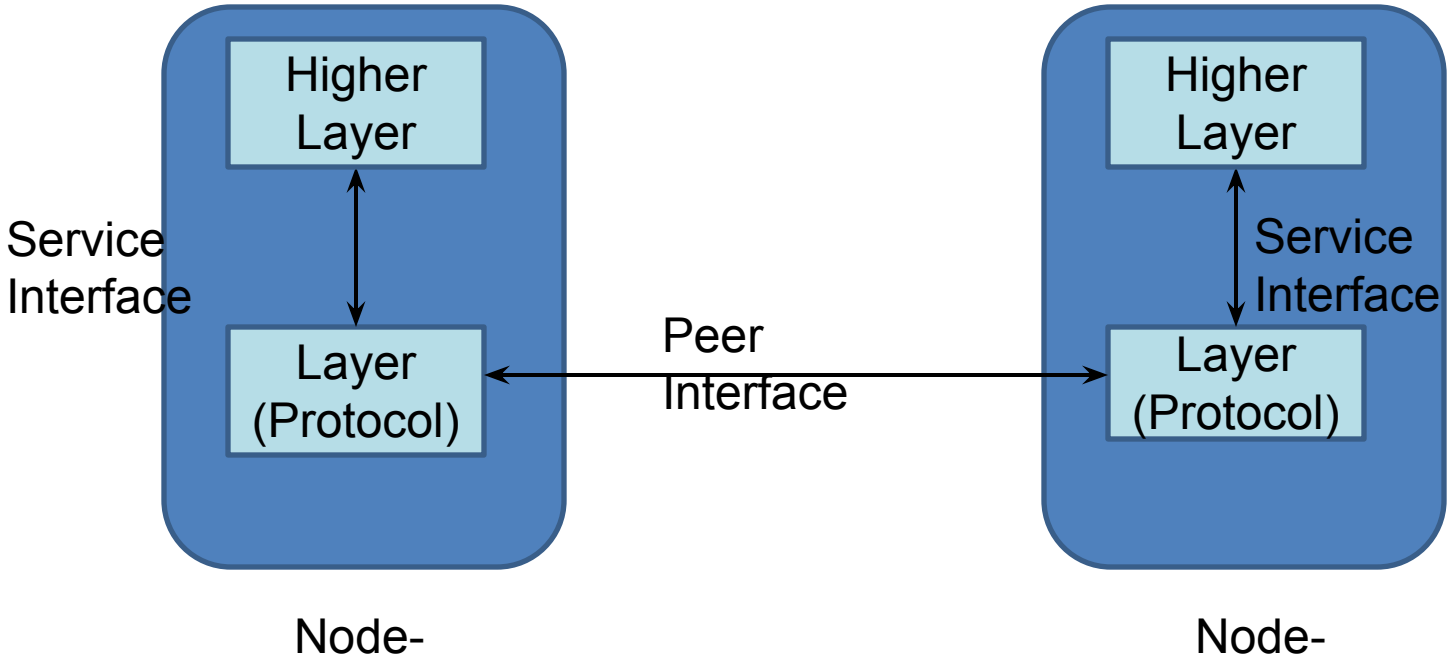
Physical
- Enables bit transmissions on media (wire/air)
- E.g. 10Base-T, OFDM



Core Concepts

- Layers and Interfaces
- Multiplexing / Demultiplexing
- End to end vs hop to hop
- Packet Switching
- Best effort service model

Layers and Interfaces



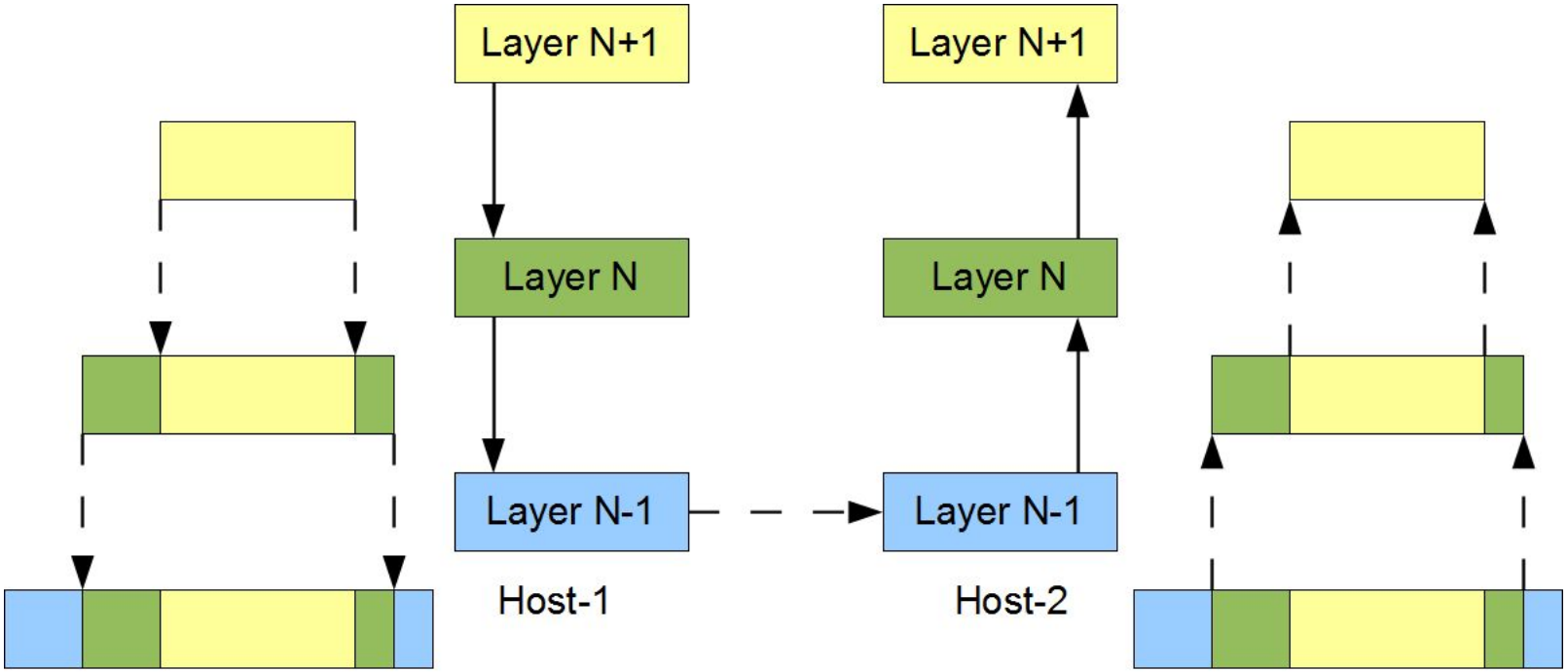
A layer (protocol) provides certain functionality.

Service Interface: Interface for users of the functionality provided by the layer

Peer Interface: Interact with peer (counterpart) to implement needed functionalit

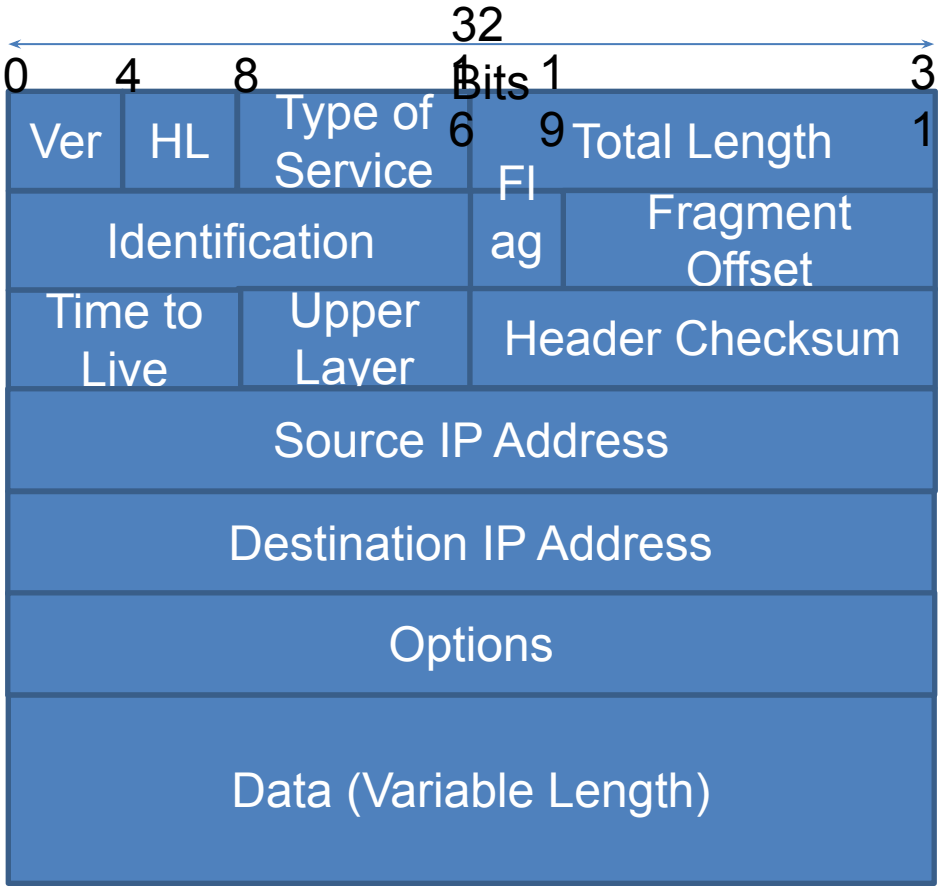
Inter Layer Communication

(Encapsulation/Decapsulation)

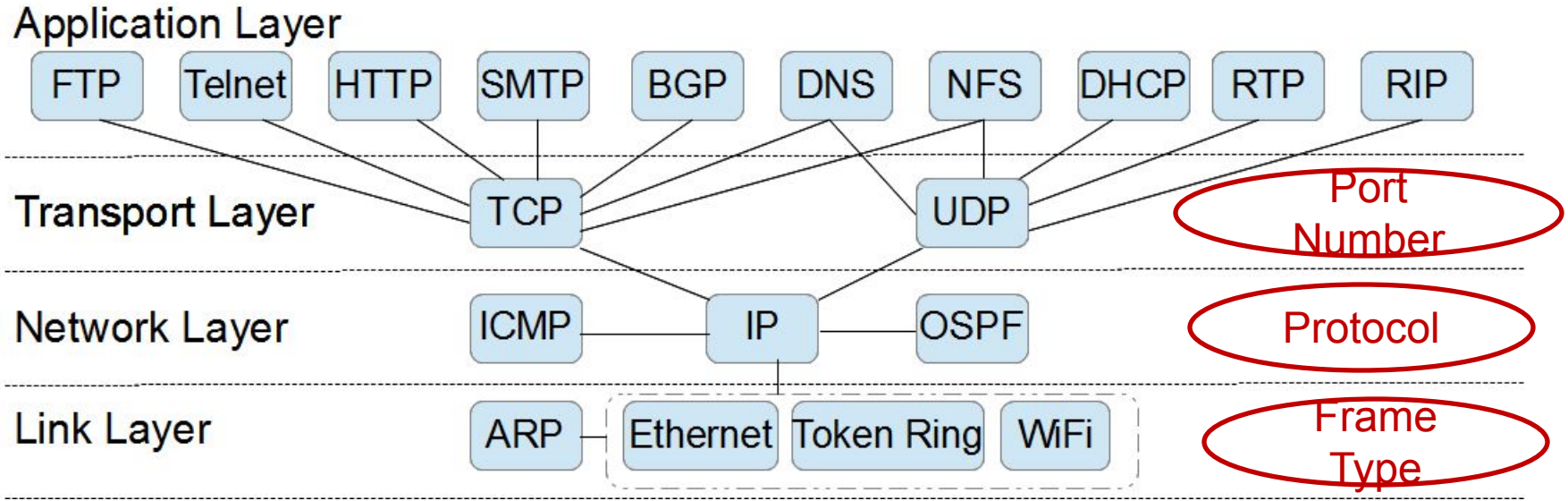


Each layer adds/removes its header

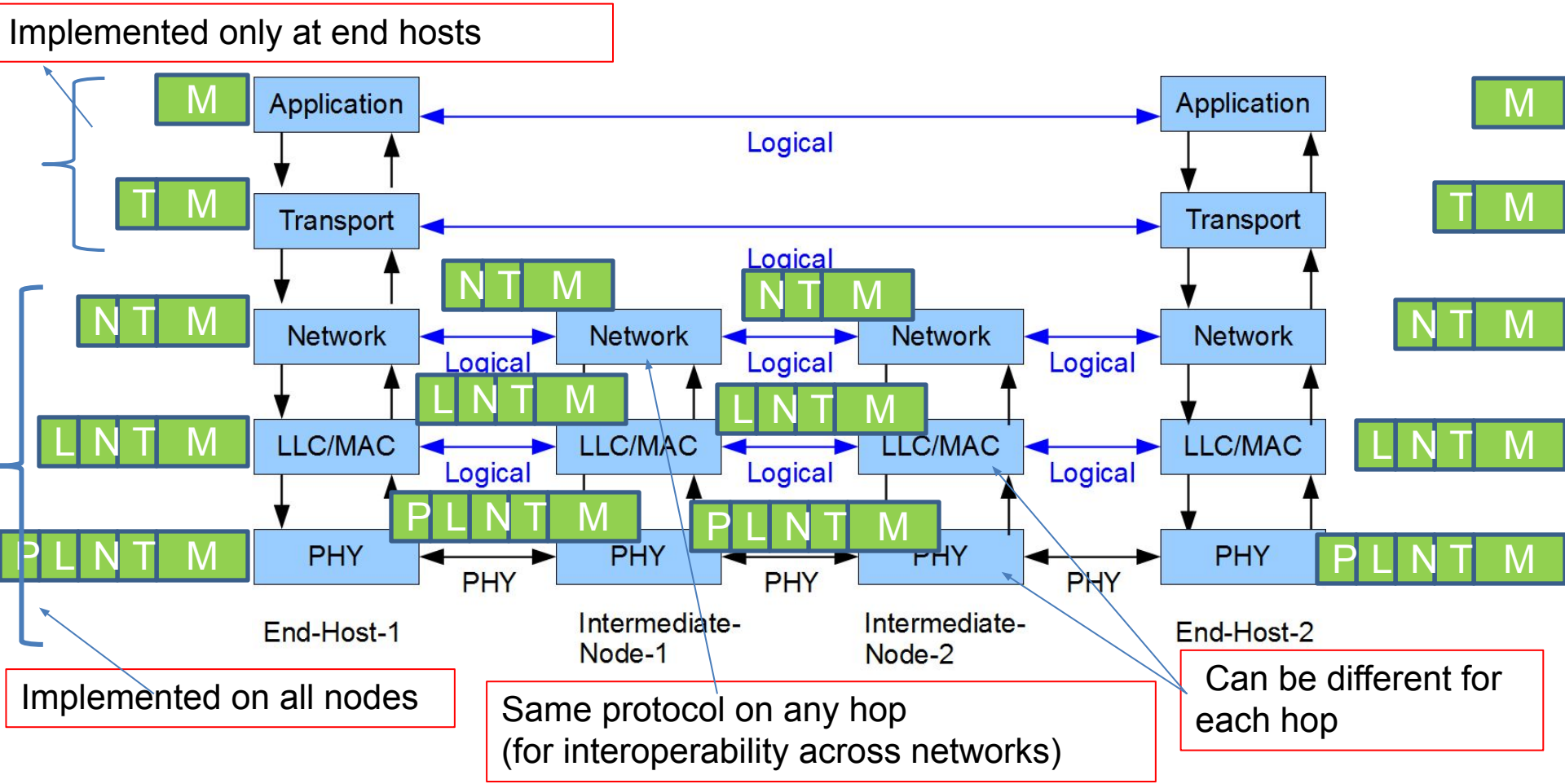
Example IP header

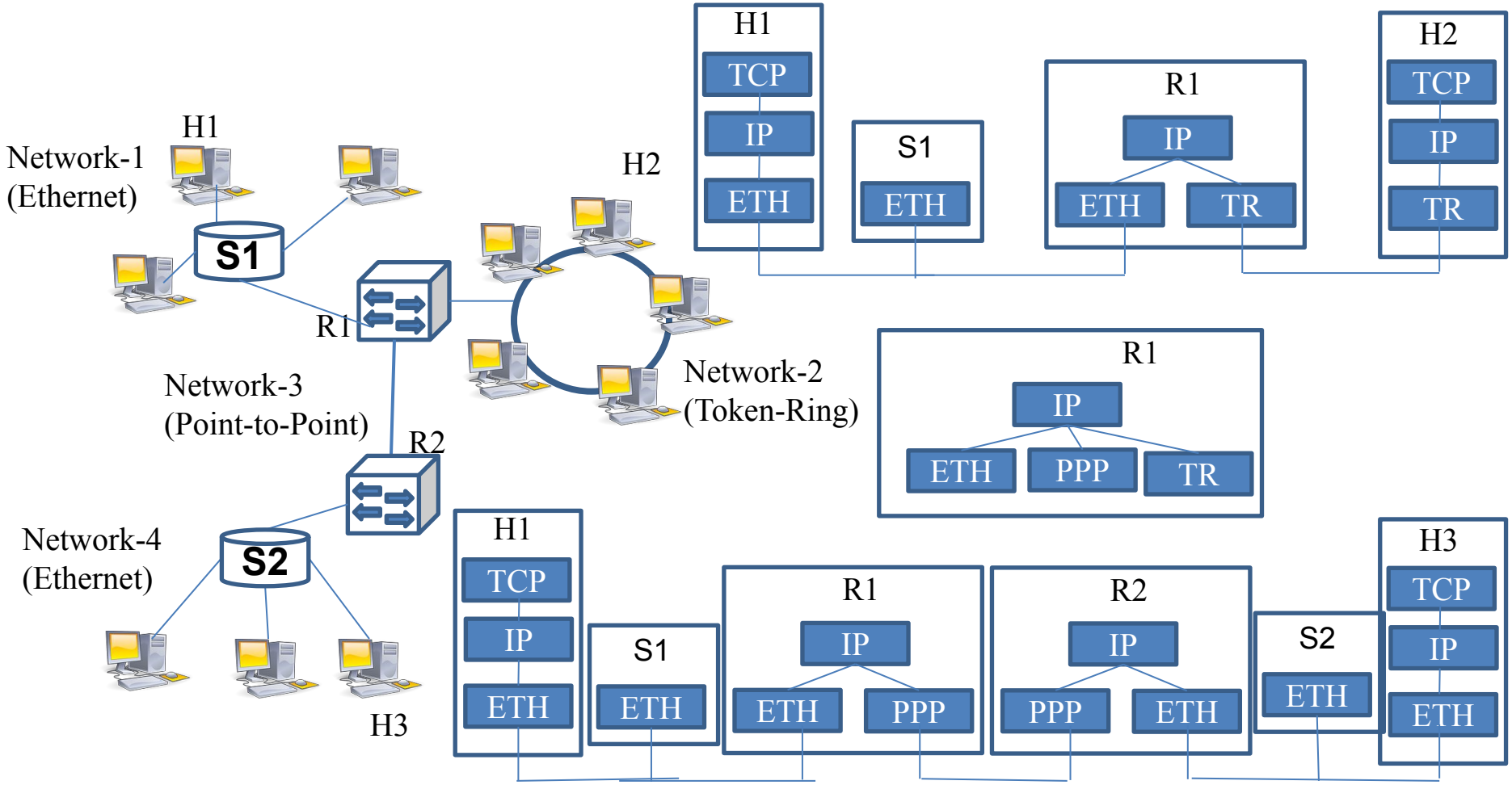


Multiplexing/Demultiplexing



End to End vs Hop to Hop

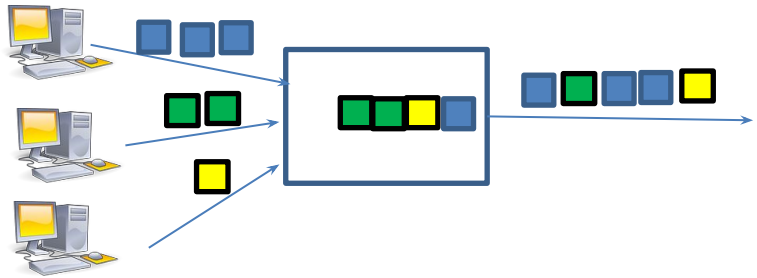



H1
Network-1
(Ethernet)
S1
H2
R1
Network-3
(Point-to-Point)
R2
Network-2
(Token-Ring)
Network-4
(Ethernet)
S2
H3
H1
TCP
IP
ETH
S1
ETH
R1
IP
ETH
TR
H2
TCP
IP
TR
R1
IP
ETH
PPP
TR
H1
TCP
IP
ETH
S1
ETH
R1
IP
ETH
PPP
R2
IP
PPP
ETH
S2
ETH
H3
TCP
IP
ETH

Packet Switching

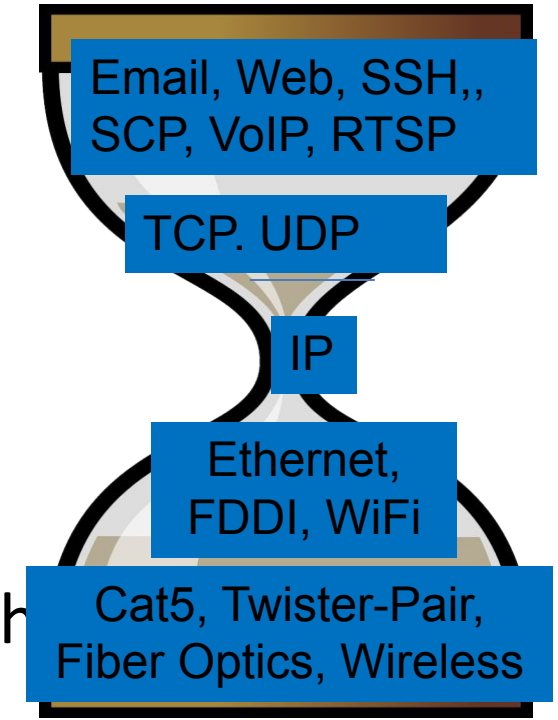
- Physical link is shared among users (in contrast to circuit switching as employed in telephone networks)
  - Sharing is on demand and not fixed

  Fairness handled by limiting amount of data(packets)
  - Store and forward mode of operation
  - Packets from different flows are interleaved
  - Packets served predominantly in a FIFO basis
  - Potential of packet loss (Buffer overflow)



Datagram Best Effort Service

- Datagram: No connection set-up
- Best Effort Service – Will make best effort to deliver the packet
- Packets can get lost, corrupted, reordered, mis-delivered, duplicated, delayed
- KISS principle in practice (Simplest service) – IP protocol's greatest strength
- Runs over anything



Outline

- ~~Networks Background (high-level)~~
  - ~~Relevant topic related details covered later~~
- Network Security Overview
  - Why are they vulnerable?
  - Composition of an attack
  - Defense Mechanisms

What is Network Security?

*"**Network security** consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer **network** and **network**-accessible **resources**. "*

(From wikipedia.org)

Why are networks vulnerable?

- **Protocols not designed with security in mind**
- Protocols complex and heterogeneous
  - Many points of attack
- Built-in anonymity
- Lot of sharing
  - Services (printer), media (e.g. wireless), files (windows sharing) etc

Protocol Security

In the past, protocols not designed with security in mind

- Confidentiality: No one can read our data
  - Reality: No encryption by default in any protocol (data or headers)
- Integrity: No one can alter our data
  - Reality: Simple checksum, CRCs; not cryptographically secure

- No notion of authenticity (signatures)
- Availability: Network resources available to us when we want (further, not available to unauthorized users)
  - Reality: Distributed implementation gives some tolerance but still susceptible to say DOS attacks

Current Status

Things are not so bad now …

- Application Layer: SSH (remote login), PGP (for emails), DNSSEC (for DNS)
- Transport Layer: SSL/TSL
  - Used by applications to add security on top of TCP
- Network Layer: IPsec, BGP-S (secure BGP routing protocol)
- Link Layer: WEP, WPA (wireless)
- Firewalls, Intrusion Detection Systems (IDS), anti-virus software etc

Network Battlefield

- Attacks
- Defenses

Real Life: Bank Robbery

- Learn first about the target (casing the joint, dumpster driving; reconnaissance, intelligence gathering)
  - When do guards change
  - Befriend guards to see what security mechanism are employed
- Cover identity: wear a mask
- Exploit vulnerability:
  - choose proper timing; specific lock mechanisms; bribe employees to get relevant keys; use guns

Composition of an Attack

1. Scanning for vulnerable machines
2. Sniffing traffic to determine current state
3. Spoofing to cover up tracks
4. Exploit i.e. use vulnerability to execute the attack

(In Real-life: can be non-technical too like eavesdropping/befriending employees; reading up on blogs, facebook pages etc)

1. Scanning

- Can scan network topology, OS used by machines; ports and services open on machines
  - Scanning often employed by sysads also
- Network topology: How?
  - Ping sweeping (which machines are up)
  - Traceroute: path taken by packet

- OS: How?
  - Make TCP connection to target; Examine initial window size, distribution of sequence numbers, TCP options etc
- Ports and Services: How?
  - Establish TCP/UDP connections to different ports
    - Check port open or closed
    - Well-known ports mapped to specific services
    - Banner grabbing: guess service at a port (what server, which version etc) based on message/challenge received from remote machine
- NMAP: A useful tool to check out

2. Sniffing

- Can sniff traffic to mine username/passwords, locate important machines (DHCP/DNS servers etc)
  - Tools: tcmpdump/wireshark; set interface in monitor/promiscuous mode
- Difficult to sniff with Ethernet star topology; Wireless is easier
  - Attacks like ARP cache poisoning, MAC flooding (to be covered later) can help sniff

3.Spoofing

- Take on some other IP or MAC address
  - Can cover track
  - Gain access to resources (e.g. MAC address based authentication)
- Note: With IP spoofing, Reply will go to original source

4. Vulnerability/Exploits

- Weak passwords, OS flaws, software bugs, poor design/implementation (of protocols)
- Example Exploits:
  - Exploit OS flaw, get remote shell with root permissions
  - Over-run state (memory) to launch DOS attacks
- Above done with good intentions → penetration test (find exploitable vulnerabilities)
- Tools to check out: Nessus, Core Impact (commercial)

Defenses

- Hard problem; need to defend against many points of attack
  - Requires proper planning, careful execution and regular maintenance

Common Techniques

- Fix Protocol shortcomings or design new ones (not always possible due to wide spread use)
- Perimeter via firewalls:
  - Keeps certain type of traffic away from computers protected by it
  - Logic: Alls eggs in one basket; watch carefully

- Intrusion Detection System (IDS)
  - Match traffic to known attack patterns (signatures) and block
  - Clever attacker can use IDS as a honey pot
    - Launch false attack to trip IDS, then carry real attack
- Host based defenses
  - Firewalls and HIPS (host based intrusion prevention system)
  - Anti-virus, anti-spyware to locate malware
  - Integrity checkers (e.g. tripwire) ensure files are not modified
    - Periodically compare file on disk with its hash

Summary

- Internet a very powerful resource but full of dangers
  - Any machine connected to it can be exploited
- Network protocols not designed with security in mind
  - Many attacks possible
- Network Security becoming increasingly important → Variety of defense mechanisms are being put in place to provide security