CIS551: Computer and Network Security

Jonathan M. Smith

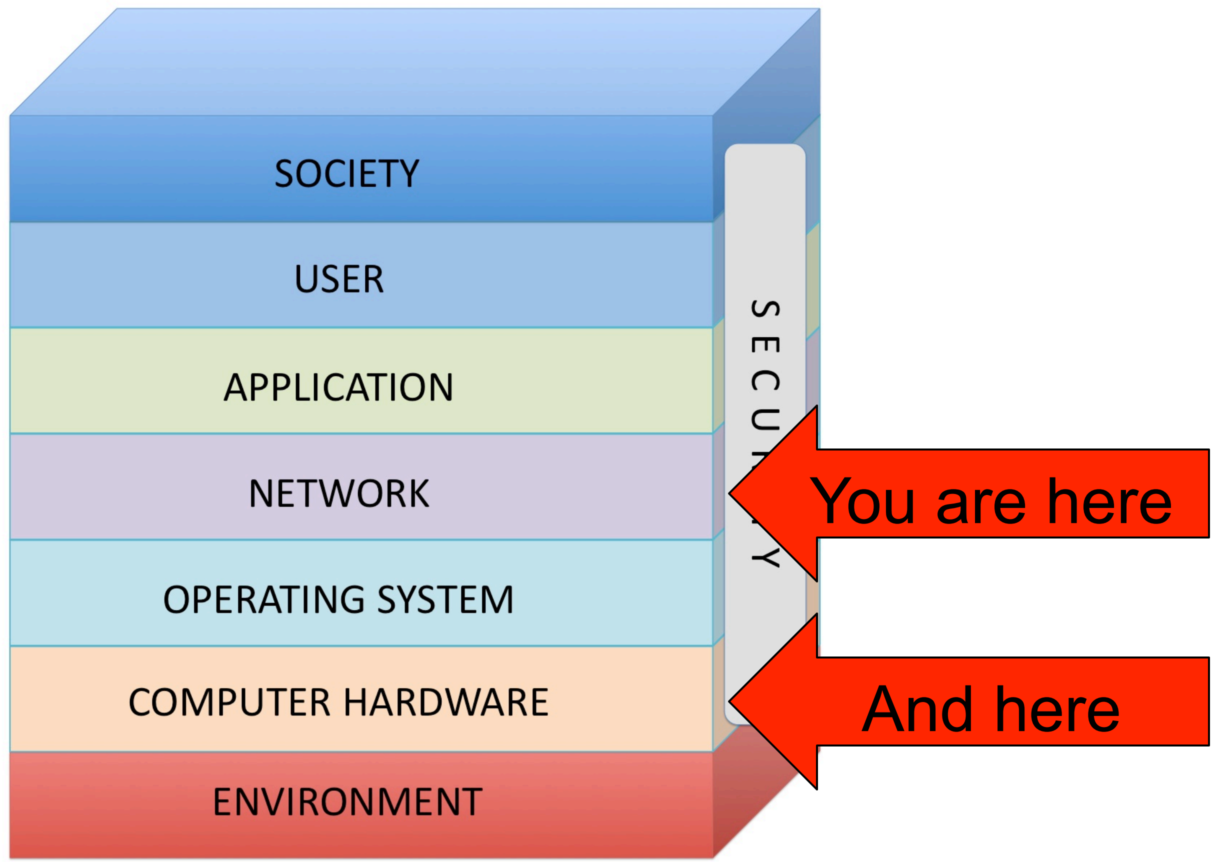
jms@cis.upenn.edu

02/05/2014

CIS551 Topics

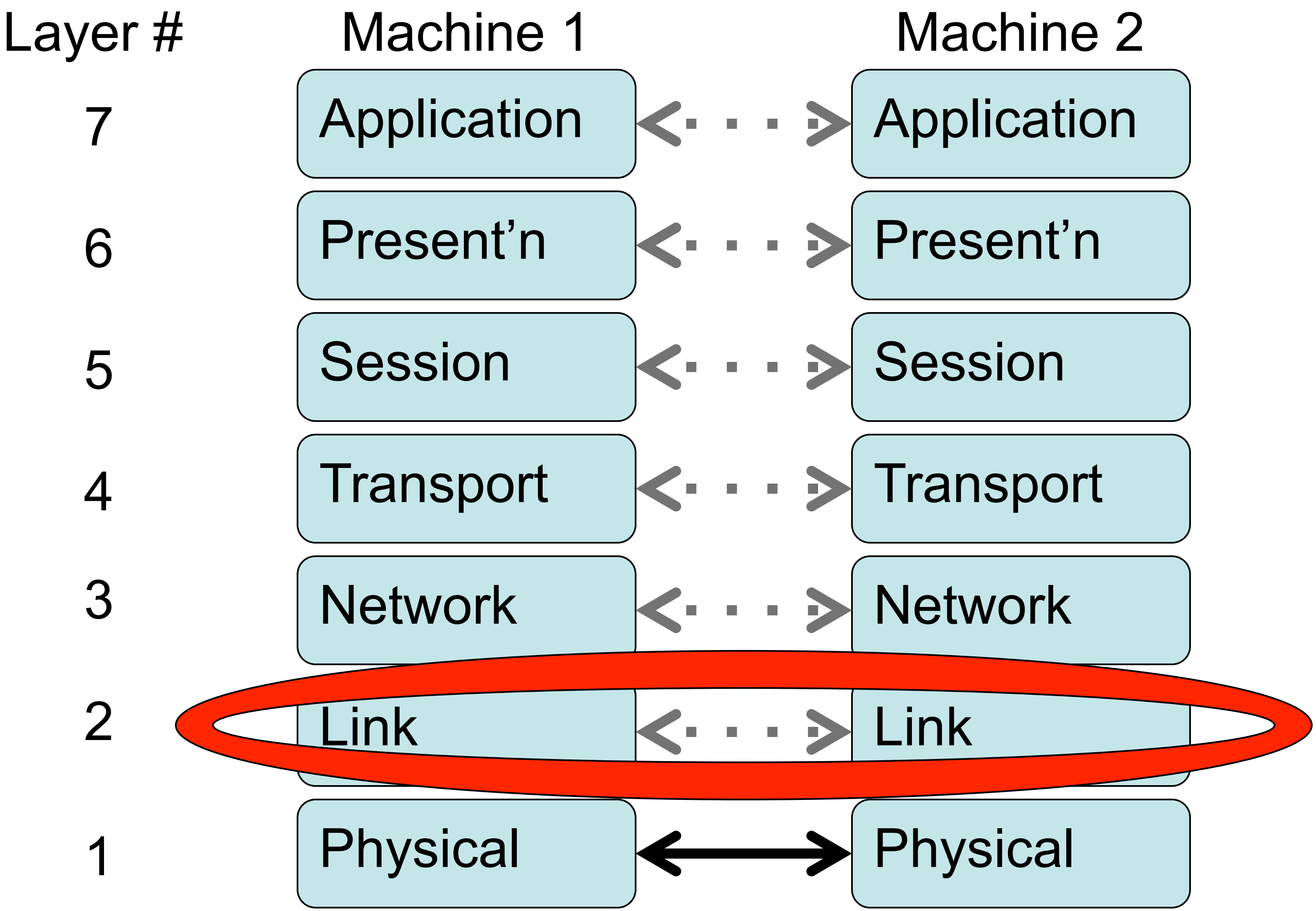
- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems Viewpoint
  - Users, social engineering, insider threats

Sincoskie NIS model



W.D. Sincoskie, *et al.* “Layer Dissonance and Closure in Networked Information Security” (white paper)

7-layer OSI network model



“Wireless Ethernet” - WiFi

- Ethernet-like to ease adoption
  - But 802.11 frames != 802.3 frames
- CSMA/CA adds:
  - CONTENTION period (wait after no-XMIT)
  - Positive ACKs – MAC re-XMIT
- 802.11 standards: b (max: 11 Mbps), g (max: 55 Mbps), n (max: 150 Mbps) – many modern devices b/g/n

Architecture

- Multiple streams of data (“channels”)
  - Usually can use only ca. 3 channels (of 14)
- Interference dealt with by FHSS, DSSS or OFDM (modulation techniques)
- Range about 100m (varies w/context)
- Lots of sources of interference
  - Potential for loss or delay
- Access points interconnect with 802.3

Security thoughts

- What is an important difference between Ethernet and WiFi?
- What effect does this have on unwanted monitoring?
- Can this affect “CIA”?
  – Confidentiality, Integrity, Availability
- Are there solutions?
  – Wired Equivalent Privacy (WEP)?
  – WiFi Protected Access (WPA) better…

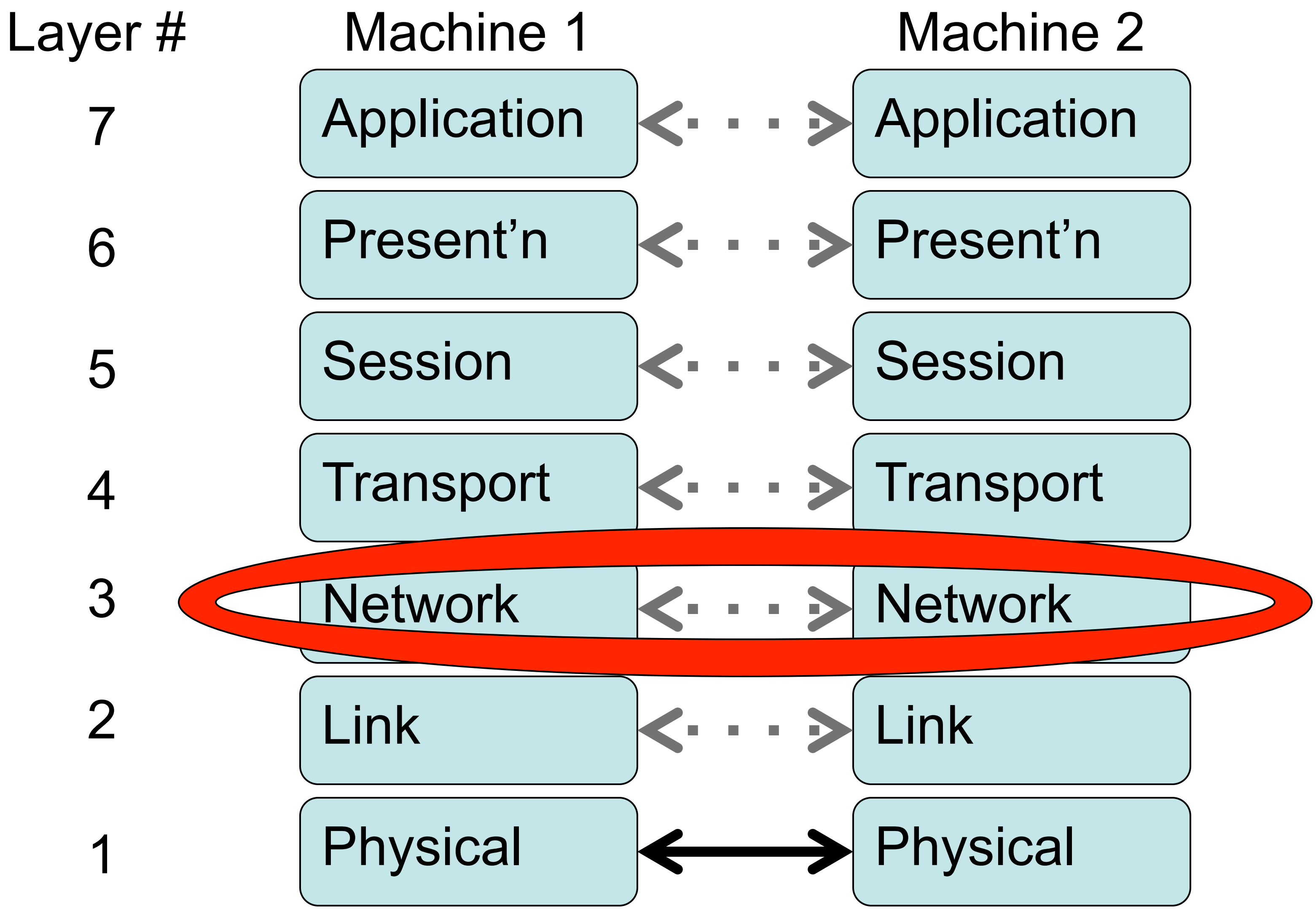
A look into the crystal ball…

- More 802.11x (people like to be mobile)
- Increasing security threats as more uses migrate to wireless
  - Can you trust *any* access pt. w/your packets? Arbitrary peers?
  - Voice over IP (VOIP) phones?
- Better technologies will emerge!

CIS551 Topics

- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems Viewpoint
  - Users, social engineering, insider threats

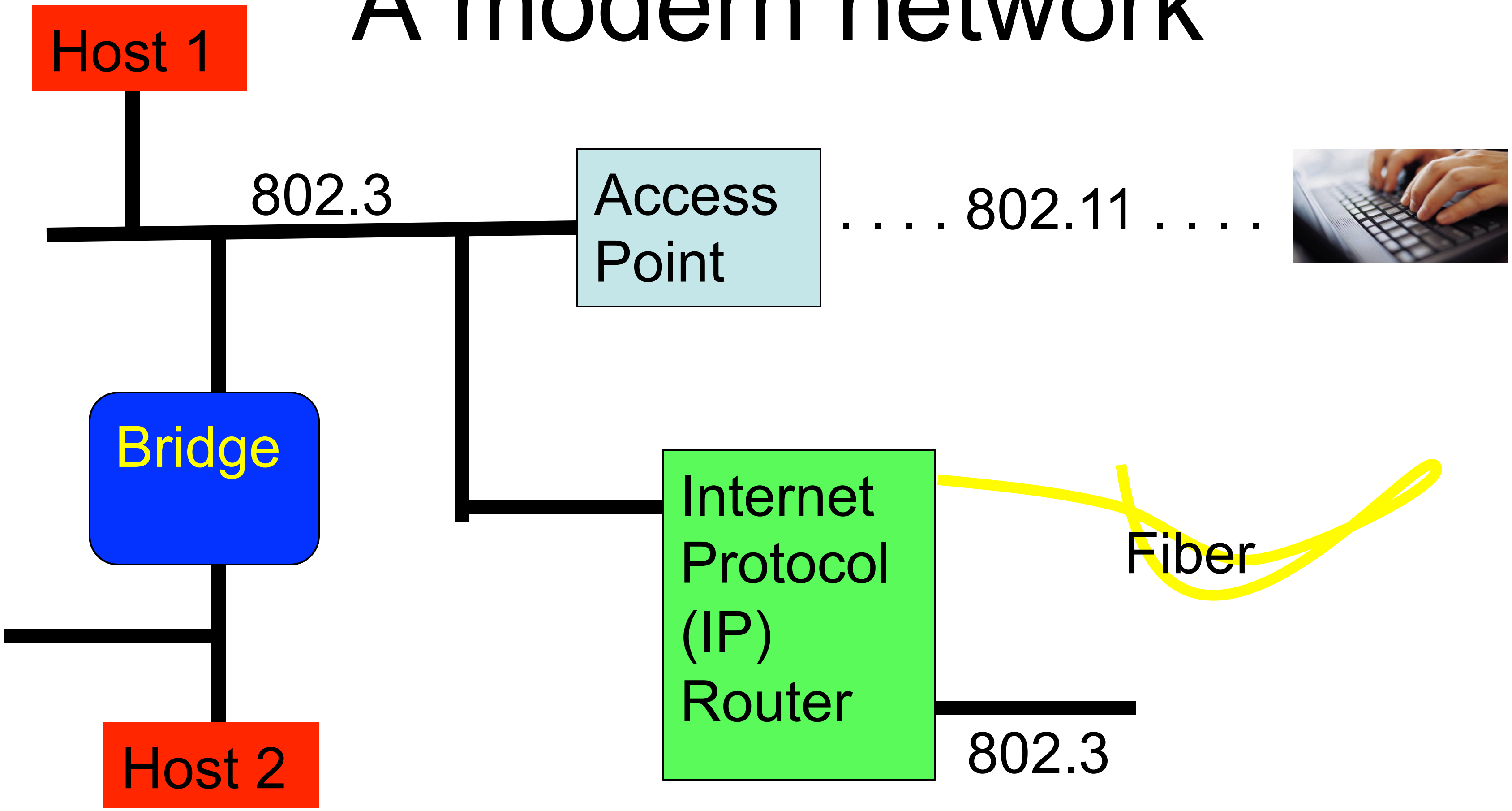
7-layer OSI network model



Incompatible Networks?

- Fiber optics: SONET frames
- Ethernet: 802.3 frames
- WiFi: 802.11 frames
- Phone lines, satellite links, …
- We could build protocol translators
  - N^2 problem
- Could convert to a standard format
  - Then, define translations to & from format

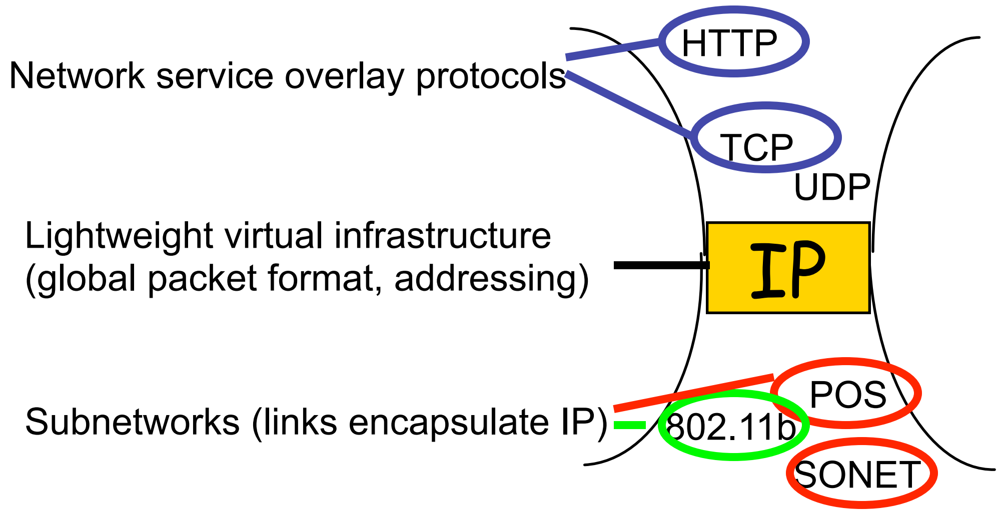
A modern network



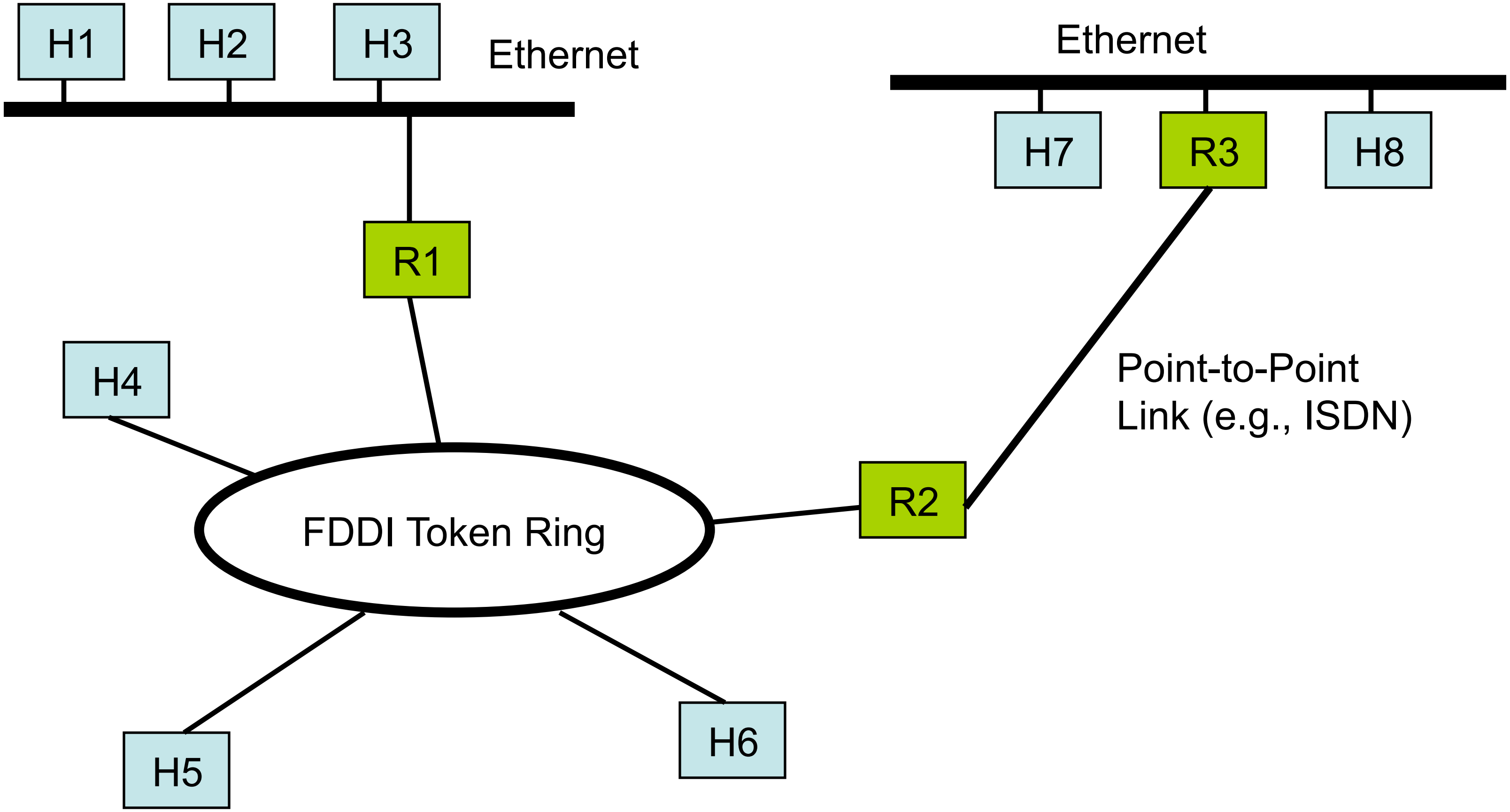
How does it work?

- Encapsulation
  - IP packets are carried in frames
- "Overlay"
- Standard packet format
- Standard Addressing Scheme
  - 32-bit IPv4 addresses
  - 128-bit IPv6 addresses

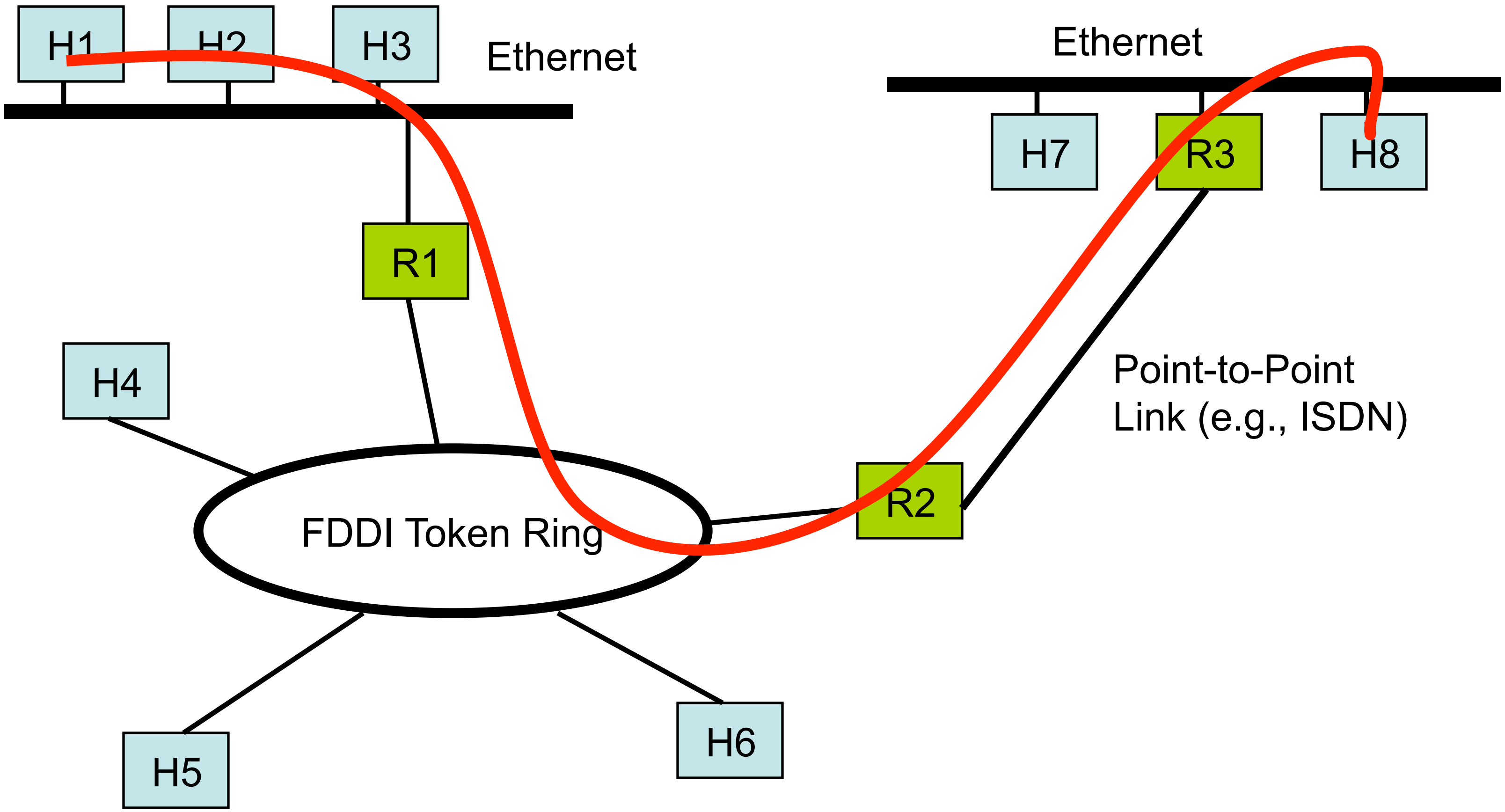
Another way to look at it



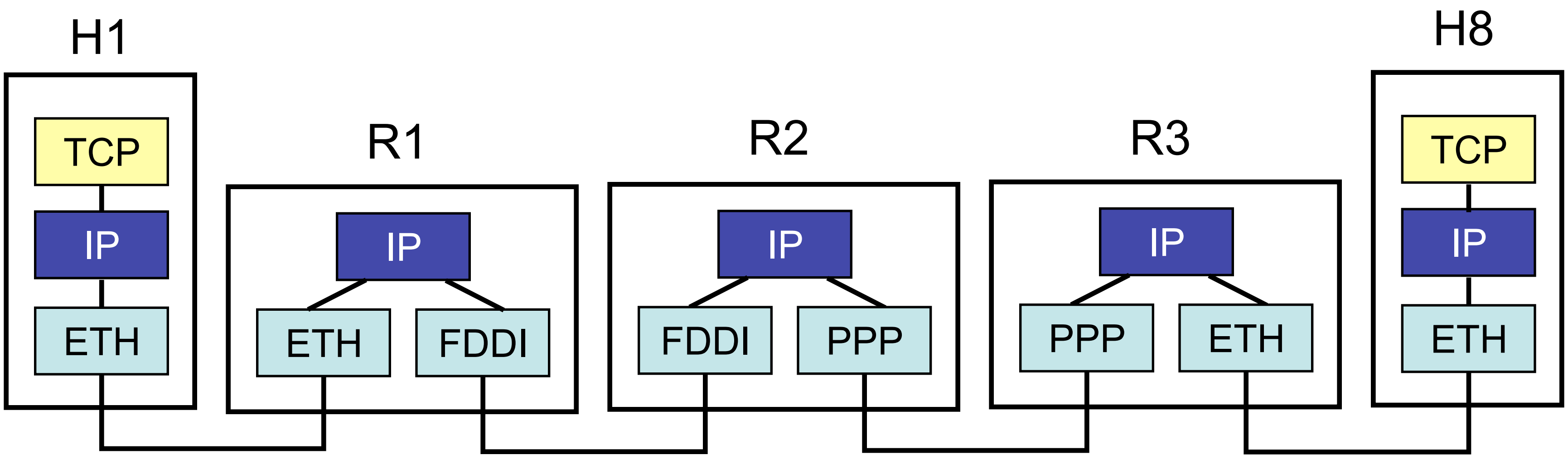
Internetworks (diagram from Peterson & Davie)



Internetworks (diagram from Peterson & Davie)



IP Encapsulation (diagram from Peterson & Davie)

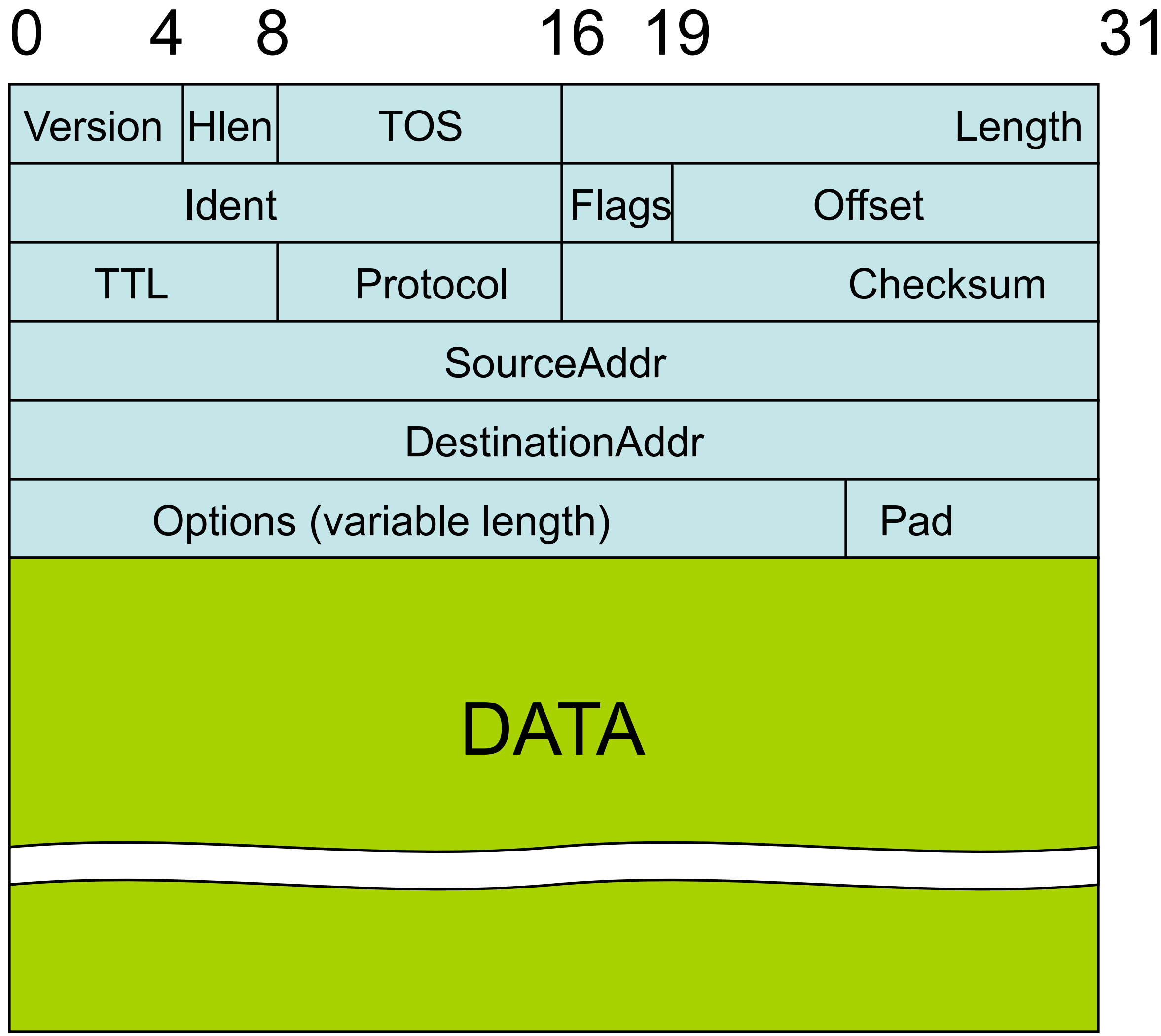


Example of protocol layers used to transmit from H1 to H8 in network shown on previous slide.

IP Service Model

- Choose minimal service model
  - All nets can implement
  - “Tin cans and a string” extremum
- Features:
  - Best-effort datagram delivery
  - Reliability, etc. as *overlays* (as in TCP/IP)
  - Packet format standardized

IPv4 Packet Format



Fields of IPv4 Header

- Version
  - Version of IP, example header is IPv4
  - First field, so easy to implement case statement
- Hlen
  - Header length, in 32-bit *words*
- TOS
  - Type of Service (rarely used)
  - Priorities, delay, throughput, reliability
- Length
  - Length of entire datagram, in *bytes*
  - 16 bits, hence max. of 65,536 bytes (but see RFC1323)
- Fields for *fragmentation* and *reassembly*
  - Identifier
  - Flags
  - Offset

Header fields, continued

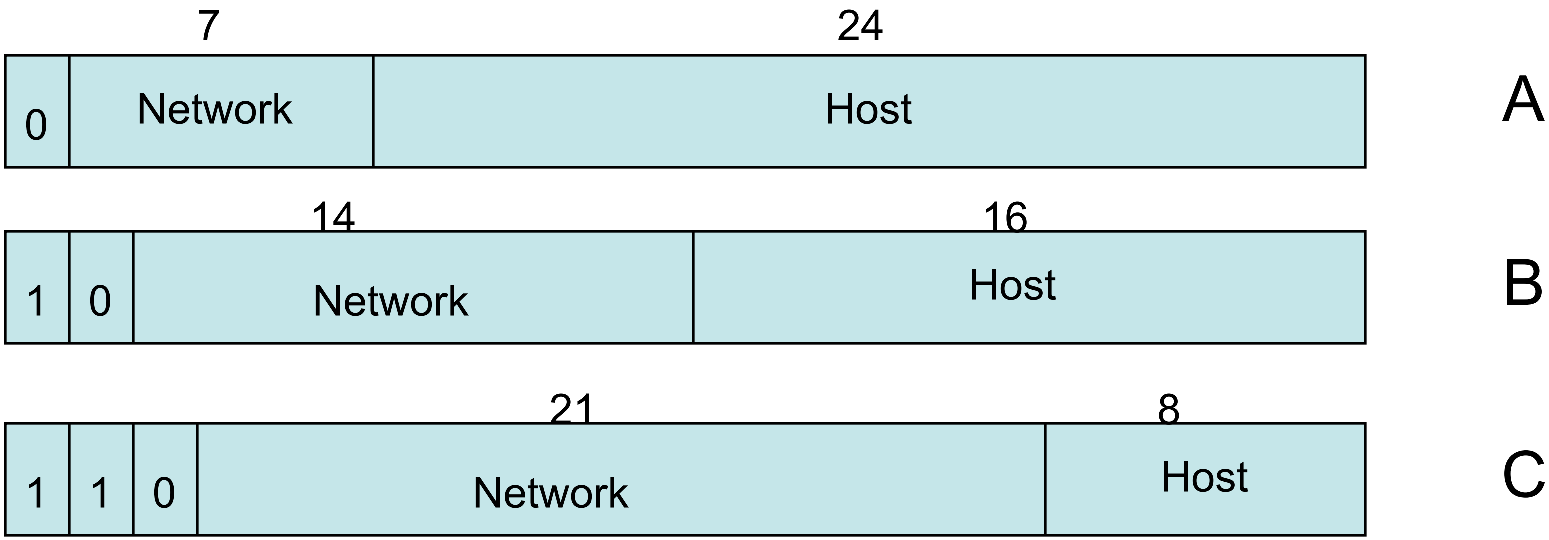
- TTL
  - Time to live (in reality, hop count)
  - 64 is the current default (128 also used)
- Protocol (this demultiplexes to a *transport* protocol)
  - e.g., TCP (6), UDP(17), etc.
- Checksum
  - Checksum of header (not CRC)
  - If header fails checksum, discard the whole packet
- SourceAddr, DestinationAddr
  - 32 bit IP addresses - global, IP-defined
- Options
  - length can be computed using Hlen

IP Datagram Delivery

- Every IP packet (datagram) contains the destination IP address
- The network part of the address uniquely identifies a single network that is part of the larger Internet.
- All hosts and routers that share the same network part of their address are connected to the same physical network.
- Routers can exchange packets on any network they're attached to.

IPv4 addresses – a hierarchy

- Hierarchical, not flat as in Ethernet



- Written as four decimal numbers separated by dots: `158.130.14.2`

Network Classes

Class	*# of nets*	*# of hosts per net*
A	126	~16 million
B	8192	65534
C	~2 million	254

IP forwarding algorithm

```
If (Network # dest == Network #
interface) then deliver to destination
over interface
else if (Network # dest in forwarding
table) deliver packet to NextHop router
else deliver packet to default router
```

Forwarding tables:

- Contain (Network #, NextHop) pairs
- Additional information
- Built by routing protocol that learns the network topology, adapts to changes

Subnetting

- Problem: IP addressing scheme leads to fragmentation
  - a Class B network with only 300 machines on it wastes > 65,000 addresses
  - Need a way to divide up a single network address space into <u>multiple</u> smaller *subnetworks*.
- Idea: One IP network number allocated to several physical networks.
  - The multiple physical networks are called *subnets*
  - Useful when a large company (or university!) has many physical networks.

Subnet Numbers (illustration P&D)

- Solution: *Subnetting*
  - All nodes are configured with *subnet mask*
  - Allows definition of a *subnet number*
    - All hosts on a physical subnetwork share the same *subnet number*

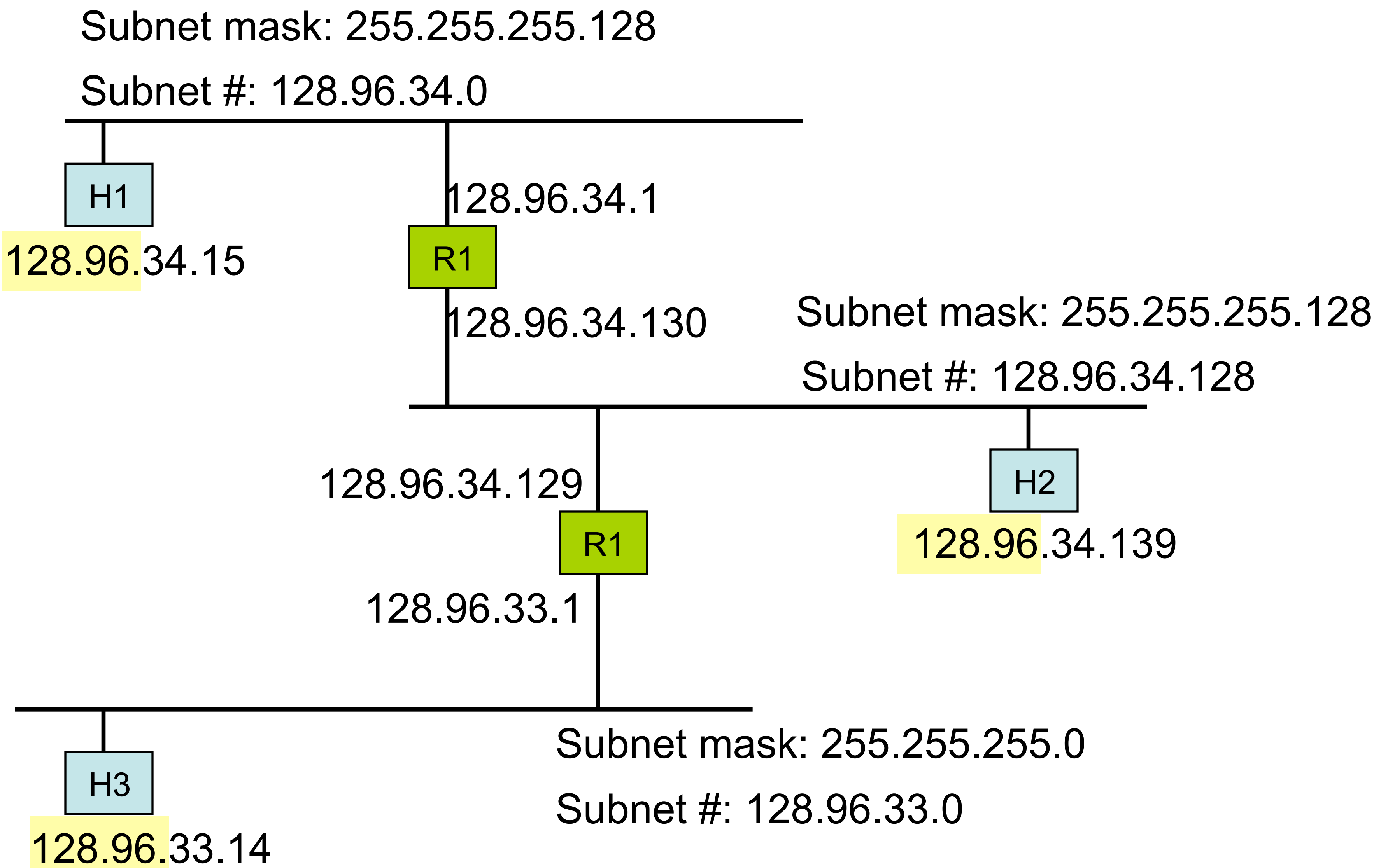
Subnet Mask (255.255.255.0)

111111111111111111111111	00000000

Subnetted Address:

Network number	Subnet ID	Host ID

Example of Subnetting (P&D)



Subnets, continued

- Mask is bitwise-ANDed with address
- This is done at routers
- Router tables in subnet model:
  - <Subnet #, Subnet Mask, NextHop>
- Subnetting allows a set of physical networks to look like a single logical network from elsewhere

Forwarding Algorithm

```
D = destination IP address
For each forwarding table entry
(SubnetNumber, SubnetMask, NextHop):
    D1 = SubnetMask & D
    if  D1 = SubnetNumber
        if NextHop is an interface
            deliver datagram directly to
               destination
        else
            deliver datagram to NextHop
               (router)

Deliver datagram to default router
     (if above fails)
```

ARP - Address Resolution Protocol

- Problem:
  - Need mapping between IP and link layer addresses.

- Solution: ARP
  - Every host maintains IP–Link layer mapping table (cache)
  - Timeout associated with cached info (15 min.)
- Sender
  - Broadcasts "Who is IP addr X?"
  - Broadcast message includes sender's IP & Link Layer address
- Receivers
  - Any host with sender in cache "refreshes" time-out
  - Host with IP address X replies "IP X is Link Layer Y"
  - Target host adds sender (if not already in cache)

ICMP: Internet Control Message Protocol

- Collection of error & control messages
- Sent back to the source when Router or Host cannot process packet correctly
- Error Examples:
  - Destination host unreachable
  - Reassembly process failed
  - TTL reached 0 (use in `traceroute`!)
  - IP Header Checksum failed
- Control Example:
  - Redirect – tells source about a better route

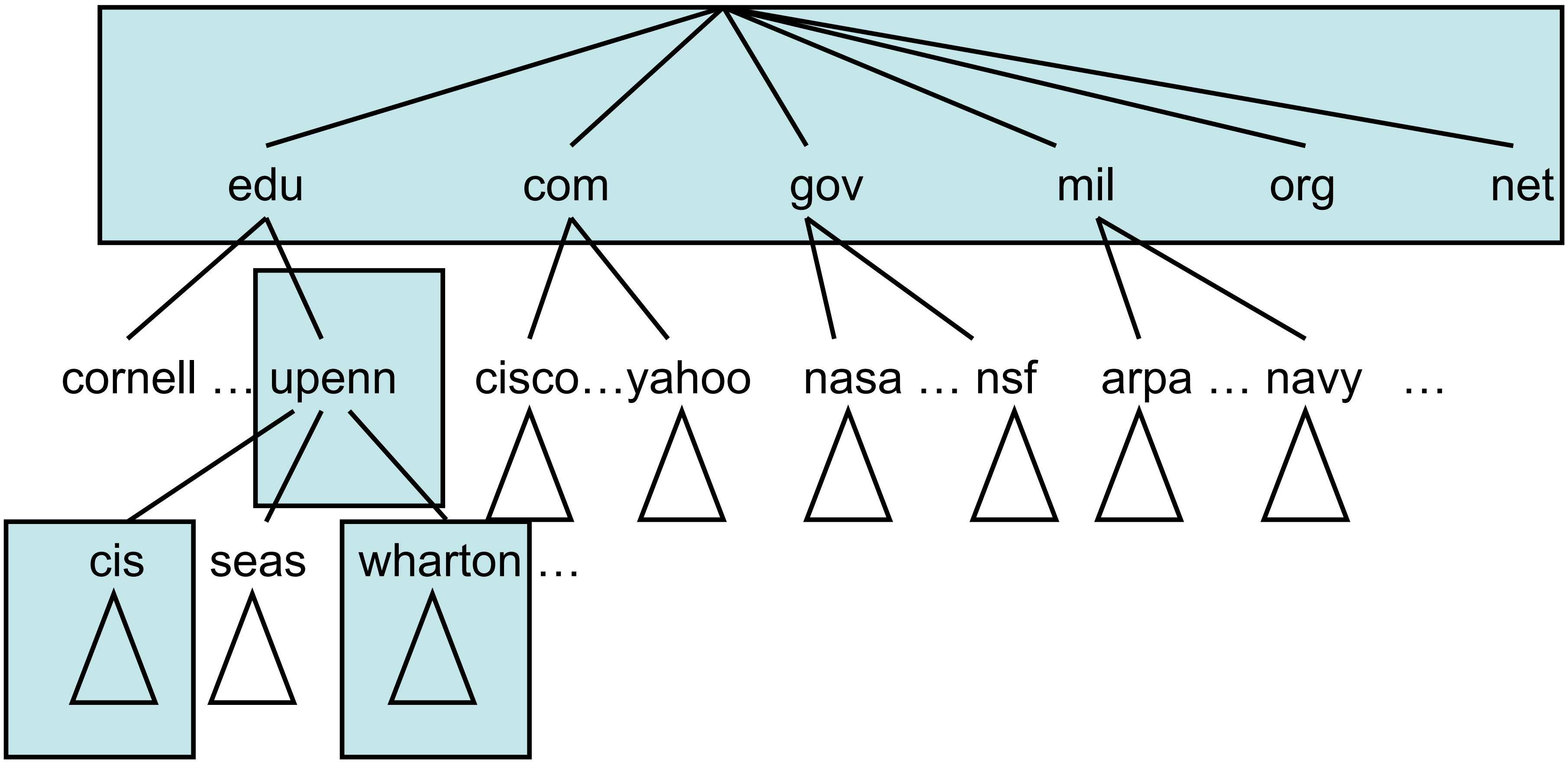
Domain Name System

- System for mapping mnemonic names for computers into IP addresses.

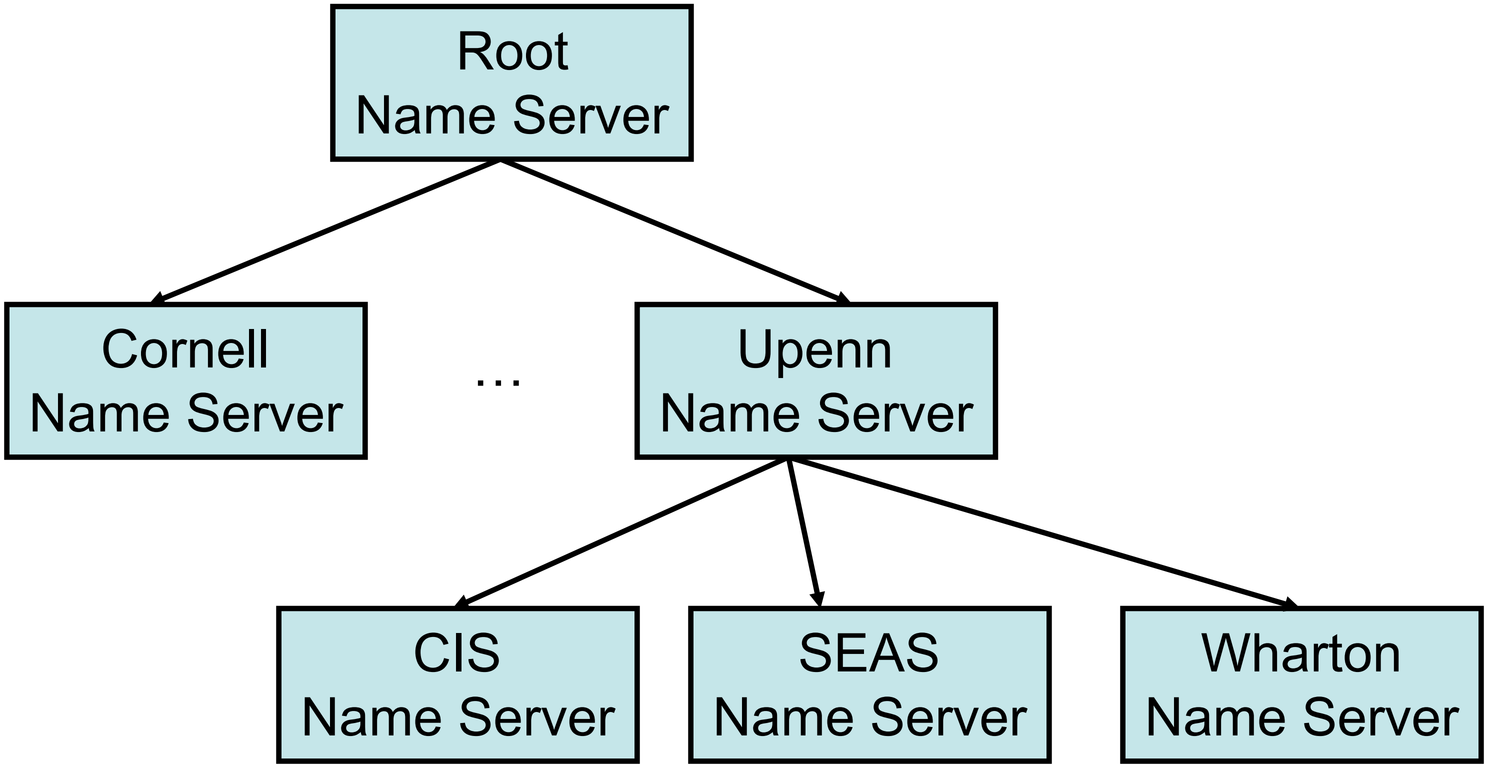
`central.cis.upenn.edu` → `158.130.66.68`

- Domain Hierarchy
- Name Servers
  - 13 Root servers map top-level domains such as ".com" or ".net”
- Name Resolution
  - Protocol for looking up hierarchical domain names to determine the IP address
  - Protocol runs on UDP port 53

Domain Name Hierarchy



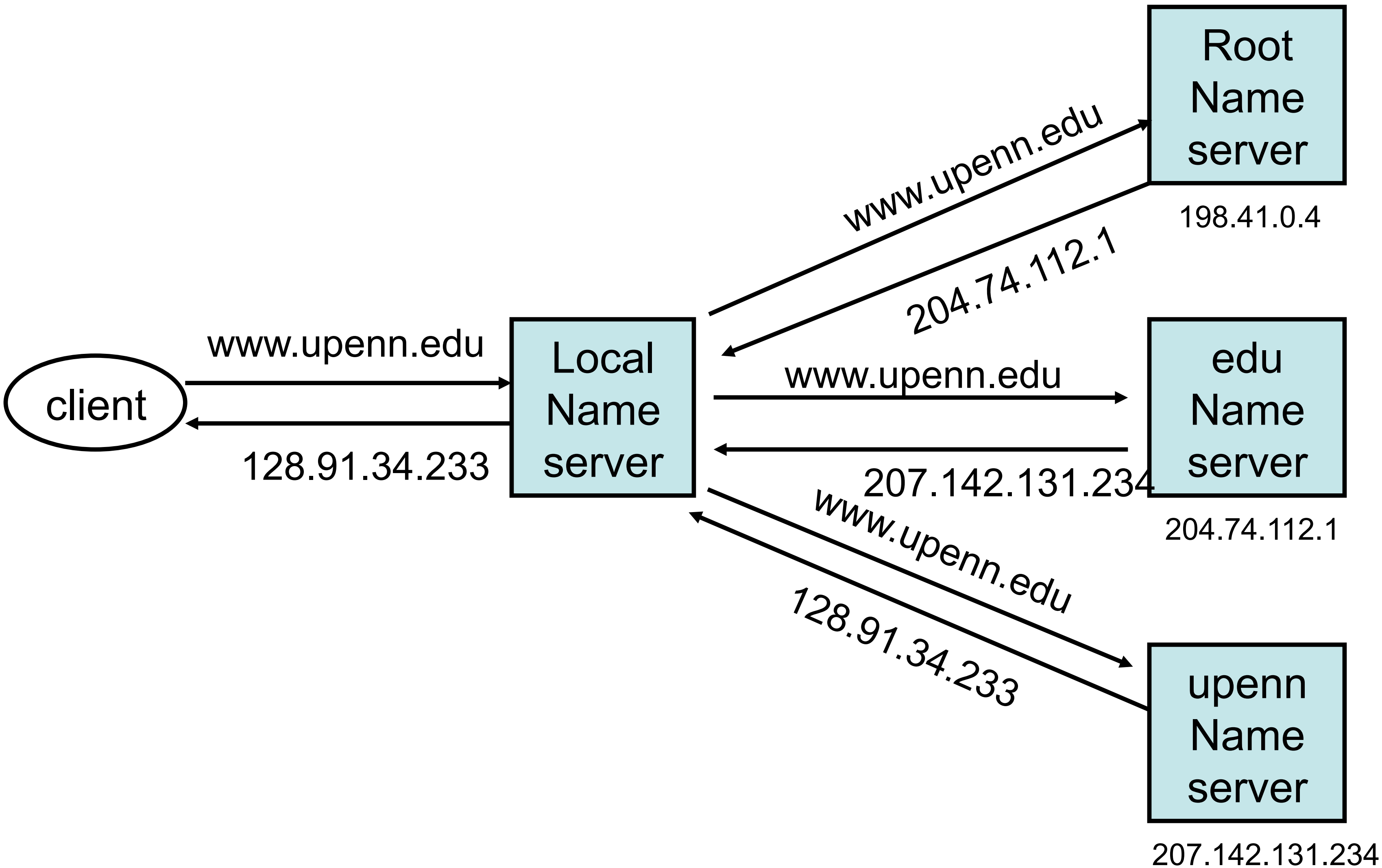
Hierarchy of Name Servers



Records on Name Servers

- < Name, Type, Class, TTL, RDLength, RDATA >
- Name of the node
- Types:
  - A Host to address mappings
  - NS Name server address mappings
  - CNAME Aliases
  - MX Mail exchange server mappings
  - … others
- Class IN for IP addresses

Name resolution



DNS Vulnerabilities

- See *"Corrupted DNS Resolution Paths: The rise of a malicious resolution authority"* by Dagon et al.
- Rogue DNS Servers
  - Compromised DNS servers that answer incorrectly
  - Do applications check for this???
- DNS Cache Poisoning
  - Request: `subdomain.example.com IN A`
  - Reply:

```
Answer:
(no response)

Authority section:
example.com. 3600 IN NS ns.wikipedia.org.

Additional section:
ns.wikipedia.org IN A w.x.y.z
```

Reflected denial of service

- ICMP message with an "echo request" is called 'ping'
  - "`man ping`"
- Broadcast a `ping` request
  - For sender's address, put target's address
  - All hosts reply to `ping`, flooding the target with responses

- Hard to trace
- Hard to prevent
  - Turn off `ping`? (Makes legitimate use impossible)
  - Limit with network configuration by restricting scope of broadcast messages (demo)

- Sometimes called a "smurf attack"

(Distributed) Denial of Service

- Coordinate multiple subverted machines to attack
- Flood a server with bogus requests
  - TCP SYN packet flood
  - > 600,000 packets per second
- Feb. 6 2007: 6 of 13 root servers suffered DDoS attack
- Oct. 21 2002: 9 of 13 root servers were swamped

- Prevention?
  - Filtering?
  - Decentralized data storage?