Lecture 20 – Denial of Service Continued

November 1, 2018

Dr. Dan Massey

Reflection Attacks

- Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- When intermediary responds, the response is sent to the target
- “Reflects” the attack off the intermediary (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- The basic defense against these attacks is blocking spoofed-source packets

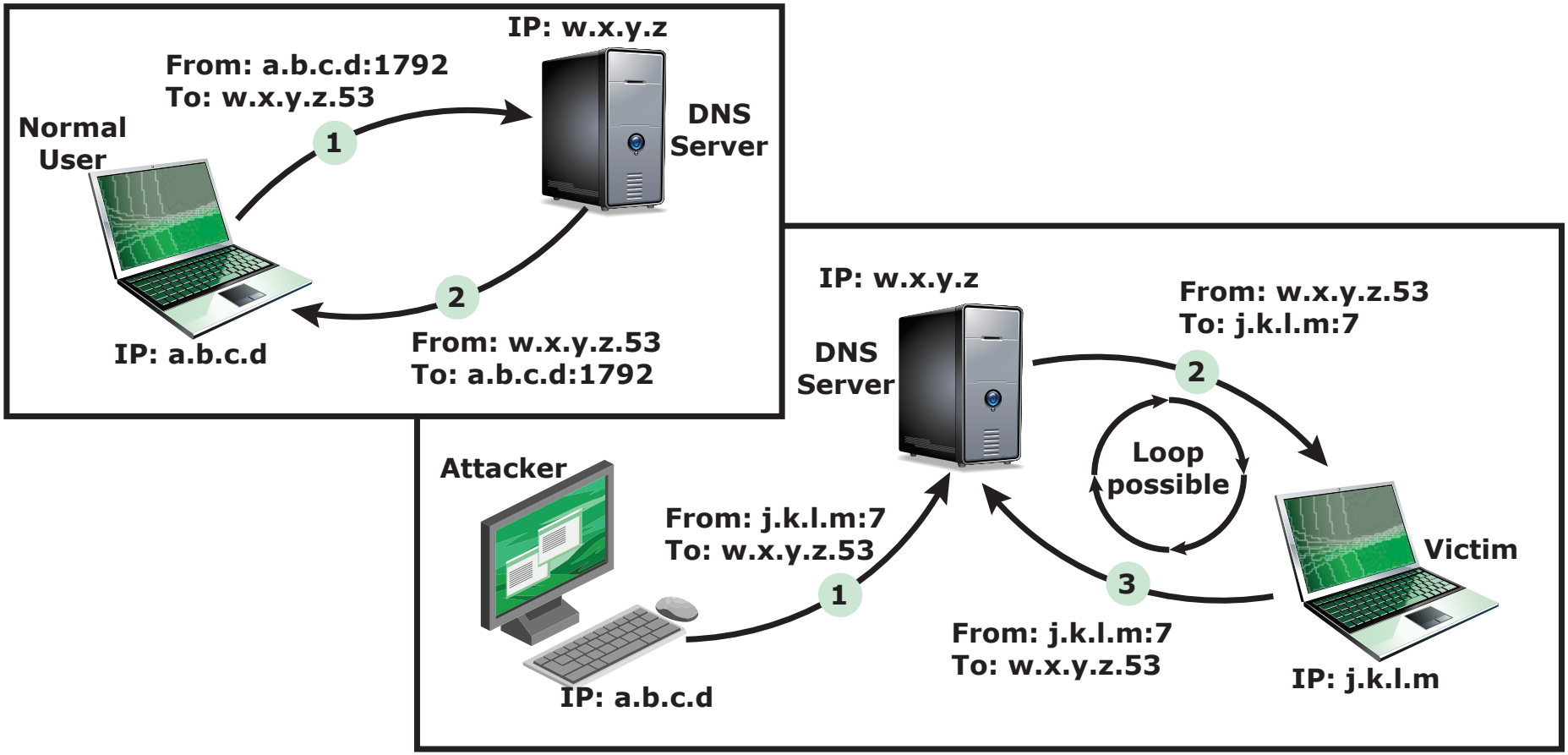


Figure 7.6 DNS Reflection Attack

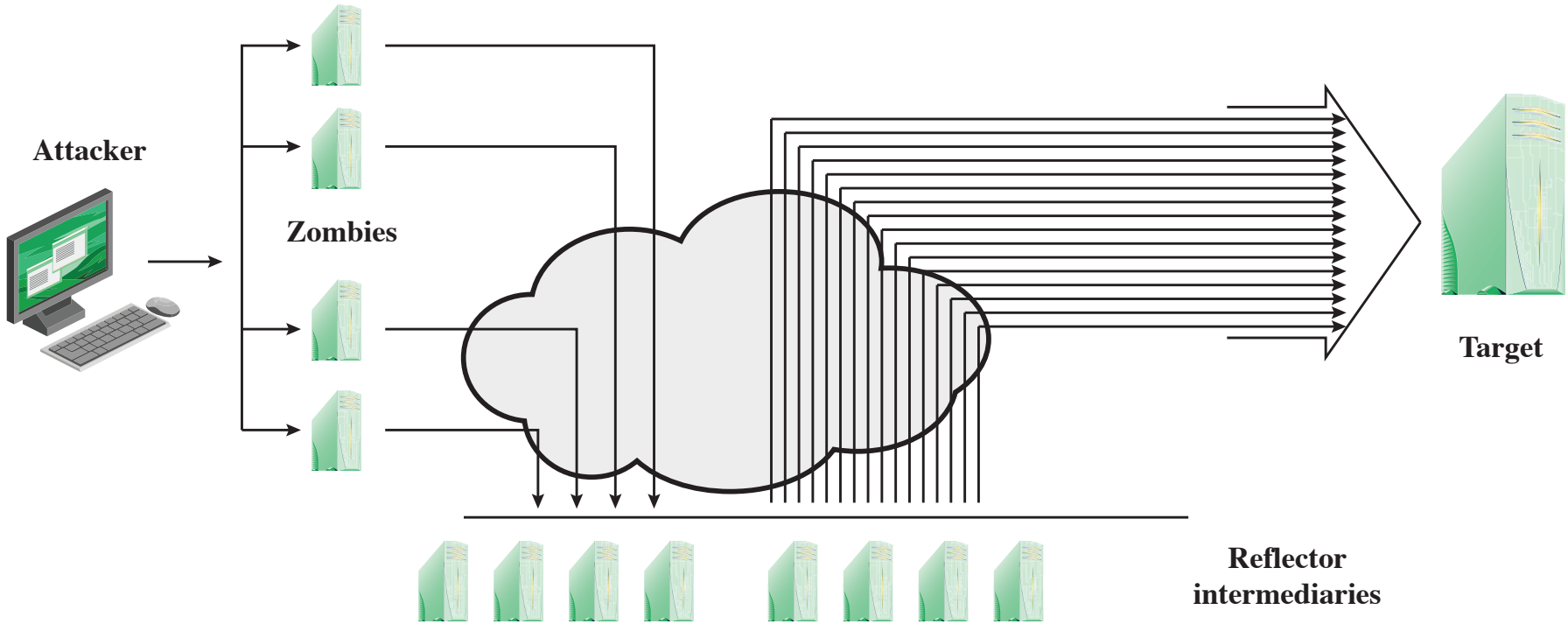
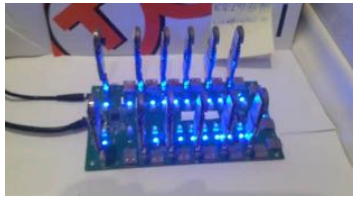


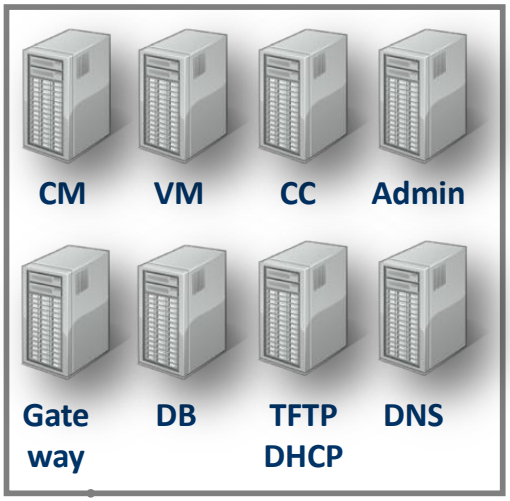
Figure 7.7 Amplification Attack

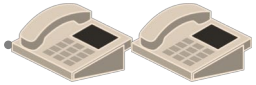
DNS Amplification Attacks

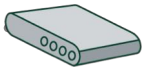
- Use packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
- Target is flooded with responses
- Basic defense against this attack is to prevent the use of spoofed source addresses

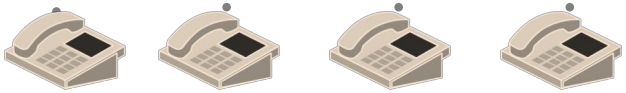
TDoS Threat – Disable 911

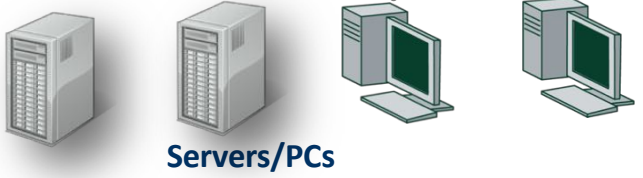












Public Voice Network

TDM/SIP Trunks

TDM Phones

Modem

Fax

Voice VLAN

IP Phones

Internet

Internet Connection

Firewall
IDS/IPS
DDoS Mitigation

Data VLAN

UC Clients

Servers/PCs

911 Statistics

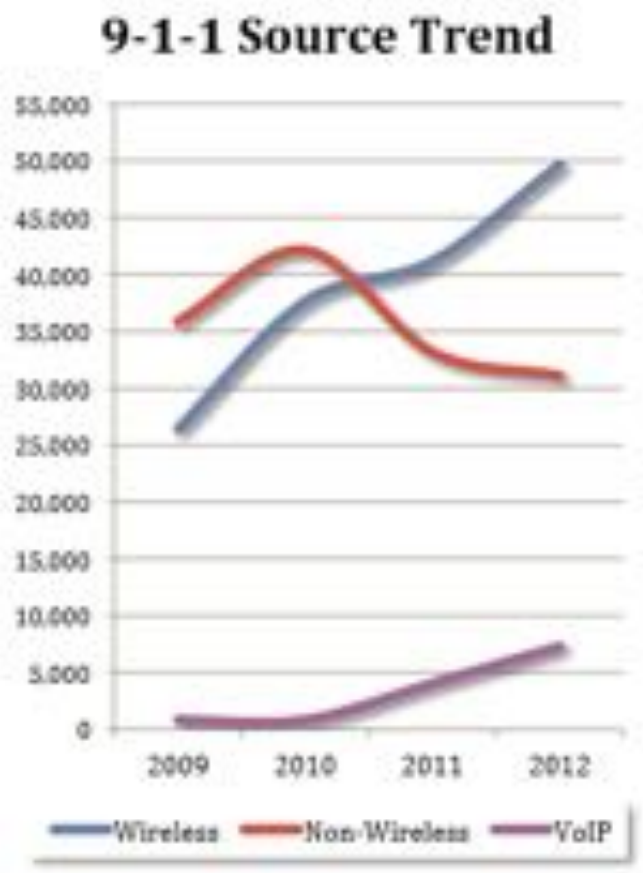
- There are **240 Million** calls to 9-1-1 each year, in some communities, 50% of those calls are made from a mobile device – NENA

2012 Annual Statistics

Telephone Statistics

Group	Incoming	Outgoing	Total Calls
911 – EMS	37,396	0	37,396
911 – Fire	7,691	0	7,691
911 – Law	49,315	0	49,315
Admin	41,531	9,7902	139,433
Business – EMS	20,805	26	20,831
Business – Fire	23,179	716	23,895
Business – Law	51,161	47	51,208
Emergency – EMS	21,514	1,172	22,686
Emergency – Fire	33,631	236	33,867
Emergency – Law	96,237	46	96,283
Microwave	8,957	17,687	26,644
Miscellaneous	10,659	8	10,667
Totals	**402,076**	**117,840**	**519,916**

Source: Overview of the San Mateo County Office of Public Safety Communications. 2012.



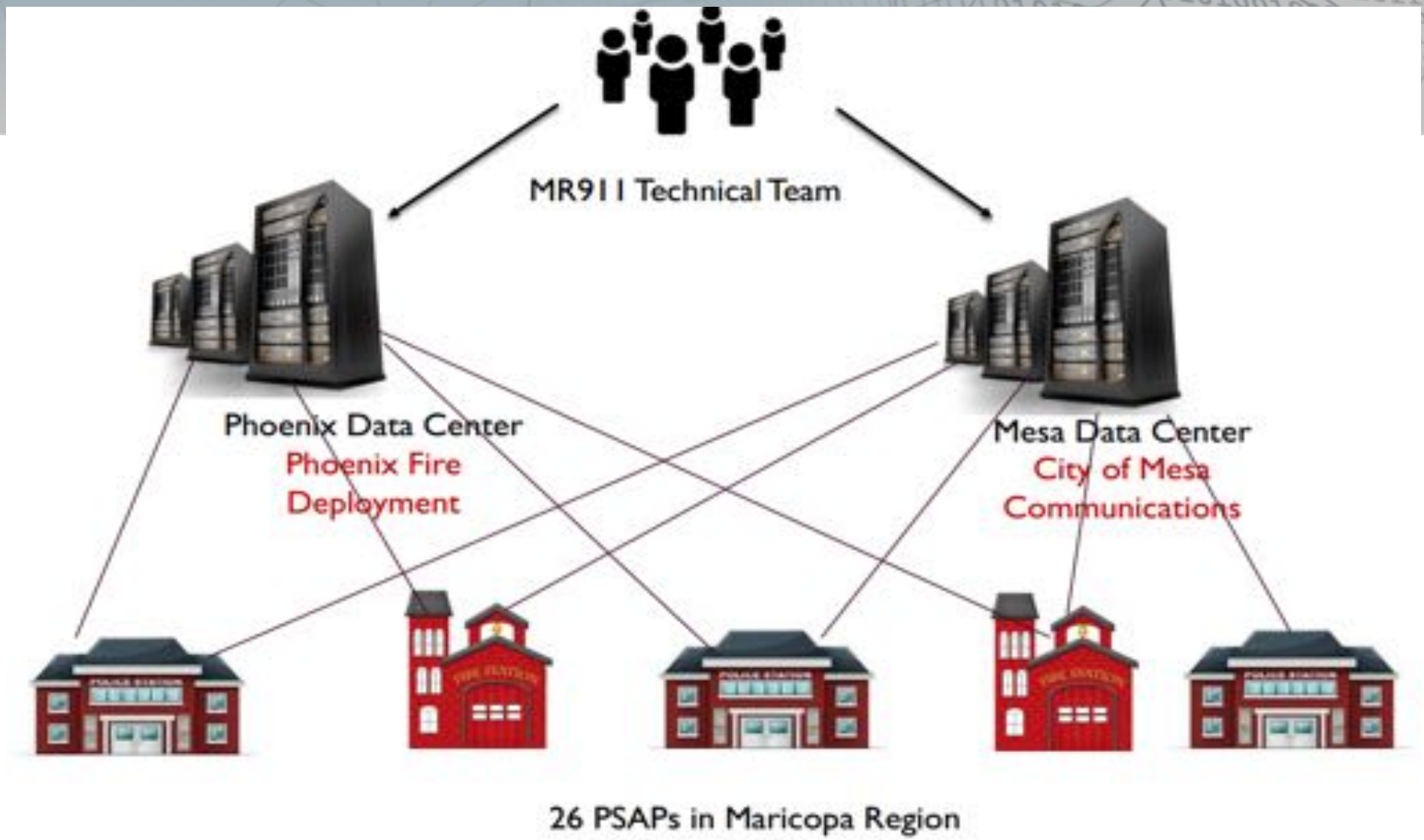
Current State of the Art from FCC

- *In 38 states, no money was spent in 2015 on cyber security for 9-1-1 centers.*
- *420 out of 6,500 9-1-1 centers had implemented a cyber security program.*

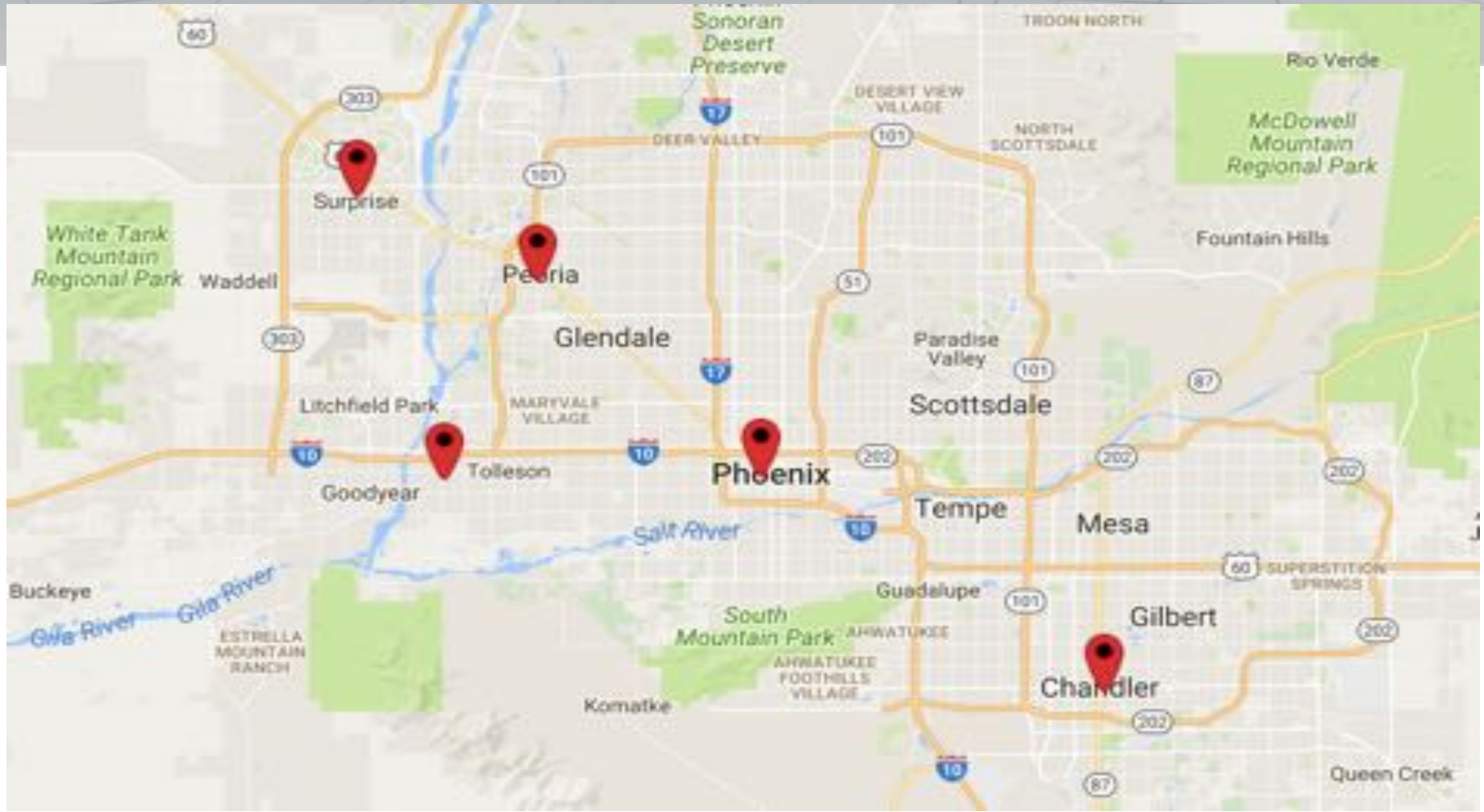
A Multi-State TDoS Attack on 9-1-1

- **INCIDENT:** *TDoS attack against PSAPS in multiple states.*
- **CAUSES:** *The attack was distributed/propagated through a Twitter mobile application.*
- **AFFECTED STATES:** *PSAPs in many states including Arizona, Texas, California, Florida, Washington State, Minnesota.*
- **DURATION:** *Approximately 10:00 p.m. on* ***October 25, 2016*** *– 2:00 a.m.* ***on October 26, 2016*** *local incident time.*

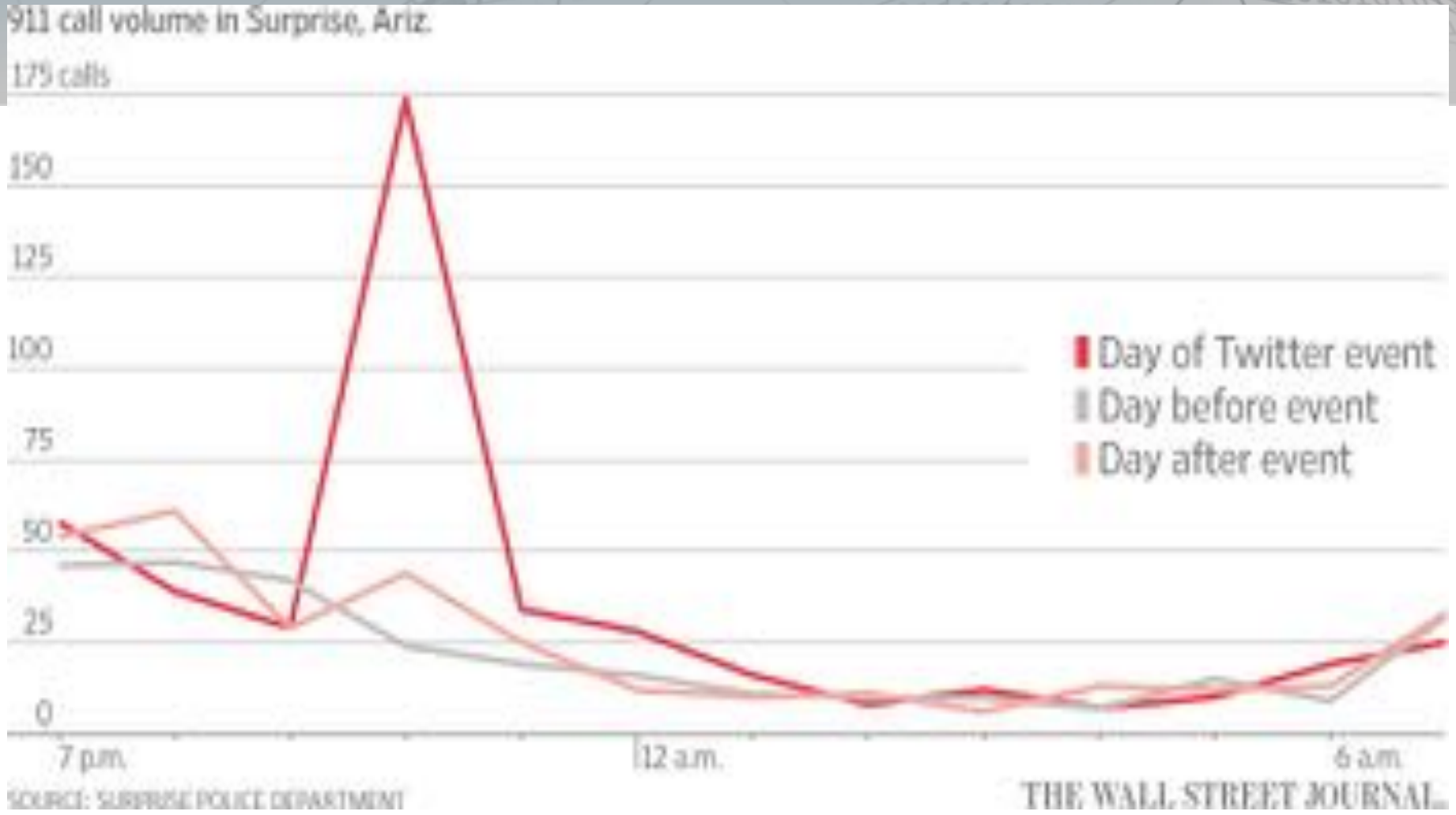
Maricopa Regional 9-1-1 Infrastructure



PSAPs in Maricopa Affected by the Oct TDoS Attack



Example Call Volume - Surprise, Ariz



The Oct 2016 Malware

- The TDoS malware exploits an iOS WebView auto dialer bug.
  - After clicking, the malware blocks the phone's UI.
  - It causes iOS to open a second application while the phone is dialing the given number.
  - User has no control to cancel the call.
- The bug was first discovered in 2008 by Collin Mulliner.
- It affects all iOS apps that embed WebView.
- The malware is written using Java script.

The Oct 2016 Attacker

- The code was first posted online by a teenage in *Phoenix, Arizona*.
- The original version was described in a Youtube video "Freak out your friends" without using 9-1-1 as the target phone number.
- The teenage made a 9-1-1 version, posted it online, and sent the link to the person who made the video.
- The link was added to the video's caption. The Youtube channel has 250K followers.
- Retweeted link including account with over 400K followers.

The Investigation

- Investigator confirmed identity of the teenage from screenshot of Internet speed test posted on social media website.

- The test records longitude and latitude information.

The picture on the right side is not the original one.

Lessons Learned

- TDoS caused by **mobile malware** poses a real threat.
- **Social media** can accelerate spread of the attack.
- The consequence could have be **much worse** if not from a teenage hacktivist.
- Similar attack could happen again in future.

Mitigating The DDoS Threat

(1) Measurement and Analysis to Promote Best Current Practices

Slow the growth in DDoS attacks by adopting best practices

(2) Tools for Communication and Collaboration

Provide existing targets more effective tools and techniques for response and mitigation.

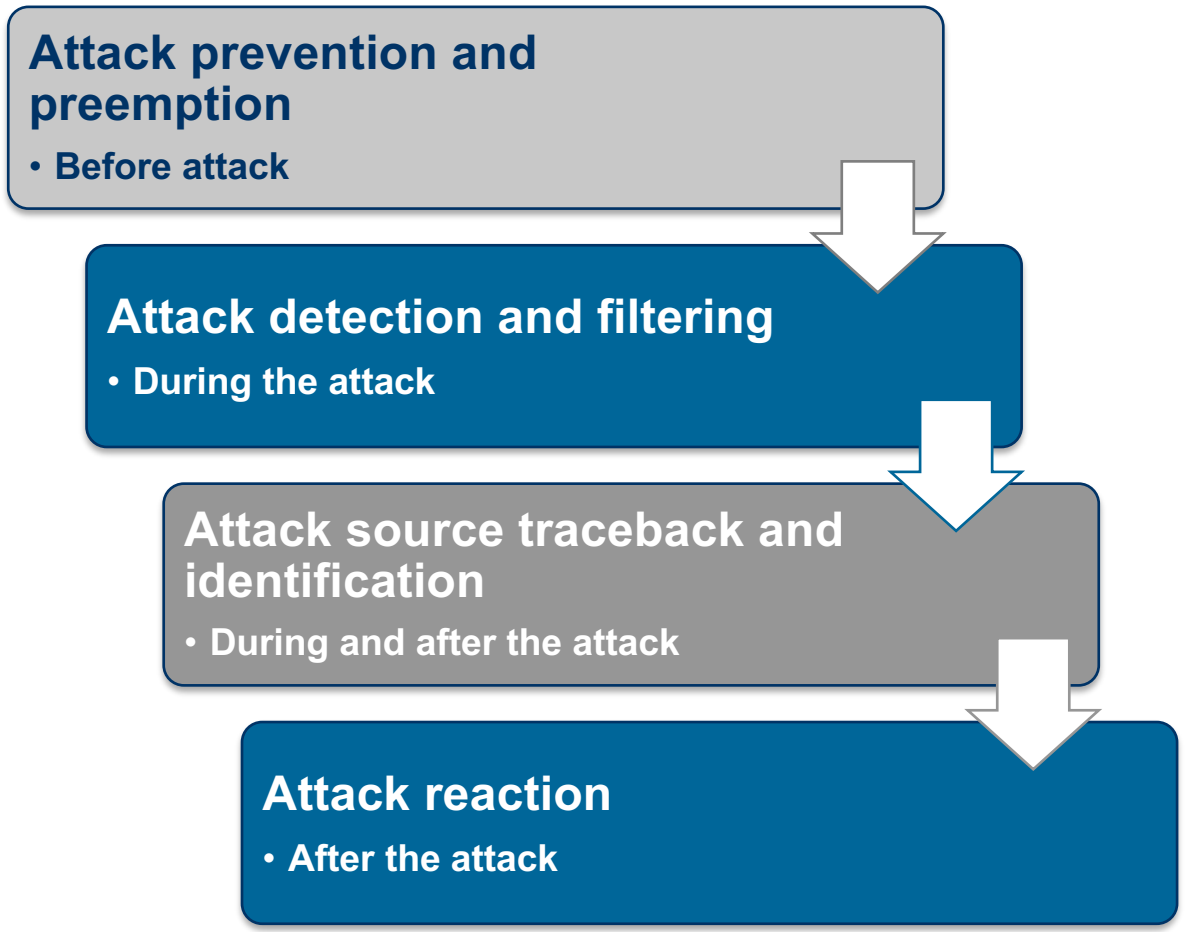
(3) Novel DDoS Attack Mitigation and Defense Techniques

Anticipate new types of attacks before they occur and apply novel new approaches to mitigation.

DoS Attack Defenses

- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
  - High publicity about a specific site
  - Activity on a very popular site
  - Described as *slashdotted, flash crowd, or flash event*

Four lines of defense against DDoS attacks



DoS Attack Prevention

- Block spoofed source addresses
  - On routers as close to source as possible
- Filters may be used to ensure path back to the claimed source address is the one being used by the current packet
  - Filters must be applied to traffic before it leaves the ISP's network or at the point of entry to their network
- Use modified TCP connection handling code
  - Cryptographically encode critical information in a cookie that is sent as the server's initial sequence number
    - Legitimate client responds with an ACK packet containing the incremented sequence number cookie
  - Drop an entry for an incomplete connection from the TCP connections table when it overflows

DoS Attack Prevention

- Block IP directed broadcasts
- Block suspicious services and combinations
- Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability is required

Responding to DoS Attacks

Good Incident Response Plan

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

- Antispoofing, directed broadcast, and rate limiting filters should have been implemented
- Ideally have network monitors and IDS to detect and notify abnormal traffic patterns

Responding to DoS Attacks

- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Or identify and correct system/application bug
- Have ISP trace packet flow back to source
  - May be difficult and time consuming
  - Necessary if planning legal action
- Implement contingency plan
  - Switch to alternate backup servers
  - Commission new servers at a new site with new addresses
- Update incident response plan
  - Analyze the attack and the response for future handling

Summary

- Denial-of-service attacks
  - The nature of denial-of-service attacks
  - Classic denial-of-service attacks
  - Source address spoofing
  - SYN spoofing
- Flooding attacks
  - ICMP flood
  - UDP flood
  - TCP SYN flood
- Defenses against denial-of-service attacks
- Responding to a denial-of-service attack
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
  - SIP flood
  - HTTP-based attacks
- Reflector and amplifier attacks
  - Reflection attacks
  - Amplification attacks
  - DNS amplification attacks

Motivating Example: SNORT Rule

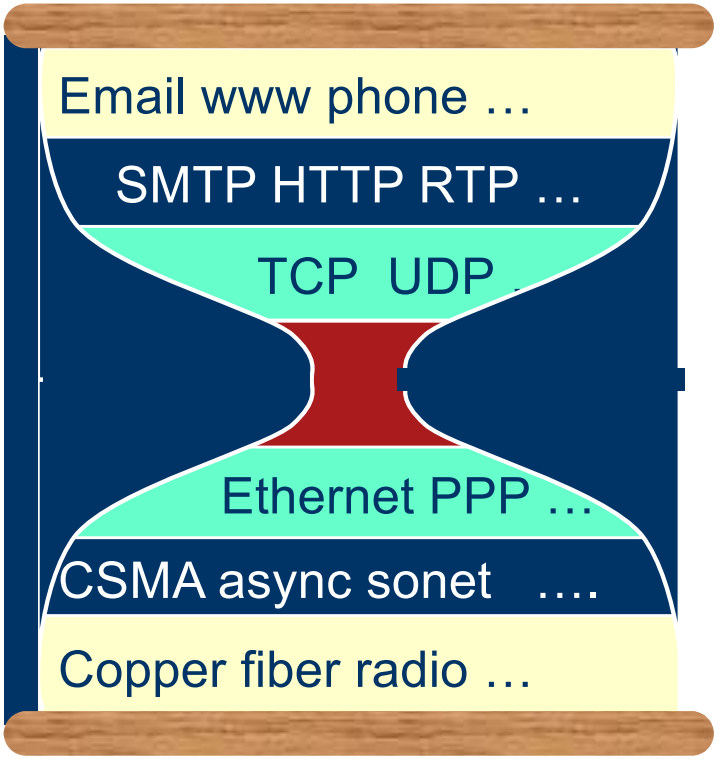
- alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-ATTACKS /bin/ps command attempt"; flow:to_server,established; uricontent:"/bin/ps"; nocase; classtype:web-application-attack; sid:1328; rev:6;)

Network Layer Basics: IP Format and Addressing
Transport Layer Basics: UDP/TCP Header and connections
Application Layer: vast numbers of applications

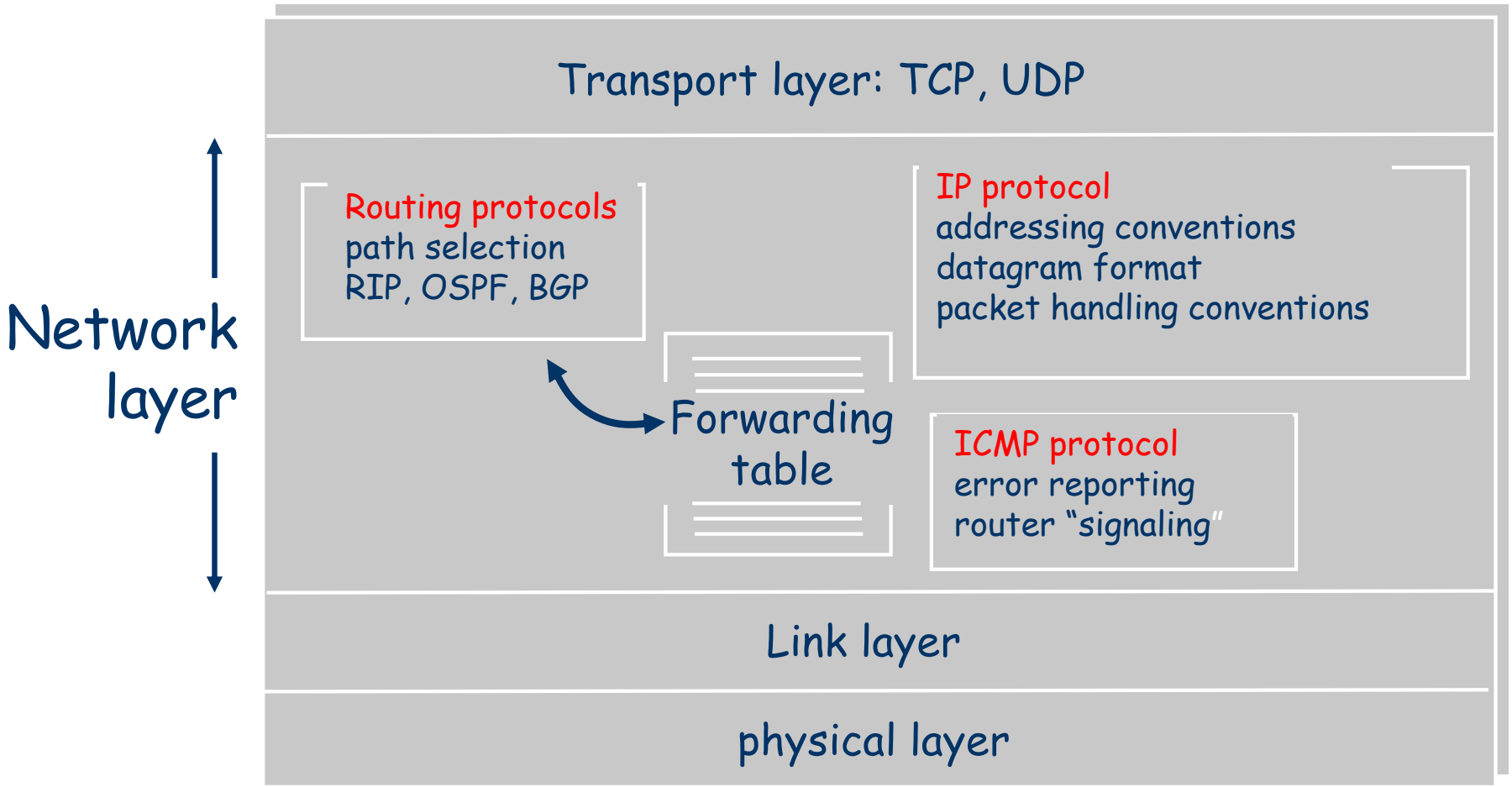
Establish a Set of Basic Network Concepts

Internet is a Layered Architecture

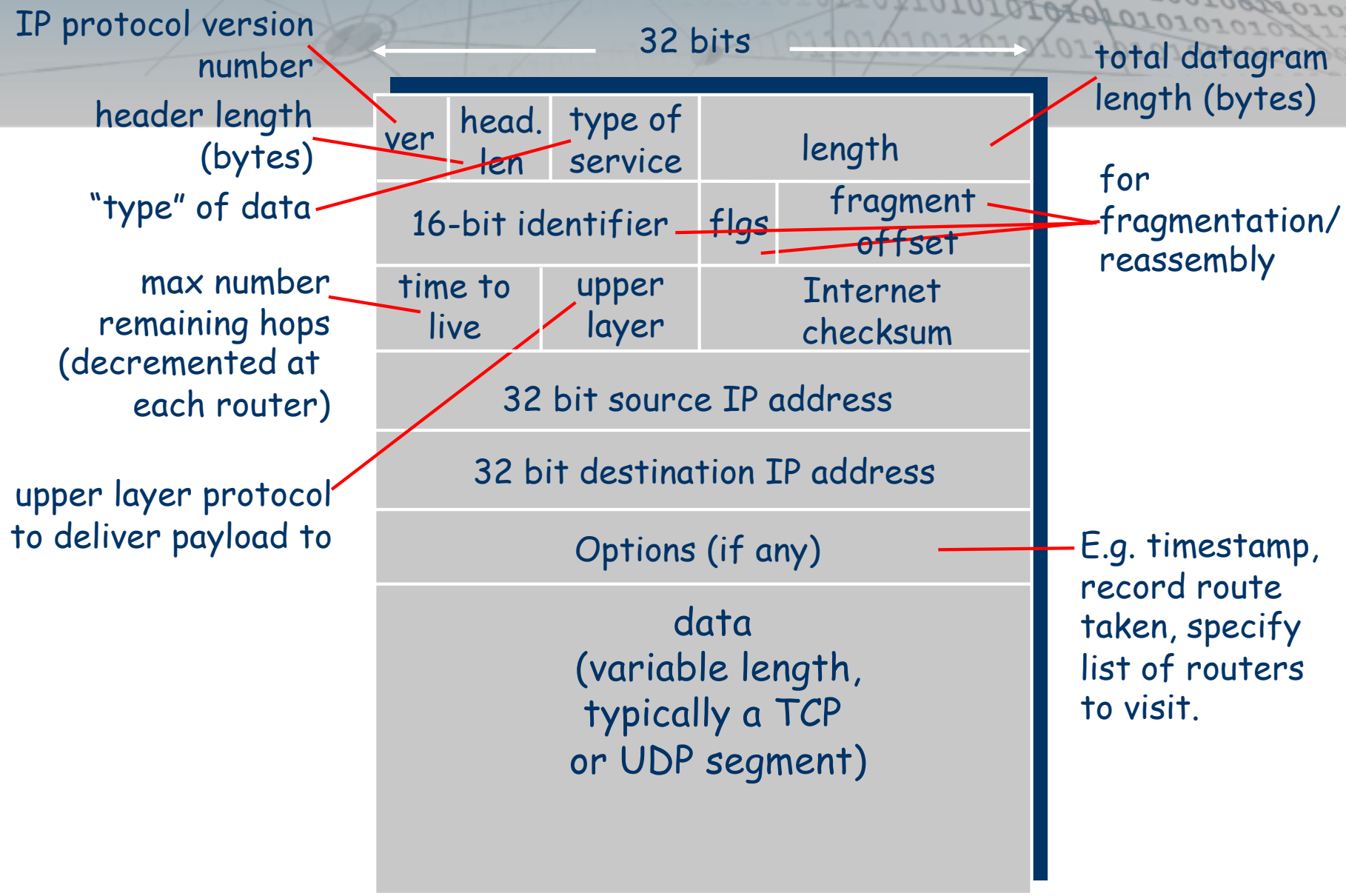
- Application layer
  - Communication between networked applications
  - Protocols: HTTP, FTP, NTP, and many others
- Transport layer
  - Communication between processes
  - Protocols: TCP and UDP
- Network layer
  - Communication between nodes
  - Protocols: IP
- Link and Physical Layers
  - Communication between devices
  - Ethernet, Wifl, Bluetooth, and many others



The Network layer

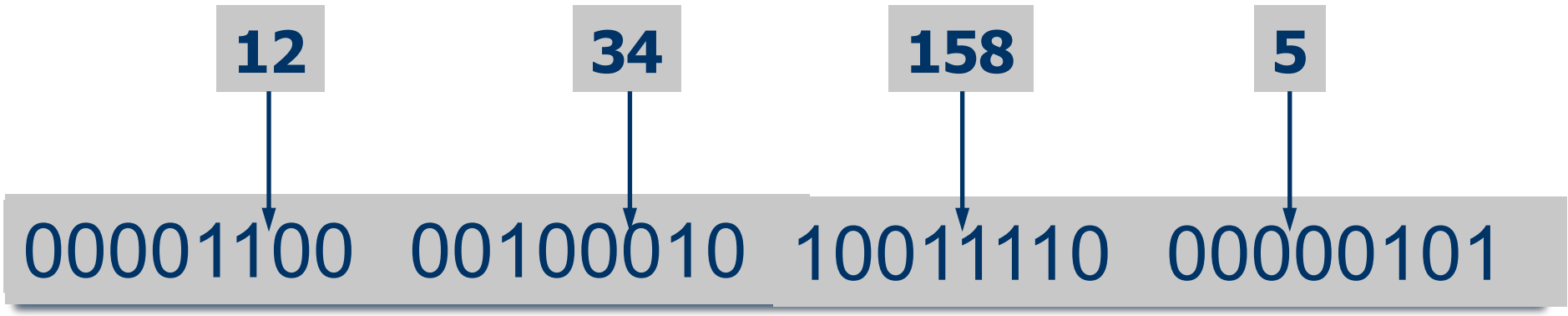


IP Datagram Format



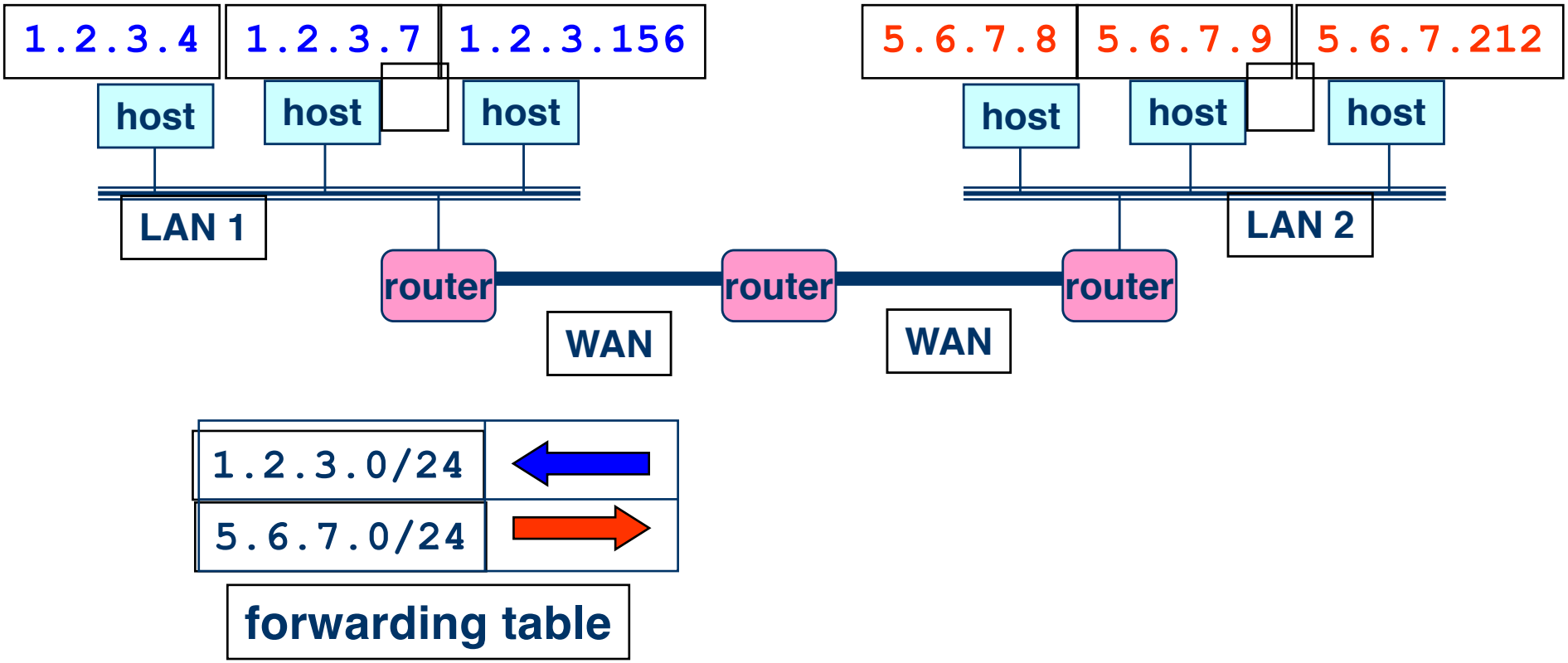
IP Address (IPv4)

- A unique 32-bit number
  (i.e., 4B addresses)
- Identifies an interface
  (on a host, on a router, …)
- Represented in dotted-quad notation



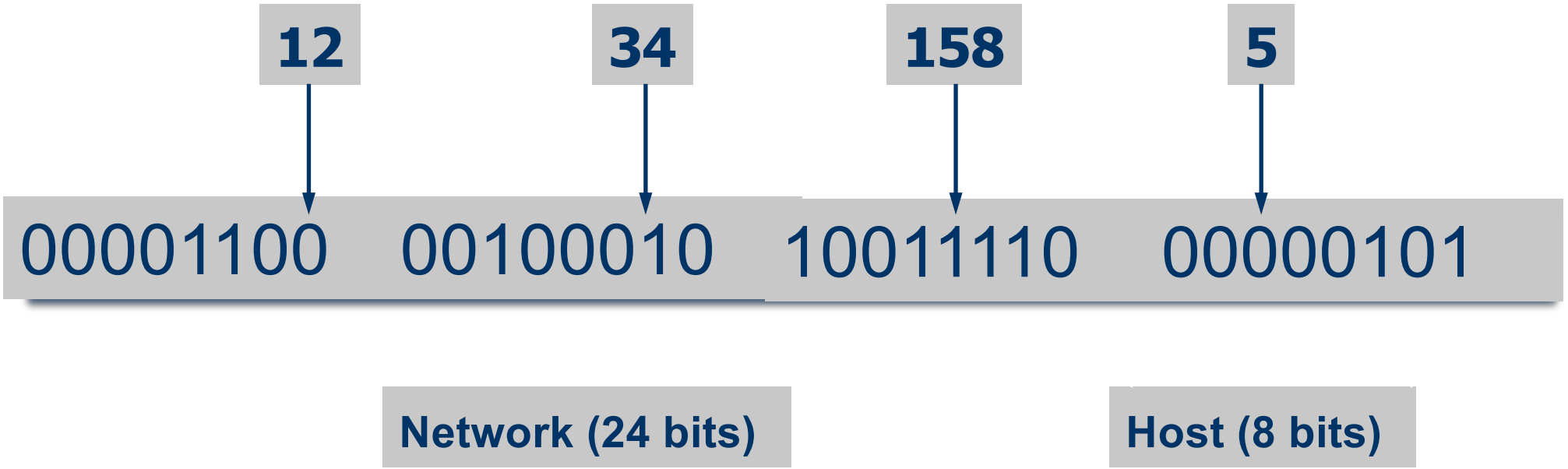
IP Addressing and Subnets

- Number related hosts from a common subnet
  - 1.2.3.0/24 on the left LAN
  - 5.6.7.0/24 on the right LAN



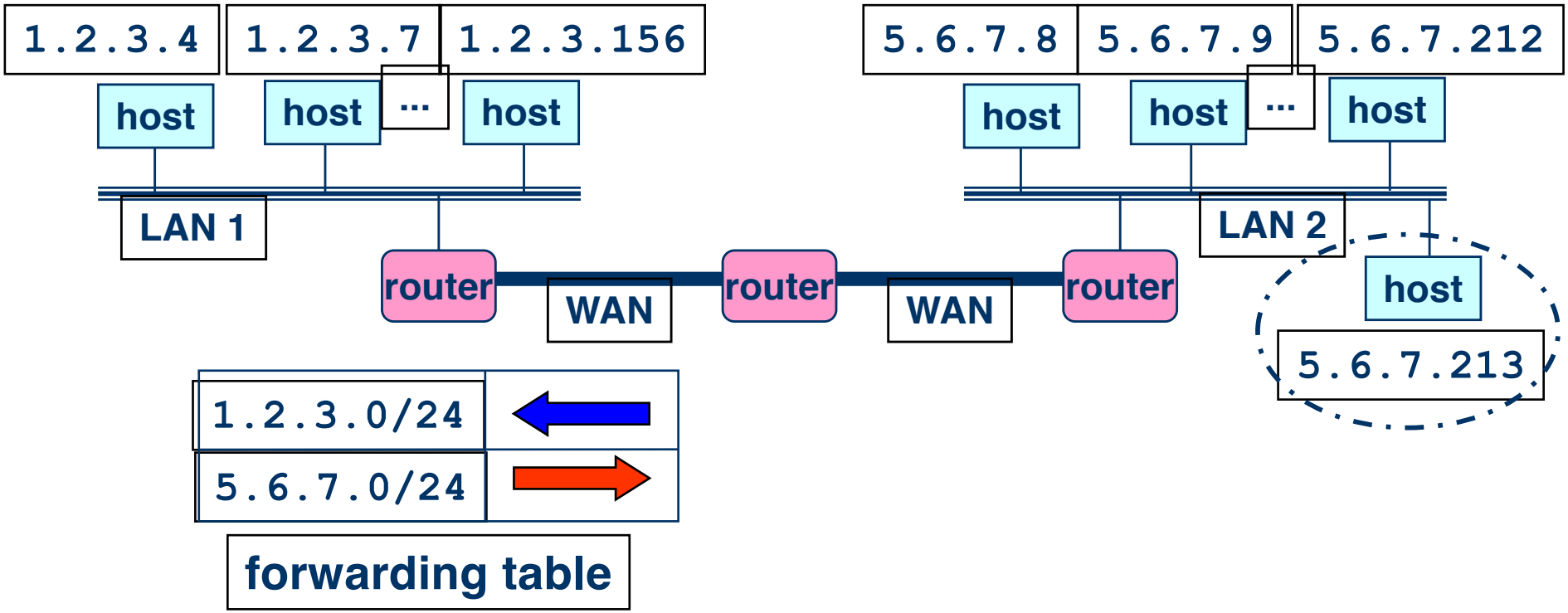
Hierarchical Addressing: IP Prefixes

- Divided into network & host portions (left and right)
- 12.34.158.0/24 is a 24-bit prefix with 2^8 addresses



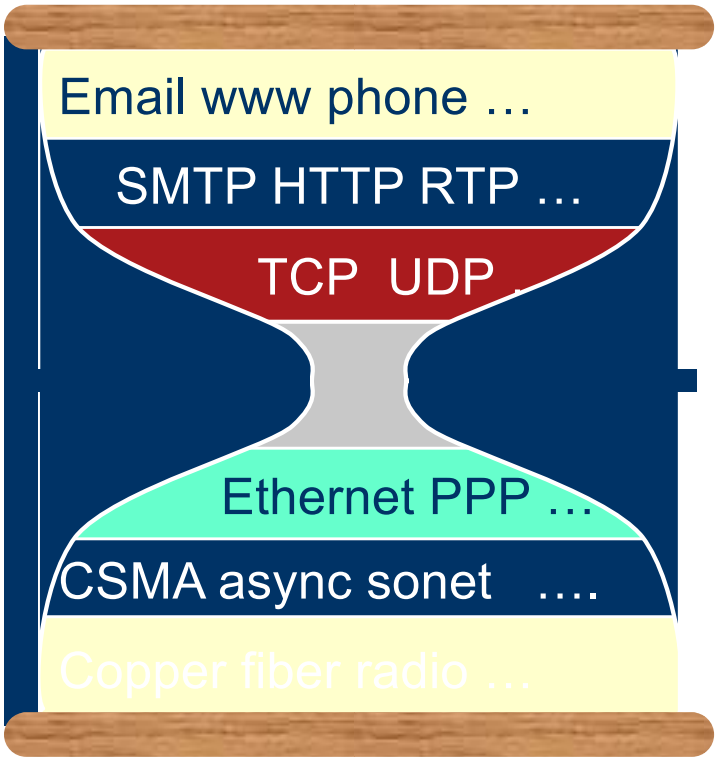
Easy to Add New Hosts

- No need to update the routers
  - E.g., adding a new host 5.6.7.213 on the right
  - Doesn't require adding a new forwarding entry



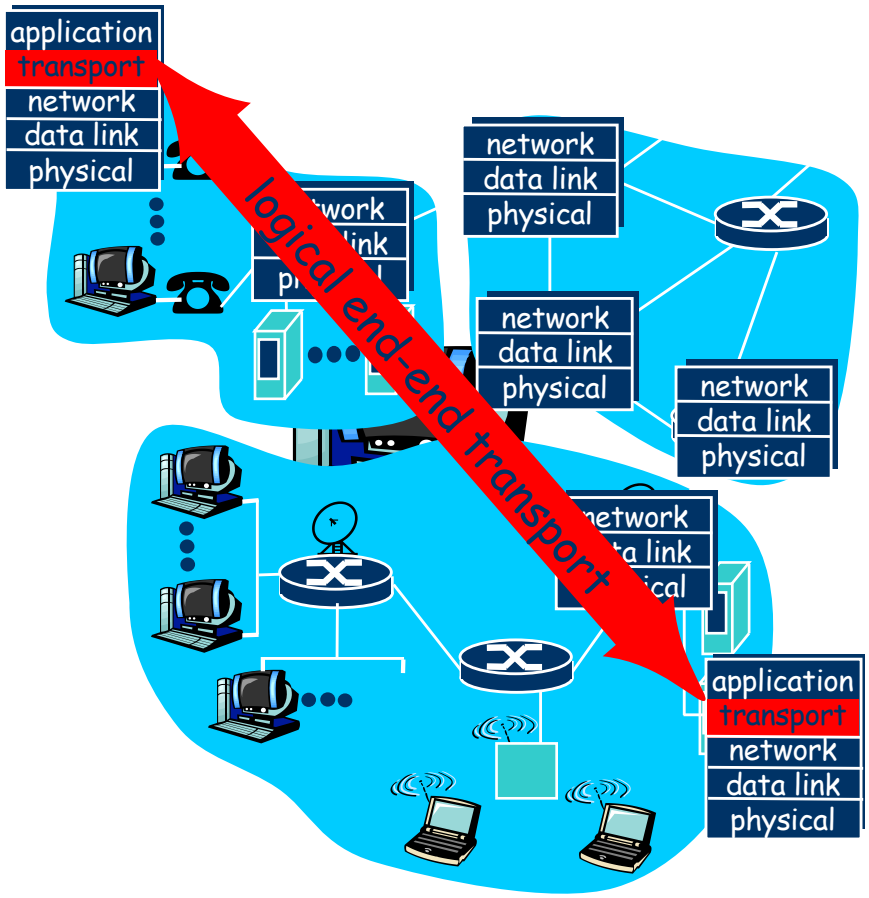
Role of Transport Layer

- Application layer
  - Communication between networked applications
  - Protocols: HTTP, FTP, NNTP, and many others
- **Transport layer**
  - **Communication between processes**
  - **Relies on network layer and serves the application layer**
  - **Protocols: TCP and UDP**
- Network layer
  - Communication between nodes
  - Protocols: IP



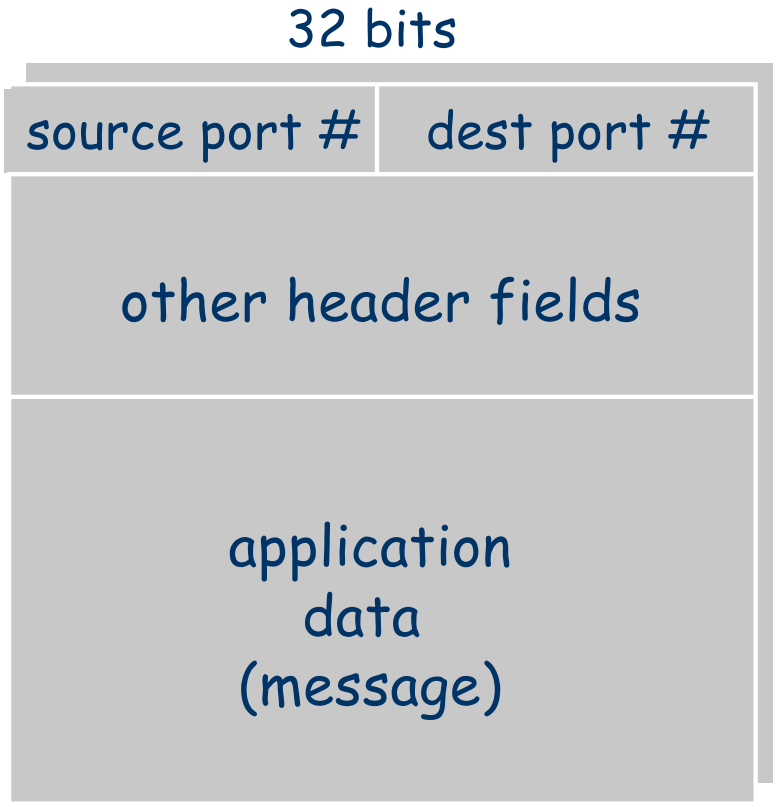
Transport Protocols

- Provide *logical communication* between application processes running on different hosts
- Run on end hosts
  - Sender: breaks application messages into segments, and passes to network layer
  - Receiver: reassembles segments into messages, passes to application layer
- Multiple transport protocol available to applications
  - Internet: TCP and UDP



Multiplexing and Demultiplexing

- Host receives IP datagrams
  - Each datagram has source and destination IP address,
  - Each datagram carries one transport-layer segment
  - Each segment has source and destination port number
- Host uses IP addresses and port numbers to direct the segment to appropriate socket

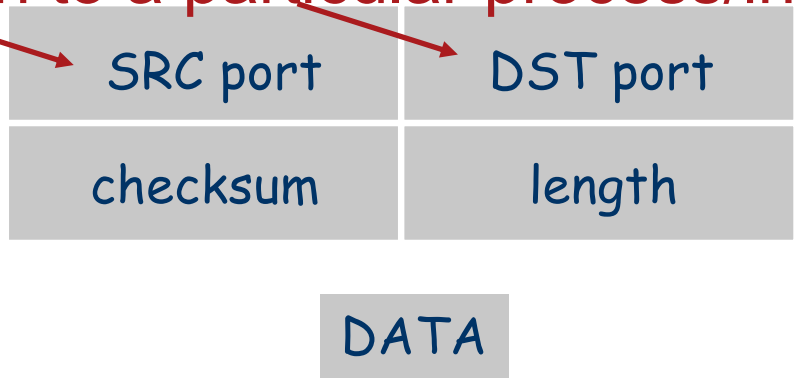


TCP/UDP segment format

User Datagram Protocol (UDP)

- Lightweight communication between processes
  - Avoid overhead and delays of ordered, reliable delivery
  - Send messages to and receive them from a socket
- Lightweight delivery service
  - IP plus port numbers to support (de)multiplexing
  - Optional error checking on the packet contents

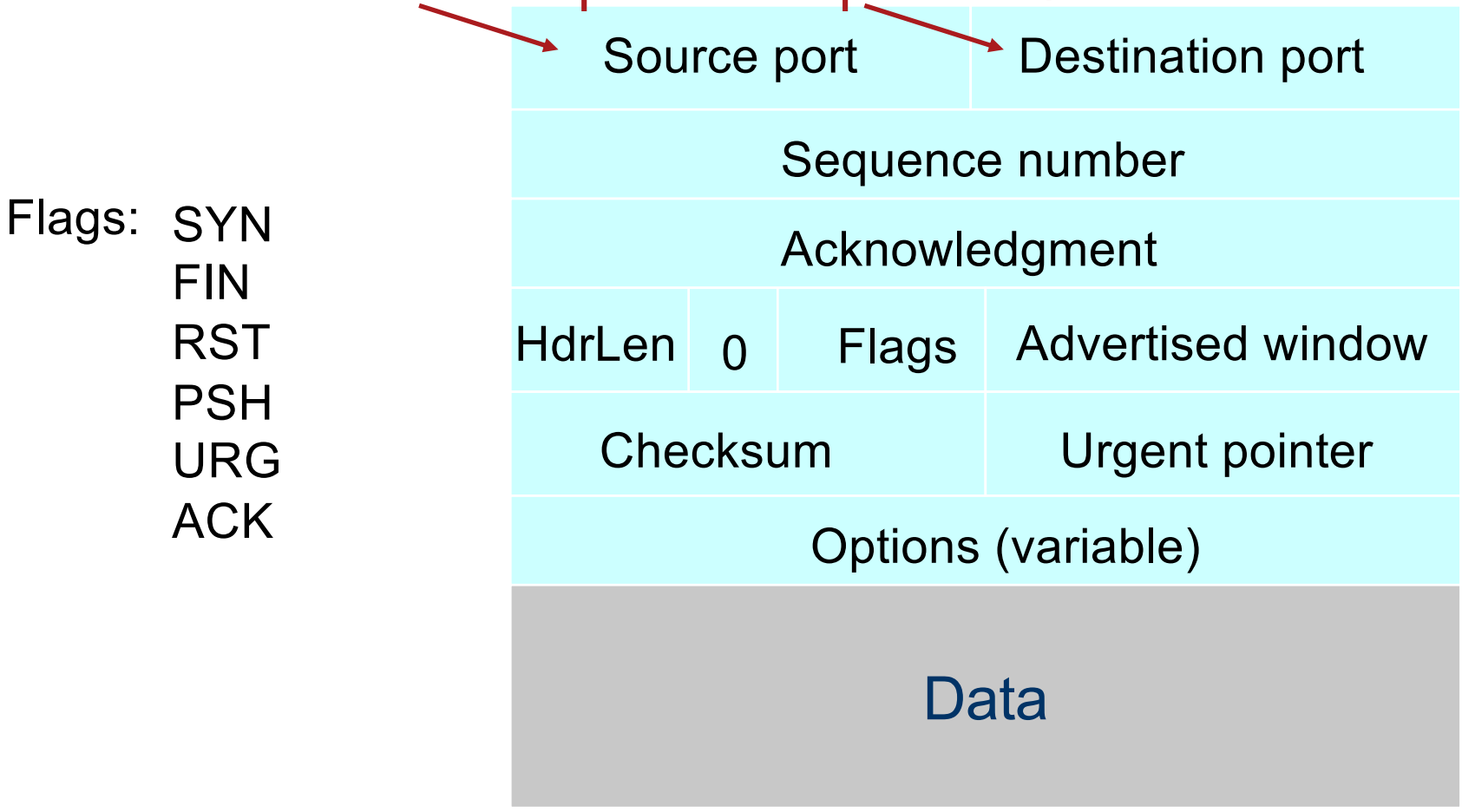
Ties the connection to a particular process/instance



Ex: port 53 typically indicates DNS

TCP Header

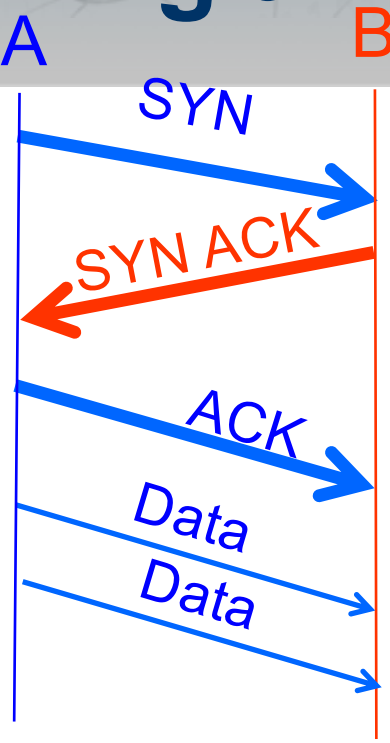
Ties the connection to a particular process/instance



Flags: SYN
FIN
RST
PSH
URG
ACK

Ex: port 80 typically indicates web/http

Establishing a TCP Connection

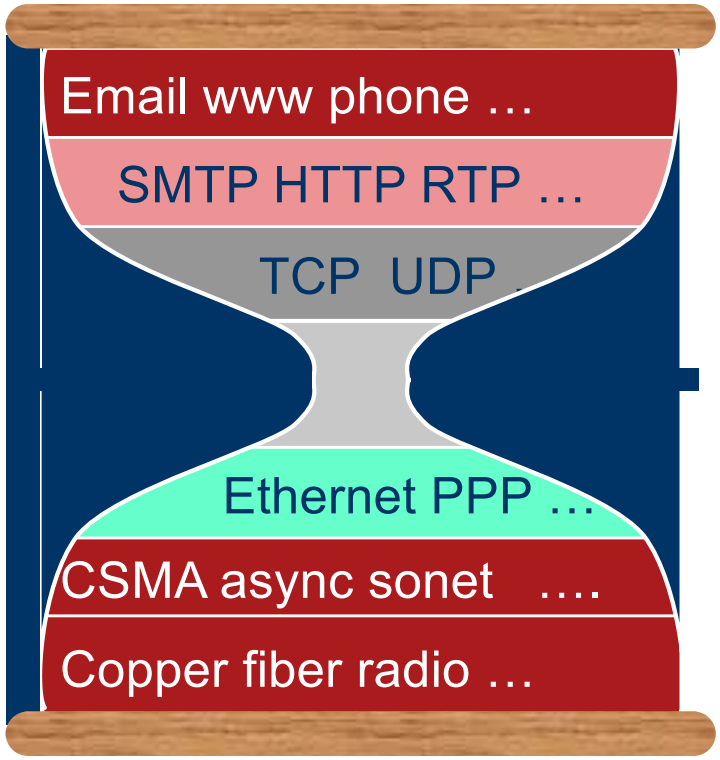


- Three-way handshake to establish connection
  - Host A sends a **SYN** (open) to the host B
  - Host B returns a SYN acknowledgment (**SYN ACK**)
  - Host A sends an **ACK** to acknowledge the SYN ACK

Link, Physical, and Application Layers

- Typically not the focus of general cybersecurity

- Application layer
  - Many standardized protocols (IETF and others)
  - Protocols may be proprietary
- Link and Physical Layers
  - Changes as packet traverses Internet
  - Protocols depend on locations
- Domain experts at the application and link/physical layers can (and do) use these features in cybersecurity.
  - We will focus on Transport and Network Layers



Motivating Example: SNORT Rule

- alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-ATTACKS /bin/ps command attempt"; flow:to_server,established; uricontent:"/bin/ps"; nocase; classtype:web-application-attack; sid:1328; rev:6;)

Network Layer Basics: IP Format and Addressing
Transport Layer Basics: UDP/TCP Header and connections
Application Layer: vast numbers of applications

Heilmeier Questions

- What are you trying to do? Articulate your objectives using absolutely no jargon.
- How is it done today, and what are the limits of current practice?
- What is new in your approach and why do you think it will be successful?
- Who cares? If you succeed, what difference will it make?
- What are the risks?
- How much will it cost?
- How long will it take?
- What are the mid-term and final “exams” to check for success?