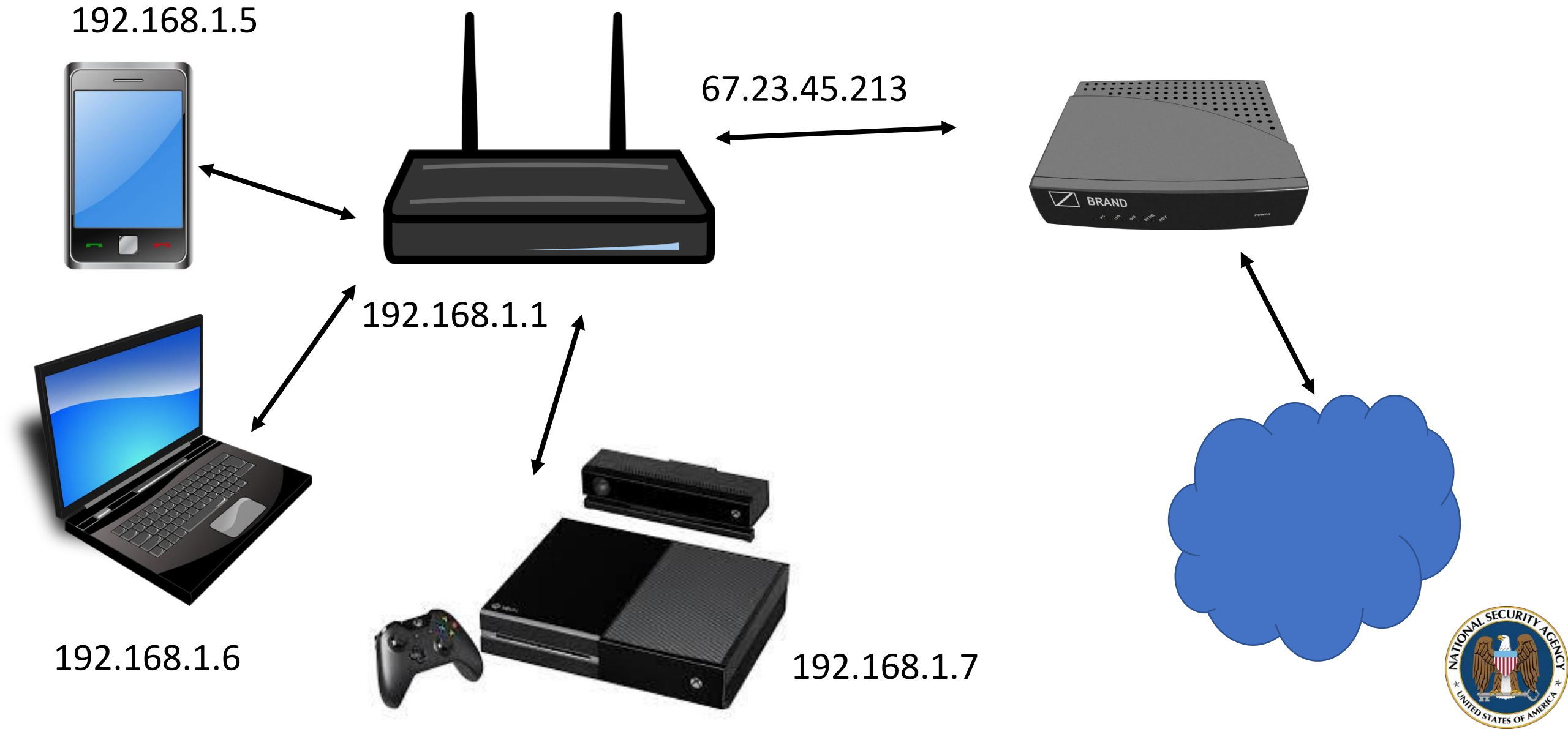
Networking

Week 2, Day 2

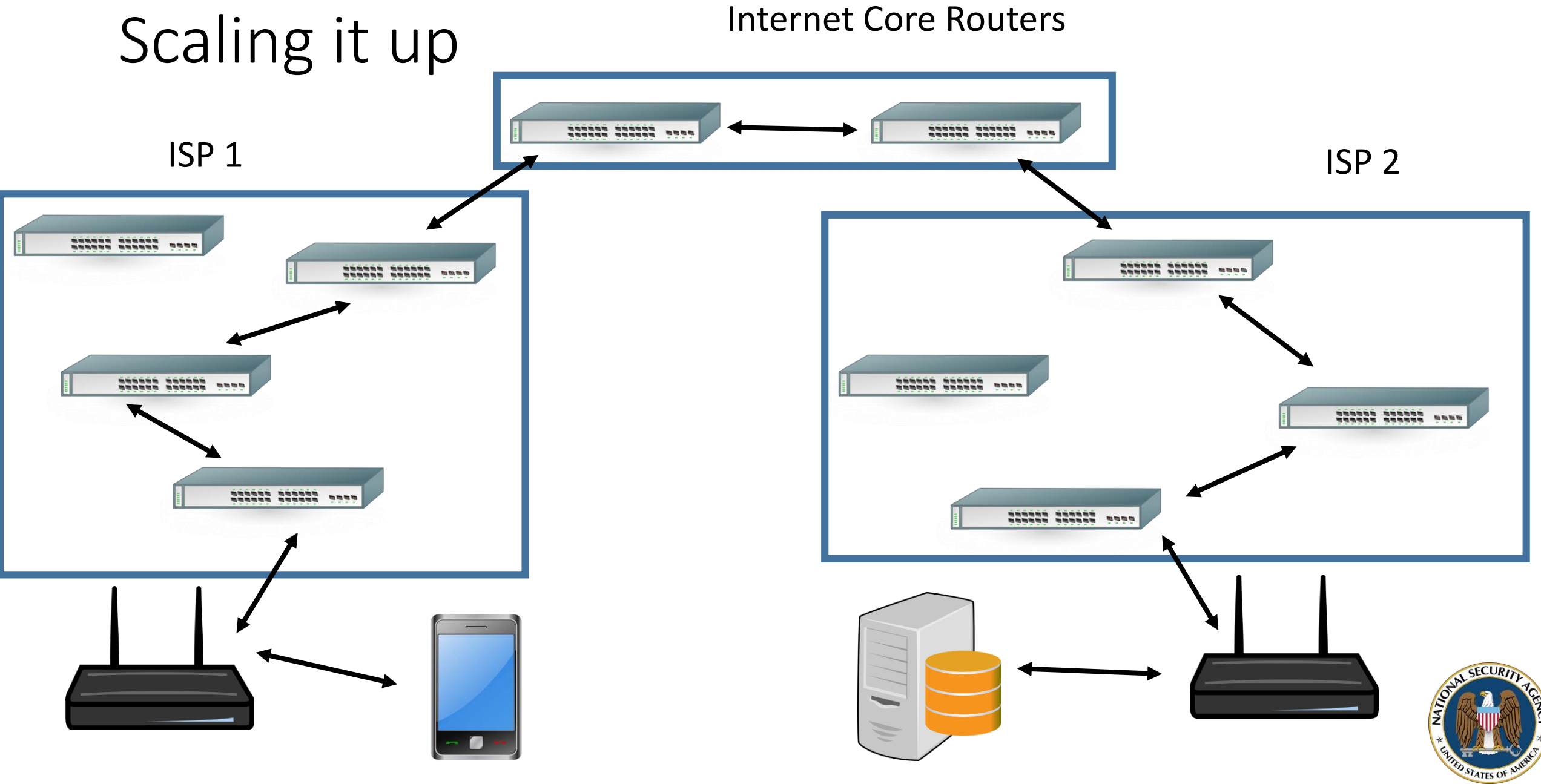
Sub-problem: Getting Message Out of Home



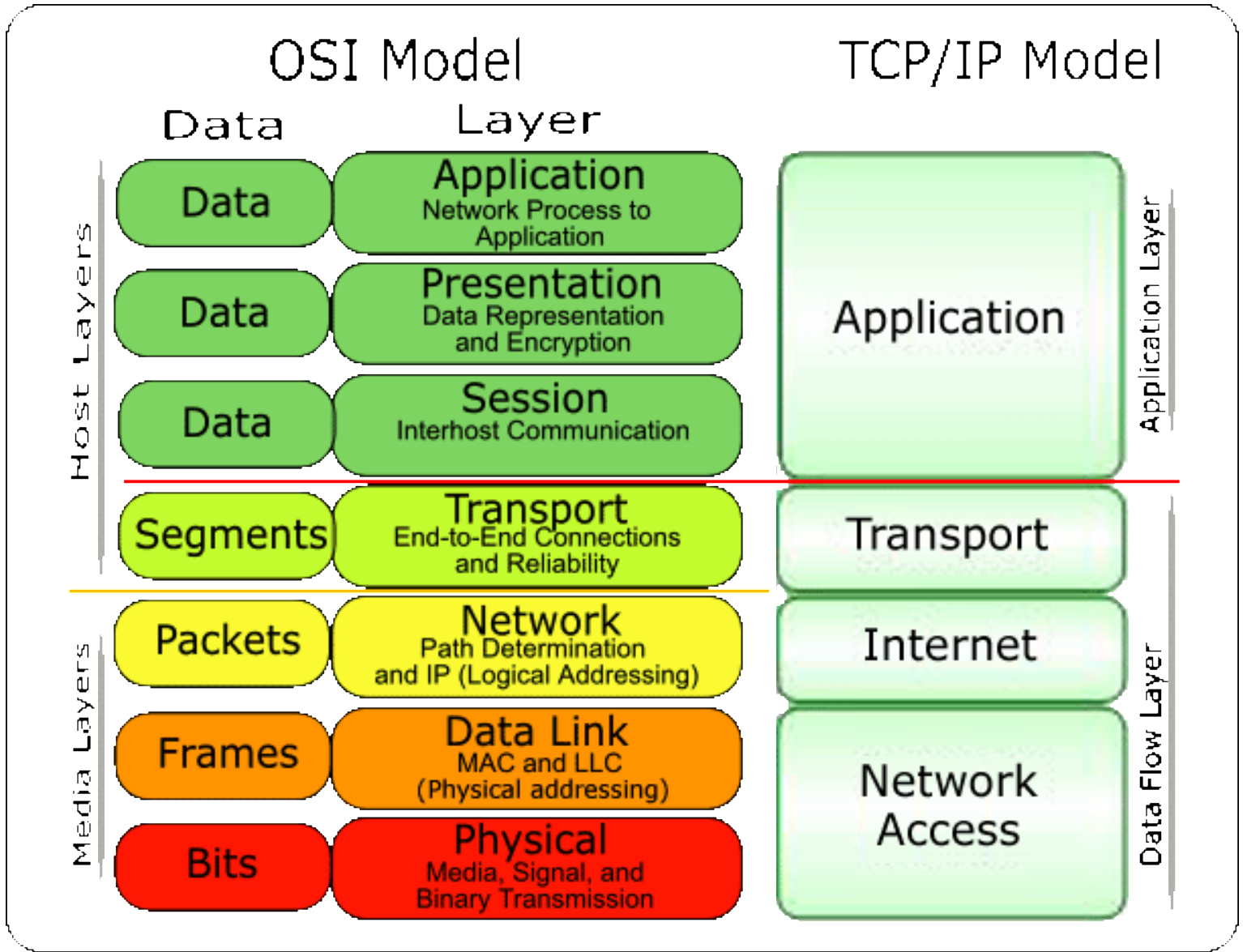
A Note on Addressing

- Physical: MAC Address
  - Hardware-based, burned into the chip
  - Unique (in theory) to each network interface card.
- Logical Addresses
  - IP Address (Internet Layer)
    - Address of a computer on a network
    - Two forms: IPv4 and IPv6
      - IPv4: 192.168.5.1 (4 3-digit numbers between 0 and 255)
      - IPv6: 2001:0db8:0000:0042:0000:8a2e:0370:7334 (8 groups of 4 hexidecimal numbers)
  - Ports (Transport Layer)
    - Address of a program on a computer
    - Value between 0 and 65,535

Scaling it up



OSI & TCP/IP Models



Solution, Part 2: Network Protocols

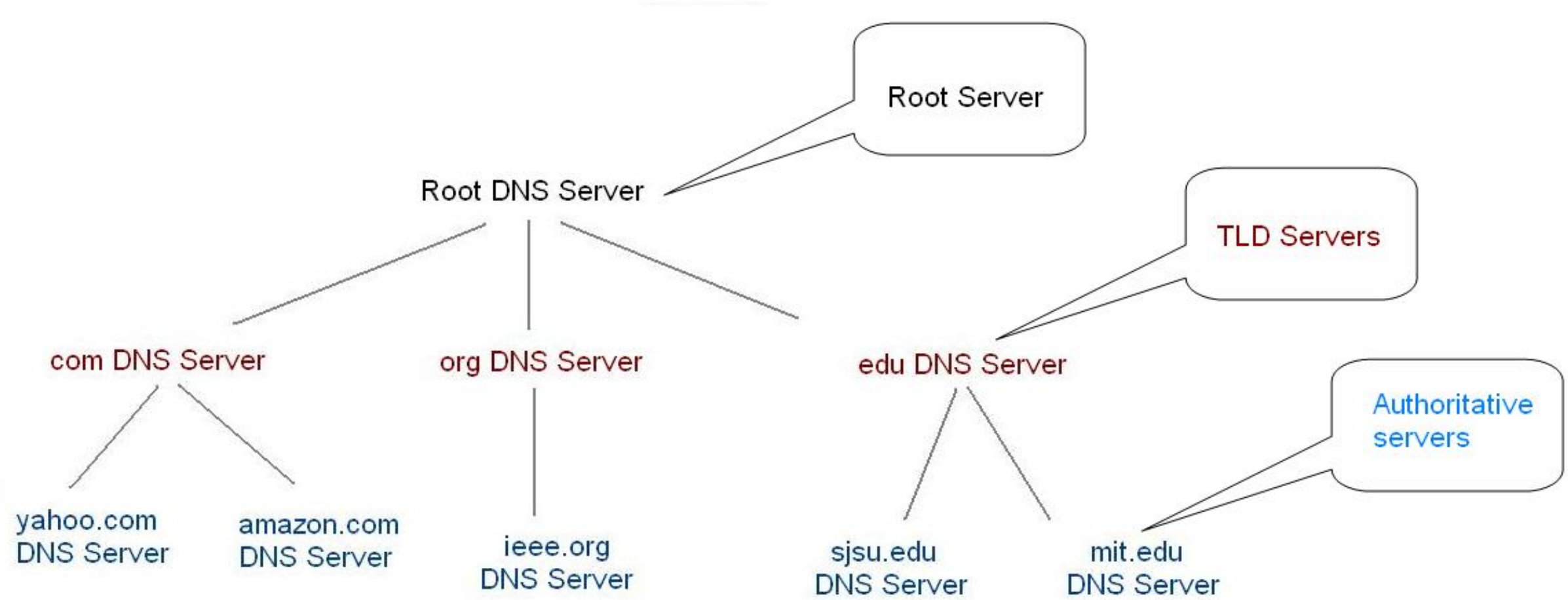
OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

More on Network Protocols

- Network Protocols
  - A standard that is, in theory, universally adhered to in order to facilitate data processing.
  - Specified in formal, public, cooperatively created documents called RFCs
    - Example: Details of HTTP are specified in RFC 2616
- Example:
  - Web browsers issue GET or POST requests for resources
  - Web servers respond with 404 if the resource is not available
  - Web servers respond with 200 if the resource is available and accessible
  - Web servers respond with 401 if the resource is available, but protected
- Things can go badly when protocols are not followed. (Good for red team!)

DNS – Yes, the Internet Really Works This Way



A Partial List of Interesting Protocols

OSI Model		TCP/IP Model
Application Layer	HTTP, FTP, SMTP, DNS, SMS	Application Layer
Presentation Layer	ASCII, GPG	
Session Layer	AppleTalk Session Protocol, NetBIOS	
Transport Layer	TCP, UDP	Transport Layer
Internet Layer	IP, ICMP	Internet Layer
Datalink Layer	ARP, Ethernet	Network Access Layer
Physical Layer	IEEE802	

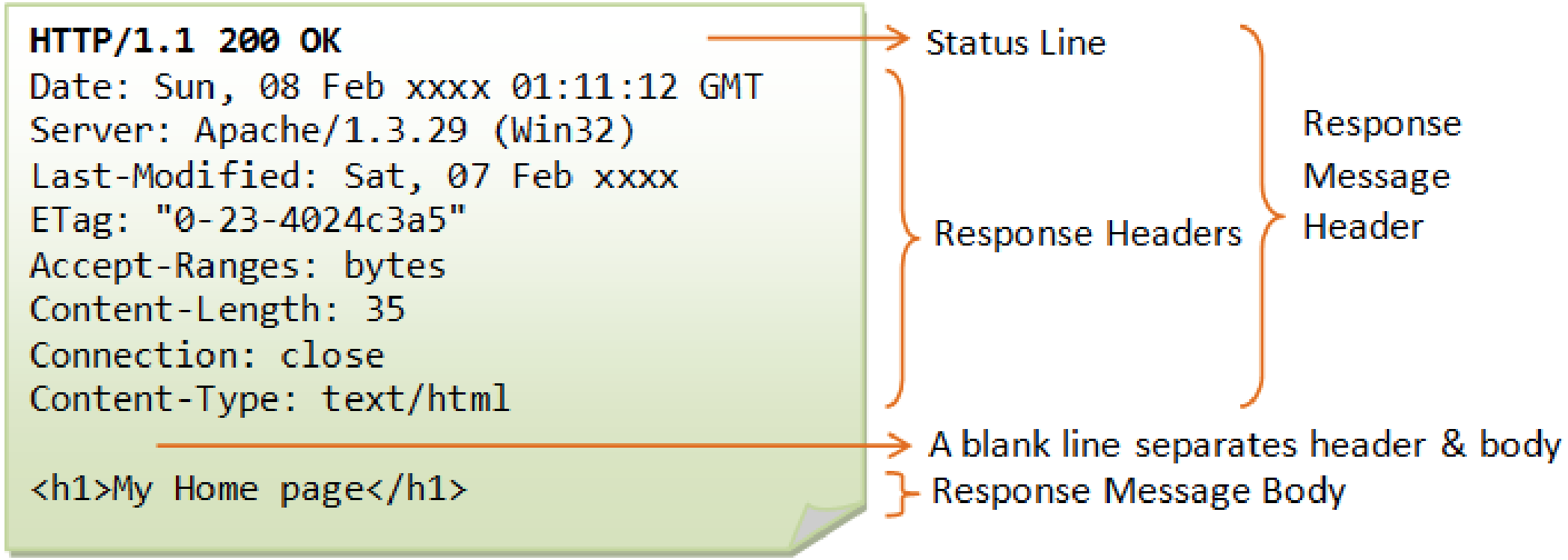
HTTP Request

method **path** **protocol**

```
GET /tutorials/other/top-20-mysql-best-practices/ HTTP/1.1
Host: net.tutsplus.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120
Pragma: no-cache
Cache-Control: no-cache
```

HTTP headers as Name: Value

HTTP Response



HTTP Request in Wireshark

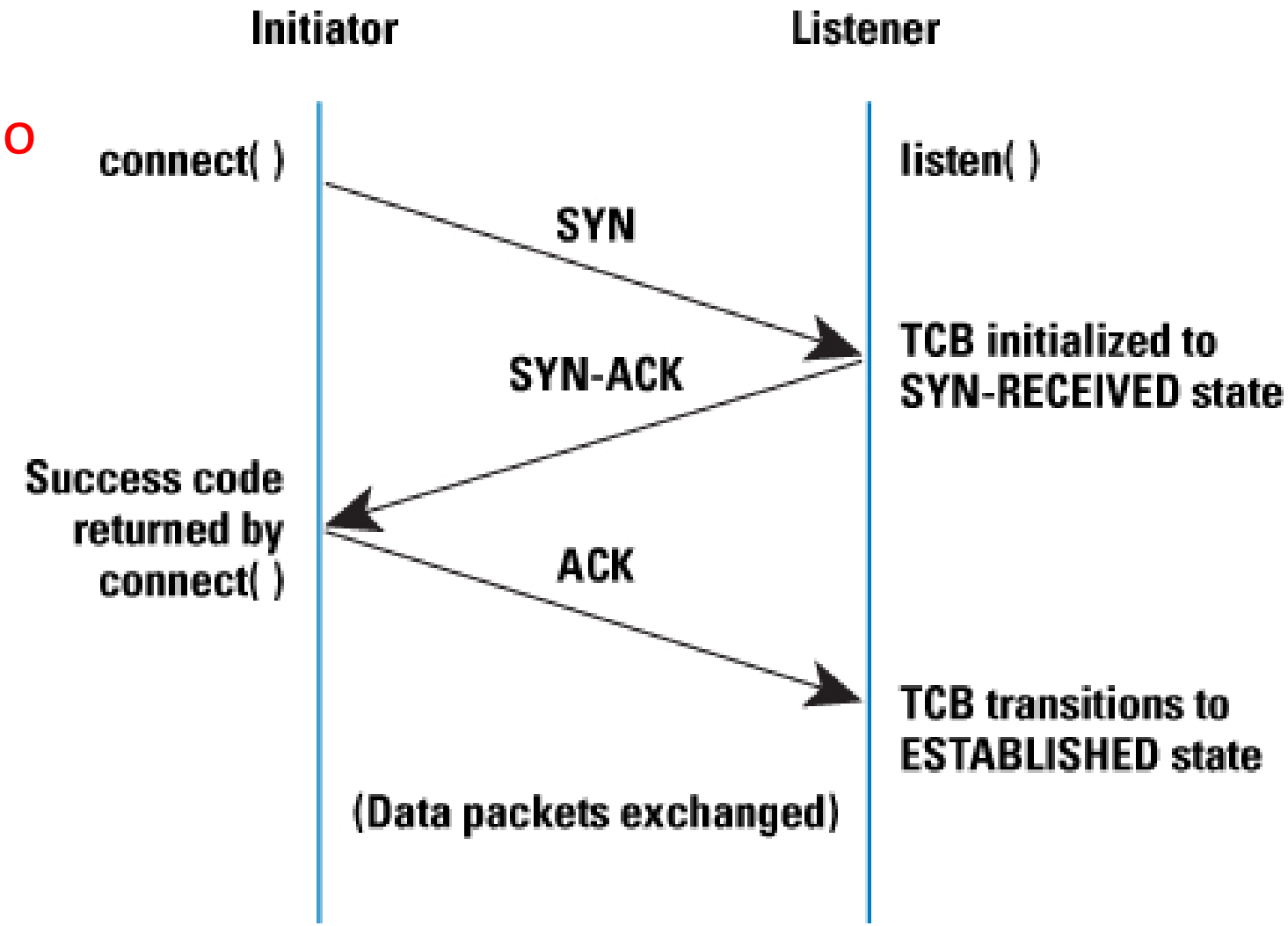
```
⊞ Frame 29: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
⊞ Ethernet II, Src: Vmware_f1:09:fa (00:0c:29:f1:09:fa), Dst: AsustekC_09:ce:ce (90:e6:ba:09:ce:ce)
⊞ Internet Protocol, Src: 192.168.2.102 (192.168.2.102), Dst: 192.168.2.173 (192.168.2.173)
⊞ Transmission Control Protocol, Src Port: sd (9876), Dst Port: 40222 (40222), Seq: 348, Ack: 407,
⊞ [Reassembled TCP Segments (352 bytes): #23(87), #25(100), #27(160), #29(5)]
⊞ Hypertext Transfer Protocol
⊟ eXtensible Markup Language
  ⊞ <?xml
  ⊟ <S:Envelope
      xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
    ⊟ <S:Body>
      ⊟ <ns2:getTimeAsStringResponse
          xmlns:ns2="http://ts.ch01/">
        ⊟ <return>
            Fri Sep 10 16:00:01 BRT 2010
            </return>
          </ns2:getTimeAsStringResponse>
      </S:Body>
    </S:Envelope>
```

Transmission Control Protocol (TCP)

- Transport-layer Network Protocol
  - Ensures reliable communication across a network
  - Takes data from session layer and breaks it up into segments
  - Segments passed to the Internet layer to be encapsulates as packets that can be transmitted across a network
- Segments….
  - Have one or more of six possible flags set
    - SYN, ACK, FIN, RST, URG, PSH
  - Has a sequence number, for ordering segments
  - Has a checksum, for ordering
- TCP is a connection-based protocol
  - Connections are formally created and terminated

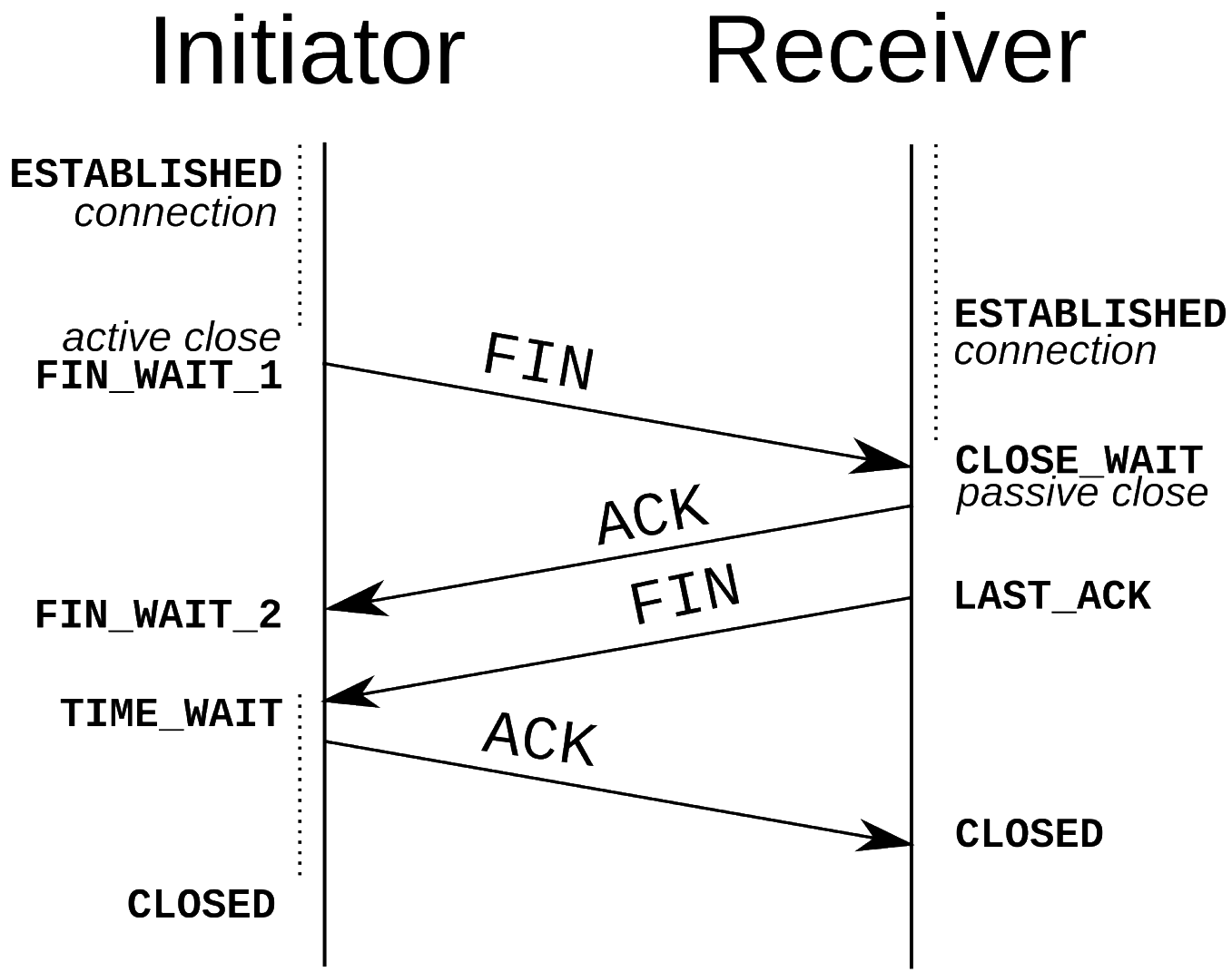
TCP: 3-way Handshake

Requires an IP/port combo

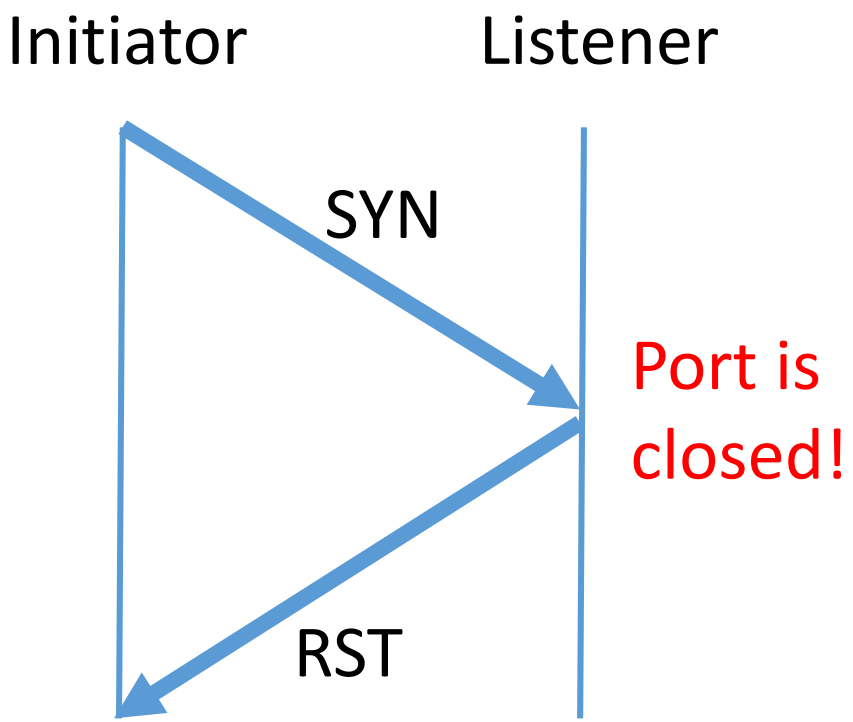


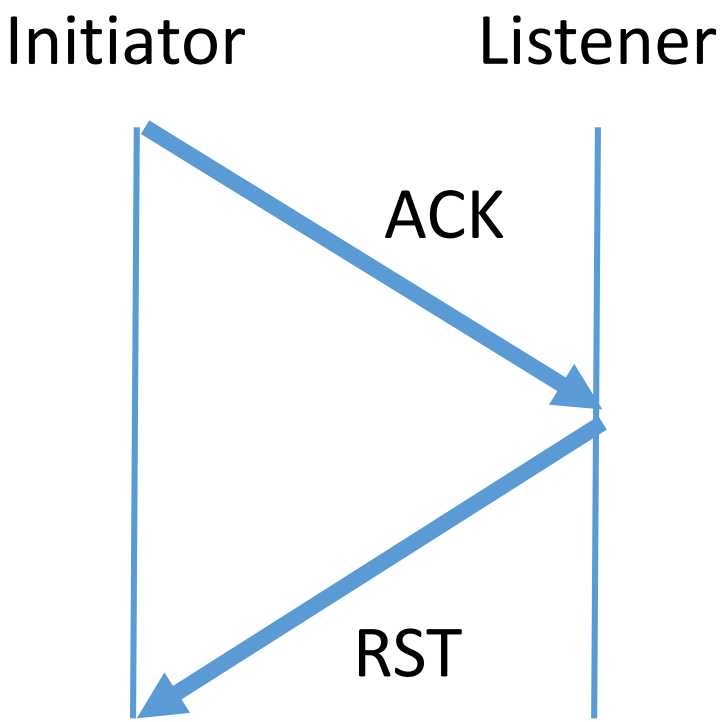
Sends SYN/ACK if the port is open and accepting connections

TCP 4-Way Shutdown [My term]

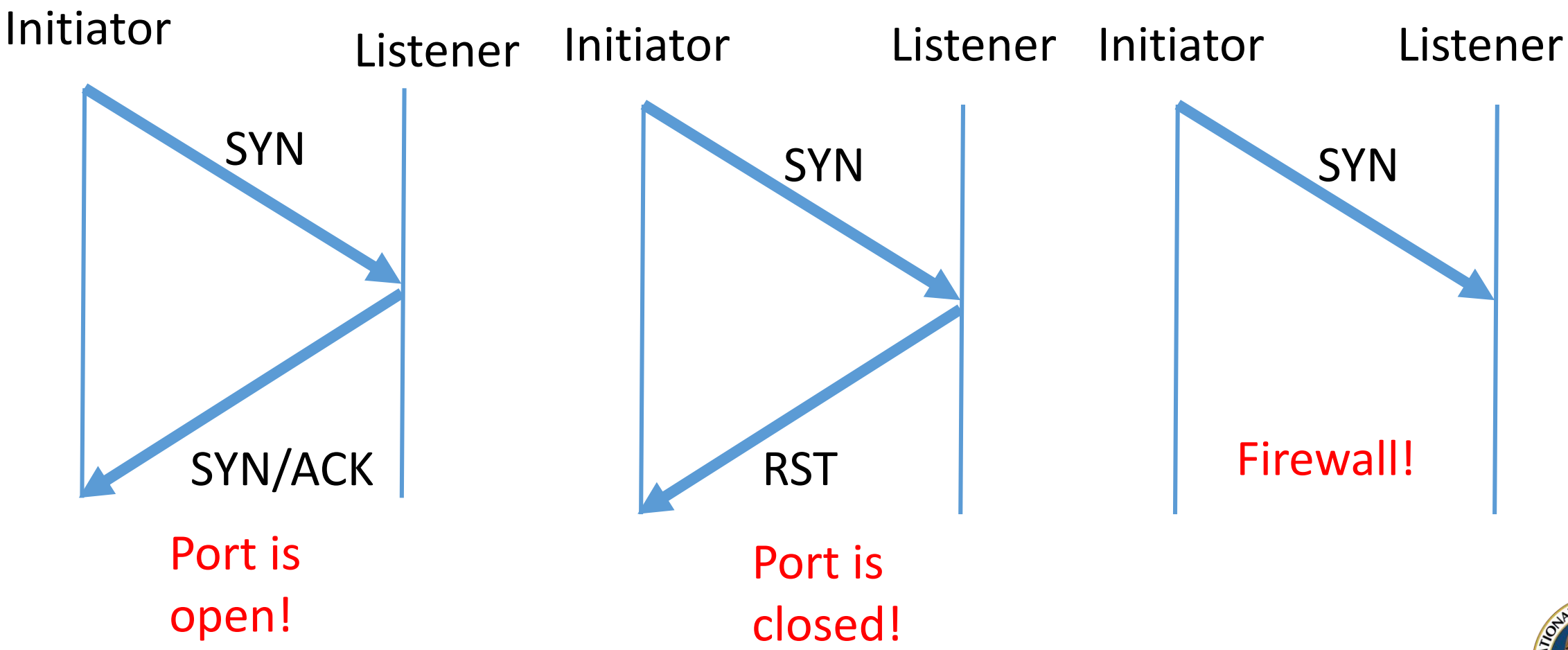


The RST Flag

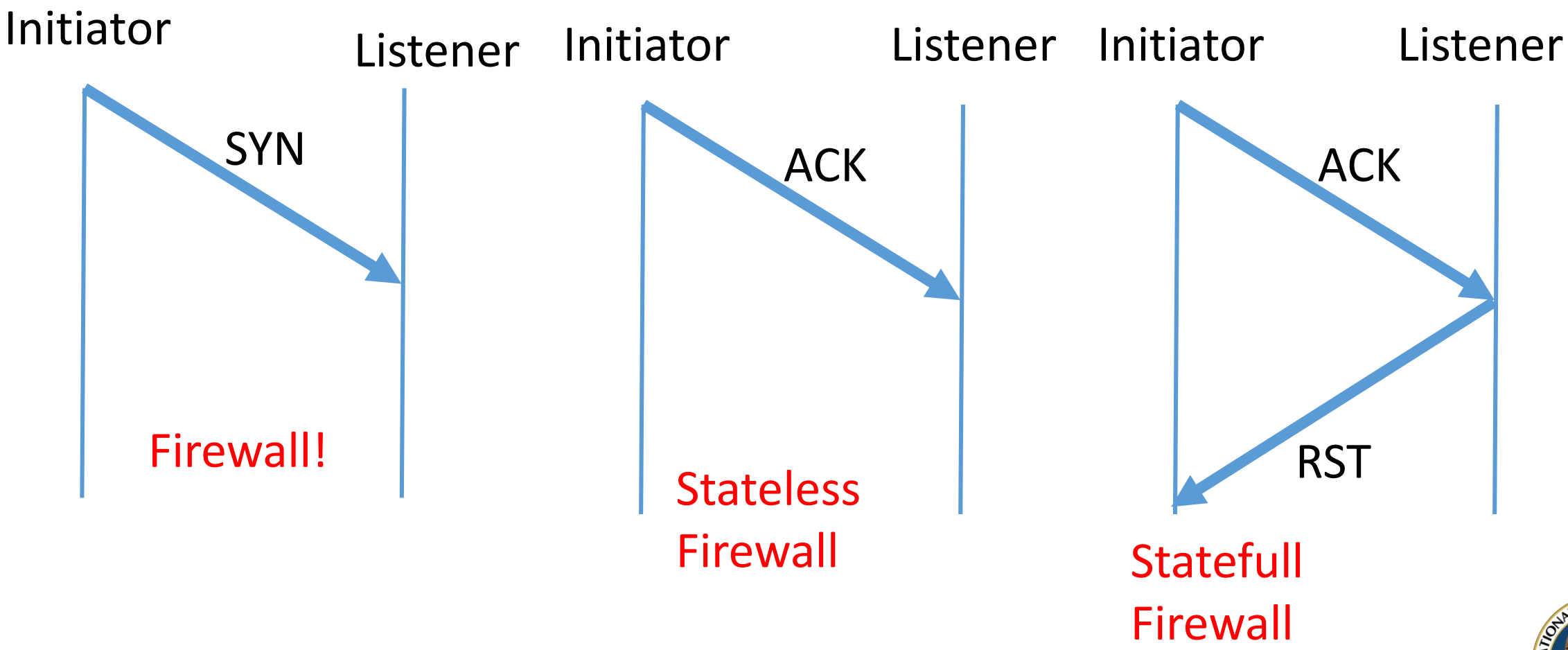

Initiator
Listener
SYN
RST
Port is closed!


Initiator
Listener
ACK
RST

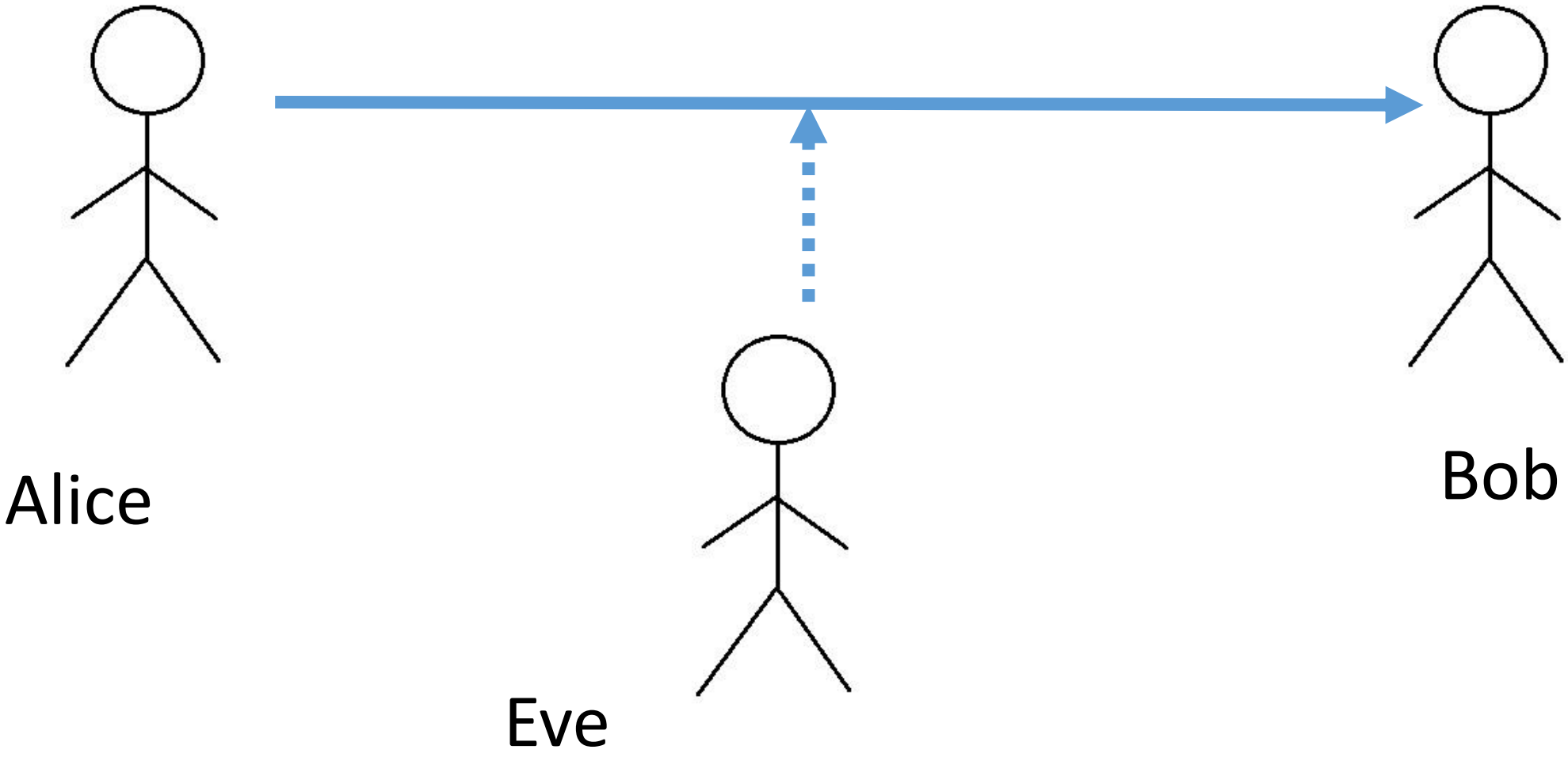
Breaking Protocol: Port-Scanning



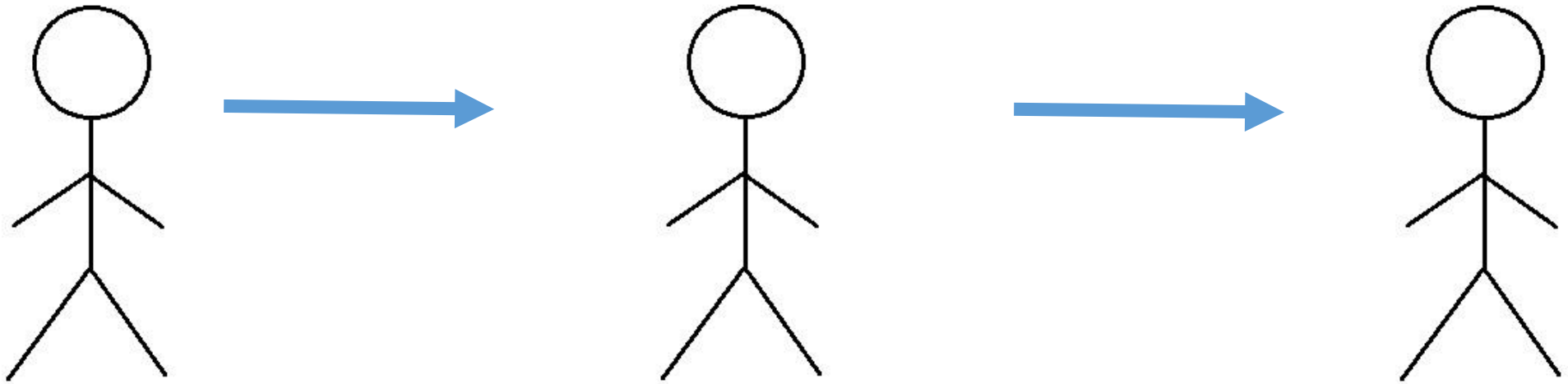
Breaking Protocol: Advanced Port-Scanning



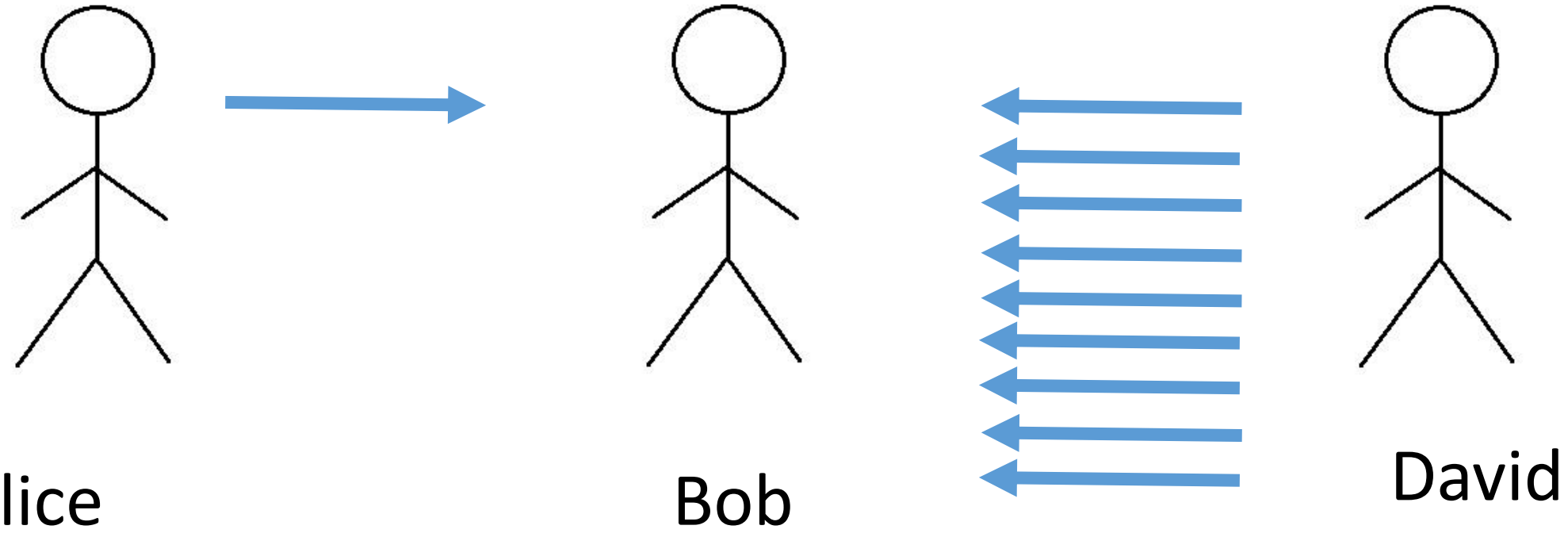
Network-based Attacks: Man on the Side (MotS)



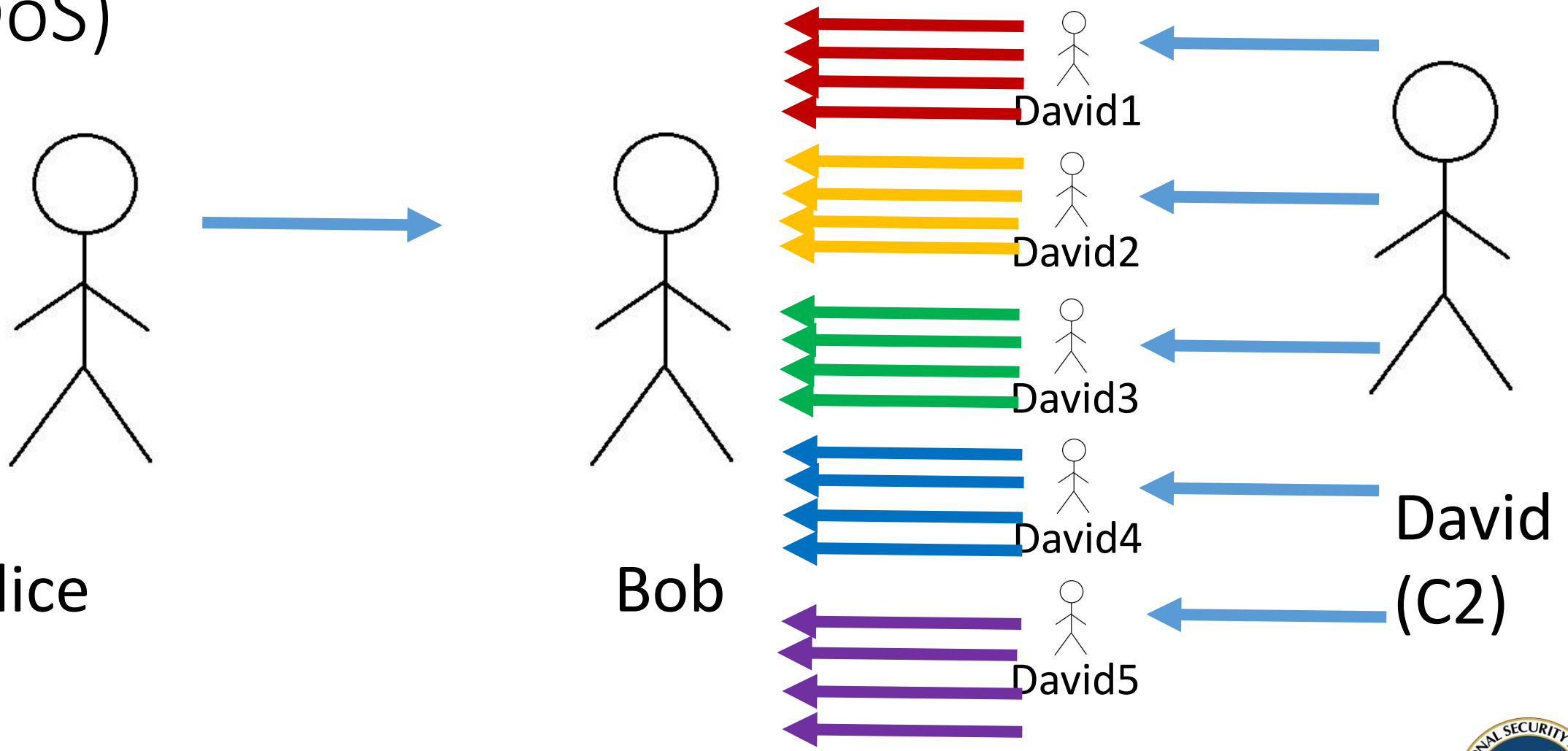
Network-based Attacks: Man in the Middle (MitM)



Network-based Attacks: Denial of Service (DoS)



Network-based Attacks: Distributed DoS (DDoS)



Summary

- The OSI and TCP/IP models provide layers of abstraction so that those working on networks – such as developers writing software – only have to worry about their part of the problem.
- Network protocols are defined in RFCs documents to which everyone implementing the protocol adheres.
- Network protocols exist at each layer of the OSI and TCP/IP models. Protocol data from each layer is wrapped in protocol data from layers below it.
- Many network protocols don’t consider security and we can discover information from systems by breaking the RFC rules.