CS 114: Network Security

Lecture 11 - TCP/IP Security

Prof. Daniel Votipka
Spring 2023

(some slides courtesy of Prof. Daniel Votipka)

Tufts UNIVERSITY

Administrivia

- Exam 1 has been graded and is available
- Homework 1, part 2 due next Tuesday at 11:59pm
  - Assume length is 4-byte unsigned integer

$$
\begin{aligned}
&iv\ + \\
&E_{k1}(len(m))\ + \\
&\text{HMAC}_{k2}(iv + E_{k1}(len(m)))\ + \\
&E_{k1}(m)\ + \\
&\text{HMAC}_{k2}(E_{k1}(m))
\end{aligned}
$$

Fixed length

Exam review

Exam 1

- Average: 66.1 (~88%)
- Pick up your exam after class or in office hours

1. True/False

T The numbers 2 and 6 are modular inverses of each other in $\mathbb{Z}_{11}$. (Hint: $\mathbb{Z}_n$ is the integers in the range $[0, n-1]$.)

2*6 mod 11 = 12 mod 11 = 1

2. That whole network thing

For each of the following descriptions, indicate which layer (by number) best matches the description. No partial credit will be given, and no justifications are necessary. Please write legibly – if I cannot identify the number you wrote, I will mark the answer as incorrect.

1. _____ This layer is used to communicate between two machines on the same local network.

Data Link

3. Symmetric Key Crypto

{5 points} Briefly explain why it is important that an encryption system not be vulnerable to a known-plaintext attack. Alternatively: why is it necessary for a practical encryption system to resist known-plaintext attacks?

Known-plaintext attack is an attack that is successful if you know some plaintext used to generate a ciphertext

3. Symmetric Key Crypto

{6 points} Suppose $S(k)$ is a cryptographically strong stream generator that is suitable for use in a stream cipher. Fill in the protocol description below that allows Alice to send Bob a message m of n-bits, i.e., $m = b_0, b_1, \ldots, b_{n-1}$ such that (1) only Alice or Bob can decrypt the message and (2) the transmission of multiple messages does not lead to a *key reuse attack* in which an eavesdropper is able to remove the effects of using the stream generator.

$$A \rightarrow B : \text{IV}, \sum_{i=0:n-1} b_i \oplus S(k \oplus \text{IV})$$

You can assume that Alice and Bob have pre-shared a symmetric key k and that Eve does not know k.

5. RSA

{4 points} Alice's public RSA key is $\langle e = 3, n = 55\rangle$ and her corresponding private key is $\langle d = 27, n = 55\rangle$. Bob's public RSA key is $\langle e = 7, n = 33\rangle$ and his corresponding private key is $\langle d = 3, n = 33\rangle$.

Suppose Alice wants to send Bob an encrypted message, $m = 9$, along with a digital signature of that message. Fill in what she needs to send to Bob using a *encrypt-then-MAC* scheme (that is, encrypt m and then compute the signature over the encrypted version of m). You can leave your answer is unsimplified form.

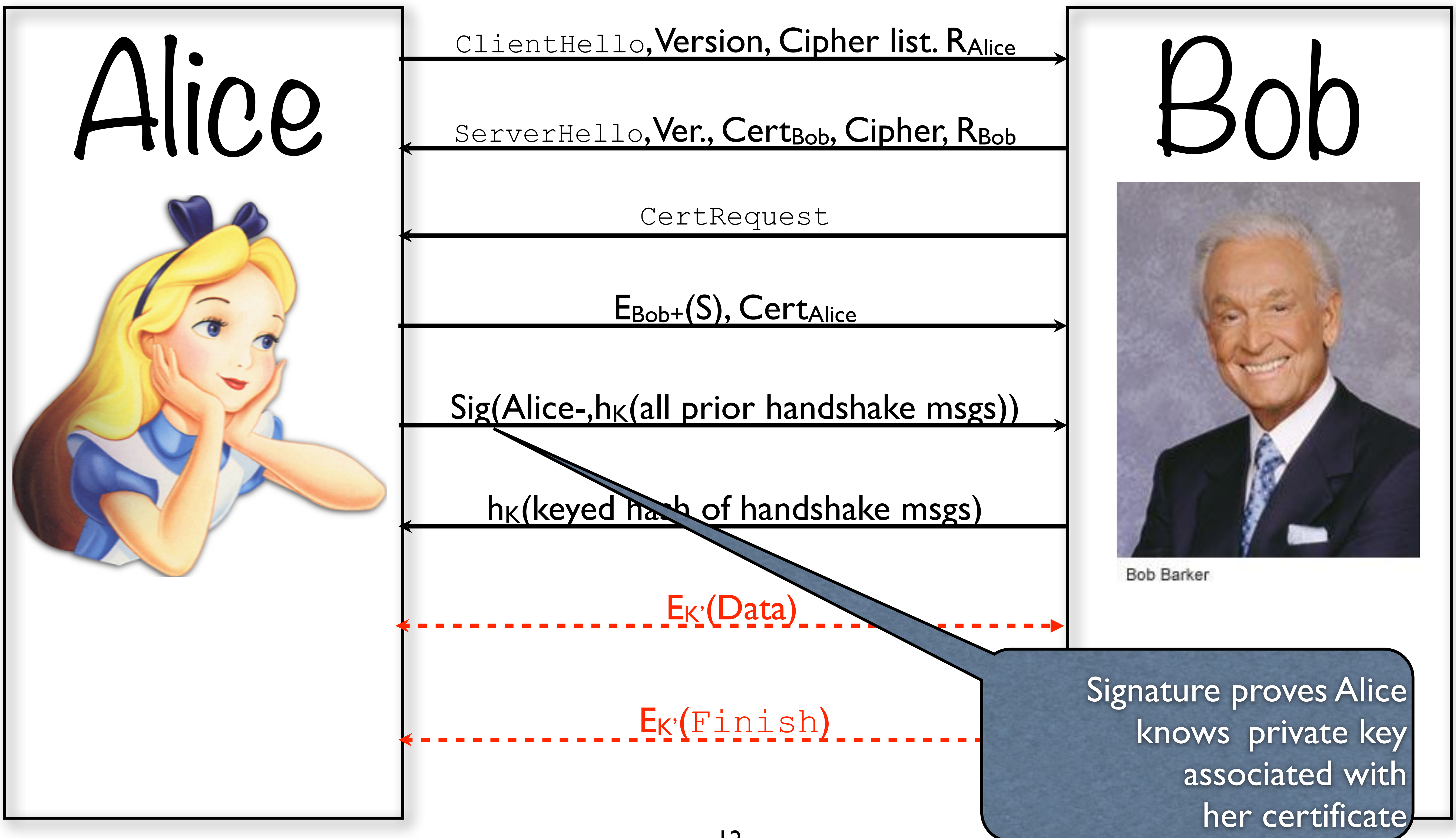
$A \rightarrow B$: $9^7 \bmod 33, (9^7 \bmod 33)^{27} \bmod 55$

Exam 1

- Average: 66.1 (~88%)
- Pick up your exam after class or in office hours
- +2 curve

SSL/TLS review

SSL/TLS with
Server and Client Authentication



Session Resumption

Alice

Bob

session-id, Cipher list, R_{Alice} →

← session-id, cipher, R_{Bob}

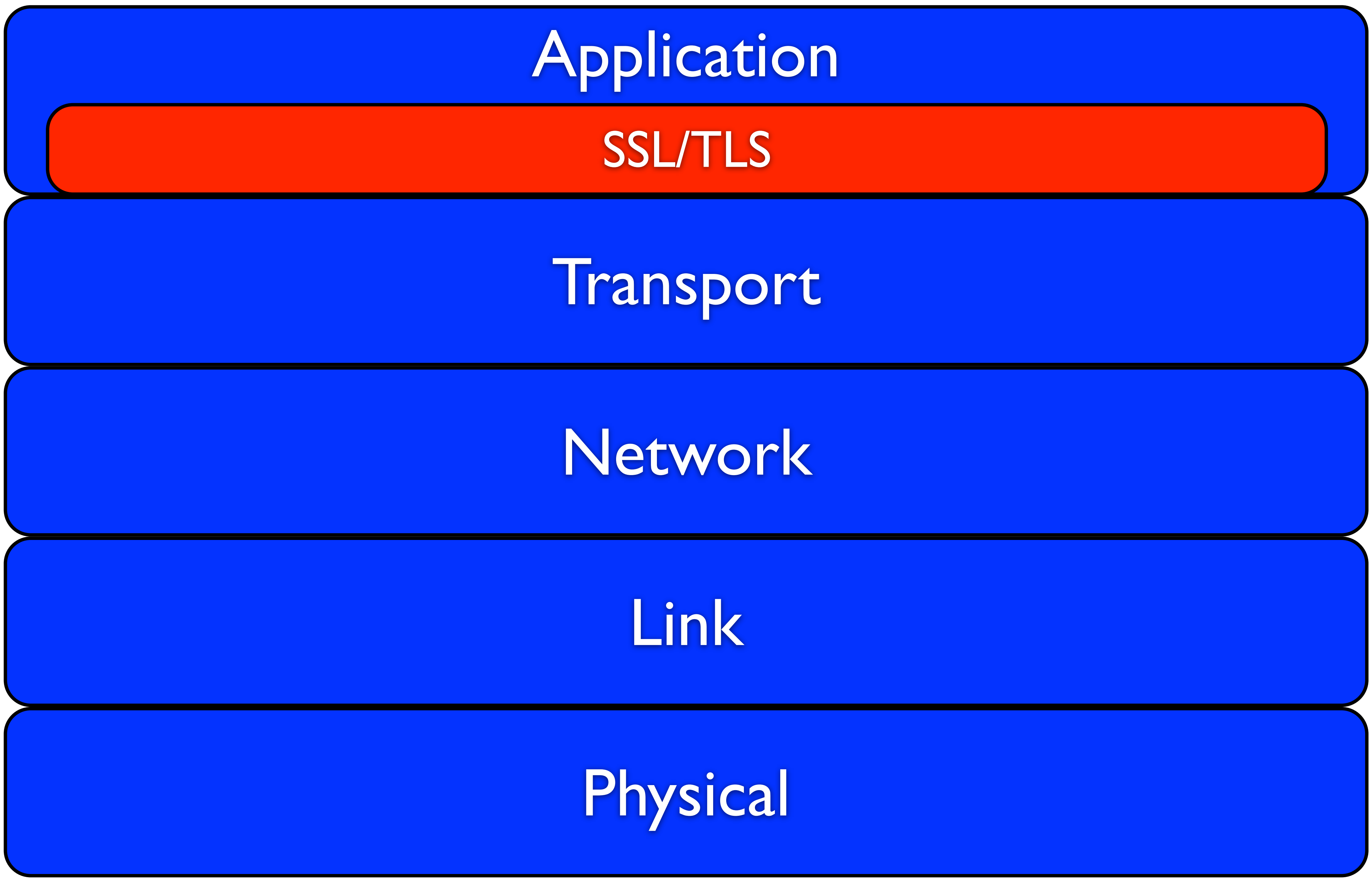
← h_K(keyed hash of handshake msgs)

h_K(keyed hash of handshake msgs) →

← $E_{K'}$(Data)

Alice and Bob compute new **master secret k** as $K' = h(S, R_{Alice}, R_{Bob})$

Network Stack, revisited



TCP/IP Security

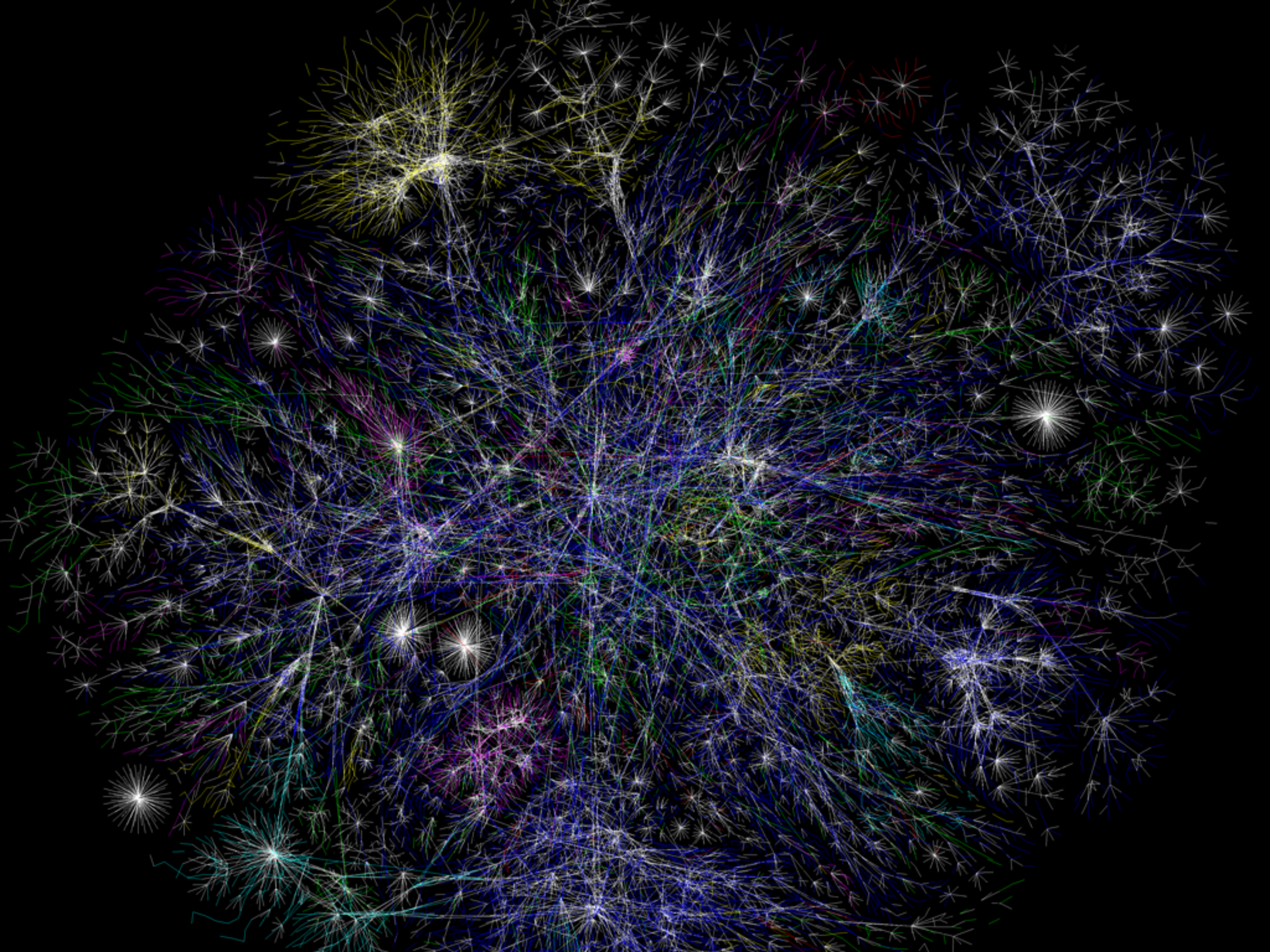
Networking

- Fundamentally about transmitting information between two devices
- Communication is now possible between any two devices anywhere (just about)
  - Lots of abstraction involved (see previous slide)
  - Lots of network components (routers)
  - Standard protocols (e.g., IP, TCP, UDP)
  - Wired and wireless
- What about ensuring *security*?

Network Security

- Every machine is connected
  - No barrier to entry
  - Not just limited to dogs as users

"On the Internet, nobody knows you're a dog."



Exploiting the network

- The Internet is extremely vulnerable to attack
  - it is a huge open system ...
  - which adheres to the end-to-end principle
    - smart end-points, dumb network
- Can you think of any large-scale attacks that would be enabled by this setup?

Network Security: The high bits

- The network is …
  - … a collection of interconnected computers
  - … with resources that must be protected
  - … from unwanted inspection or modification
  - … while maintaining adequate quality of service.

Network Security: The high bits

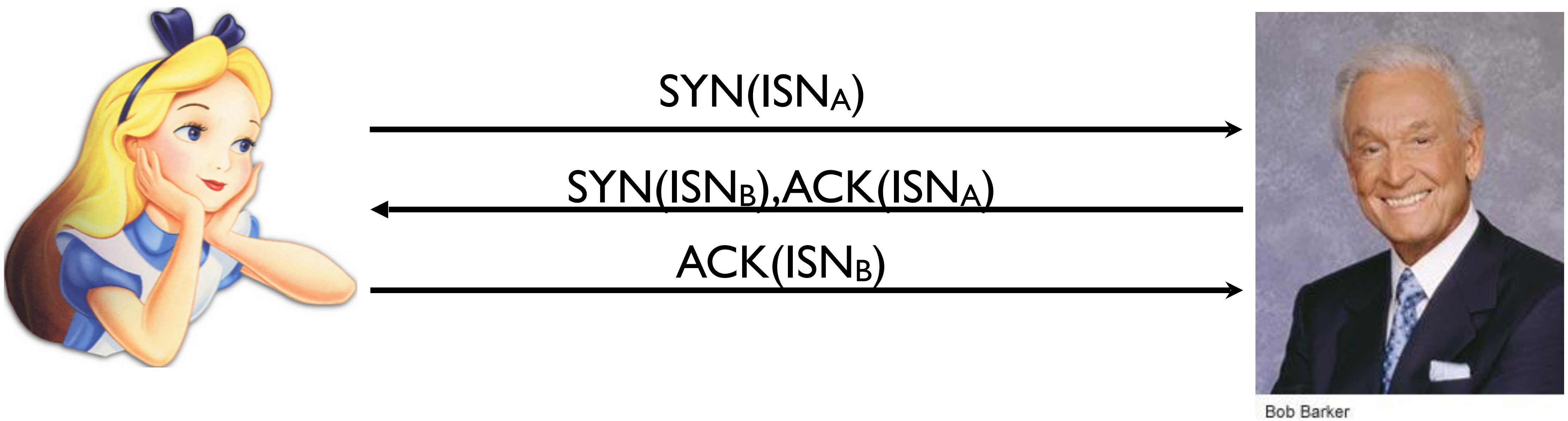
- Network Security (one of many possible definitions):
  - Securing the network infrastructure such that the integrity, confidentiality, and availability of the resources is maintained.

Steven Bellovin's Security Problems in the TCP/IP Protocol Suite

- Bellovin's observations about security problems in IP
    - Not really a study of how IP is misused (e.g., IP addresses for authentication), but rather what is inherently bad about the way in which IP is set up
- A really, really nice overview of the basic ways in which security and the IP design is at odds

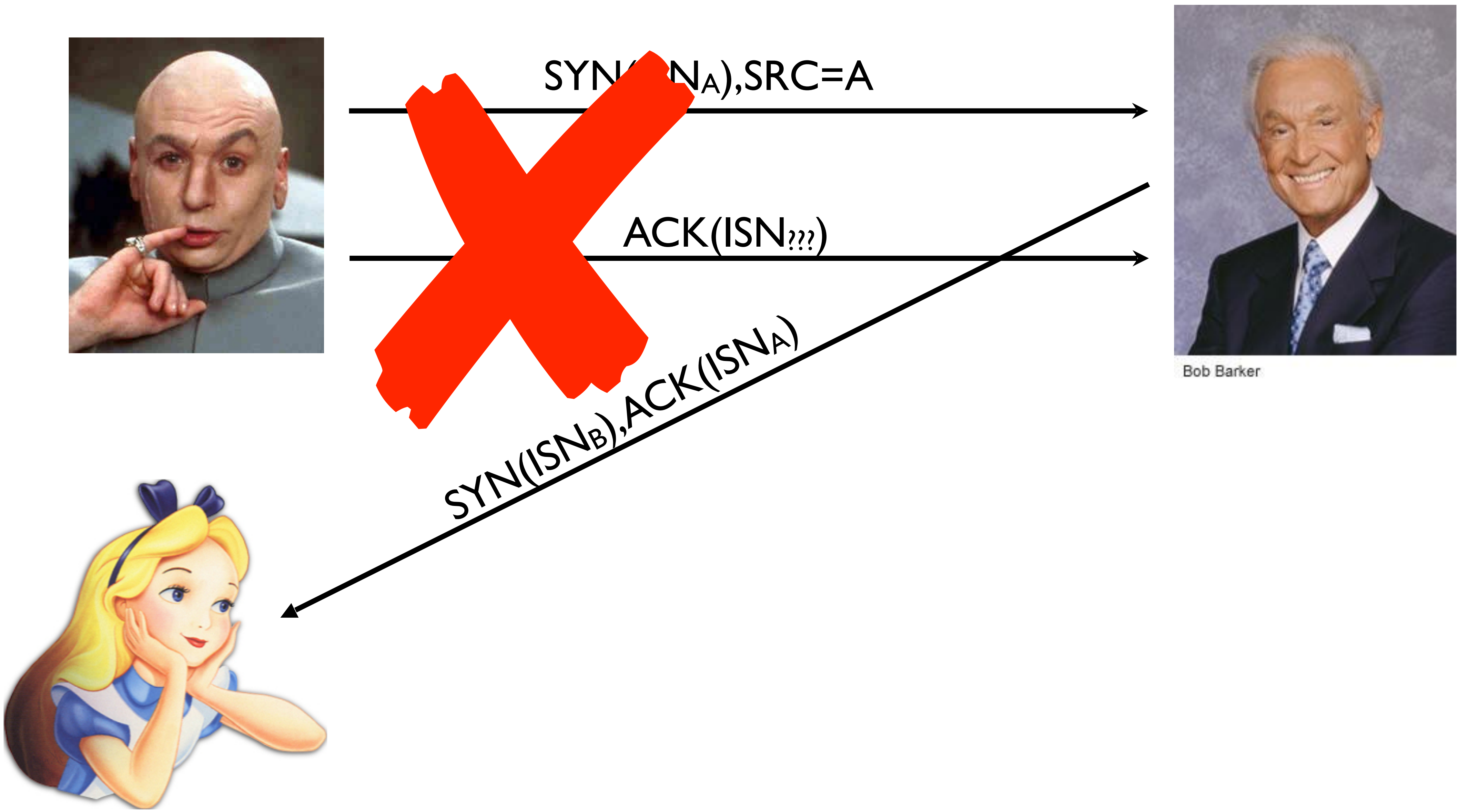
TCP sequence numbers

TCP Sequence Numbers

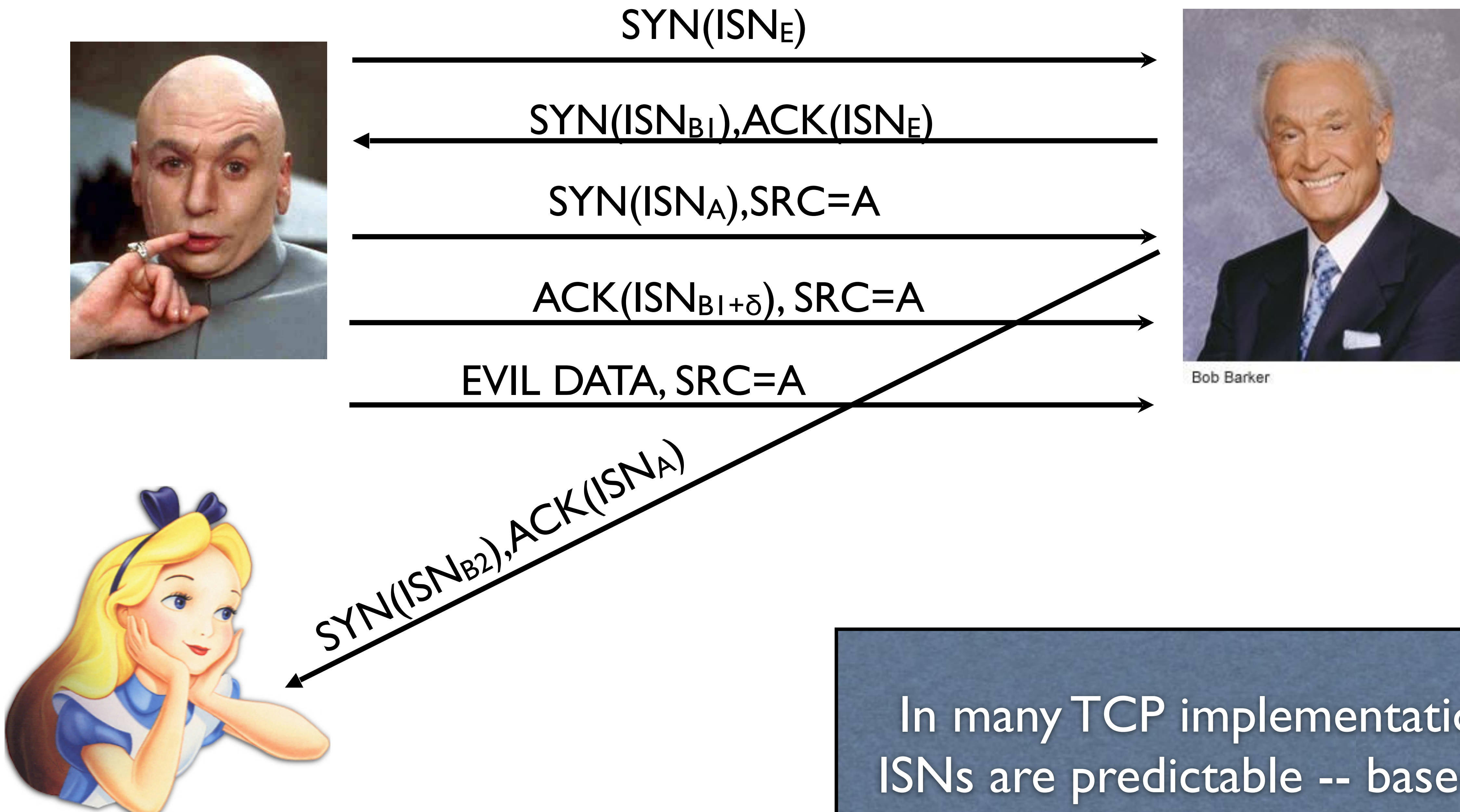


- TCP's "three-way handshake":
  - each party selects Initial Sequence Number (ISN)
  - shows both parties are capable of receiving data
  - offers some protection against forgery -- **WHY?**

TCP Sequence Numbers



TCP Sequence Numbers



In many TCP implementations, ISNs are predictable -- based on time (e.g,. ++ each 1/128 sec)

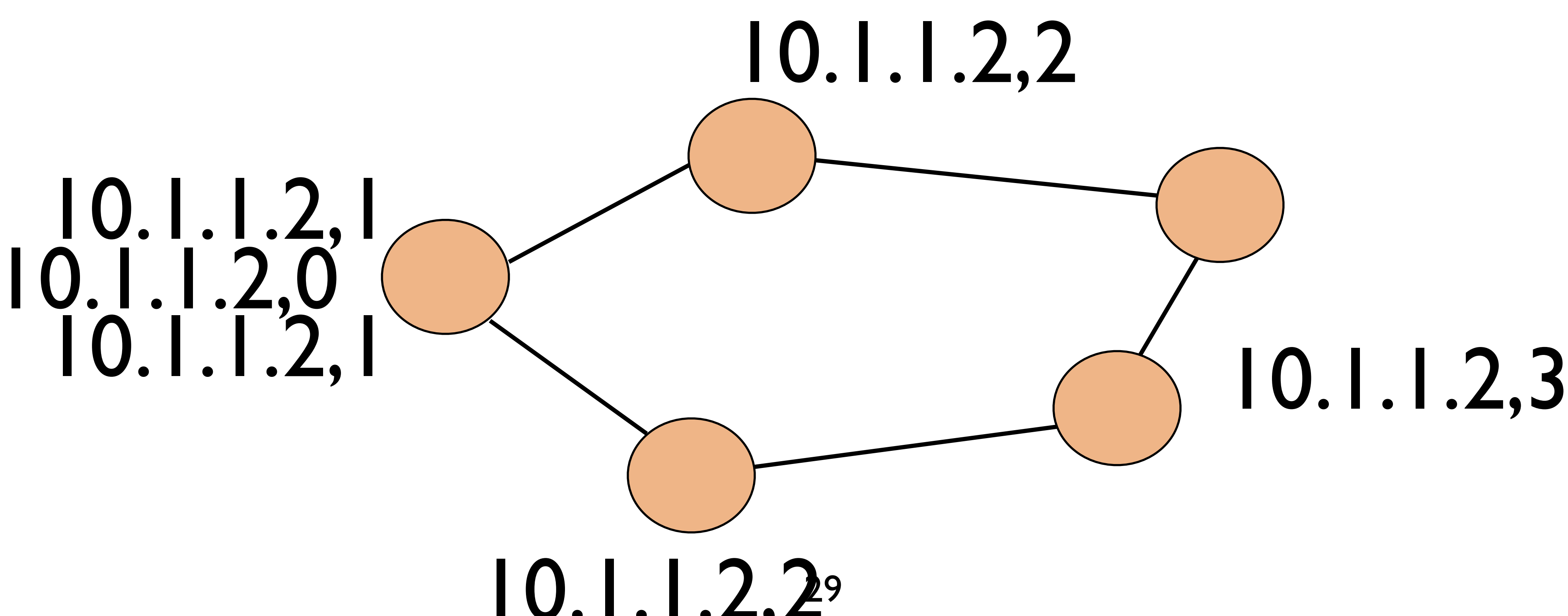
How do we fix this?

- More rapidly change ISNs
- Randomize ISNs

Routing security

Routing Manipulation

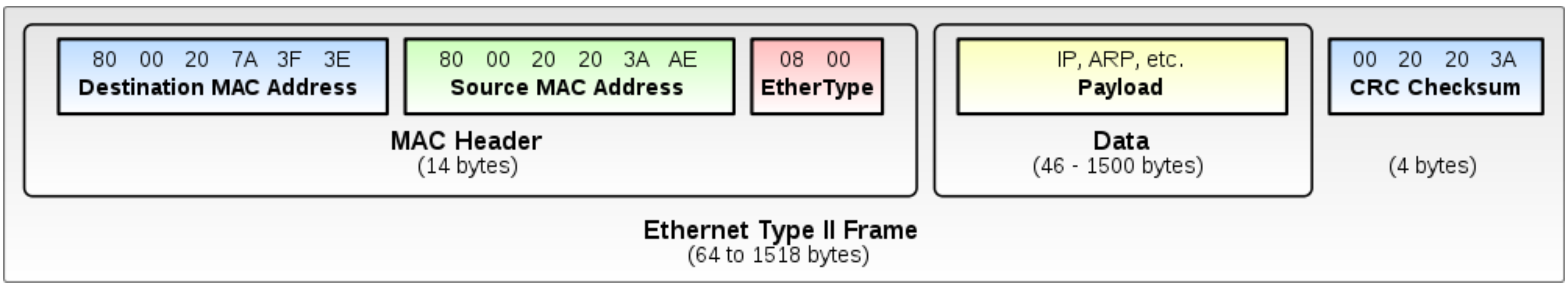
- RIP - Routing Information Protocol
  - Distance vector routing protocol used for the local network
  - Routers exchange reachability and "distance" vectors for all the sub-networks within (a typically small) domain
  - Use vectors to decide which route is best



Routing Manipulation

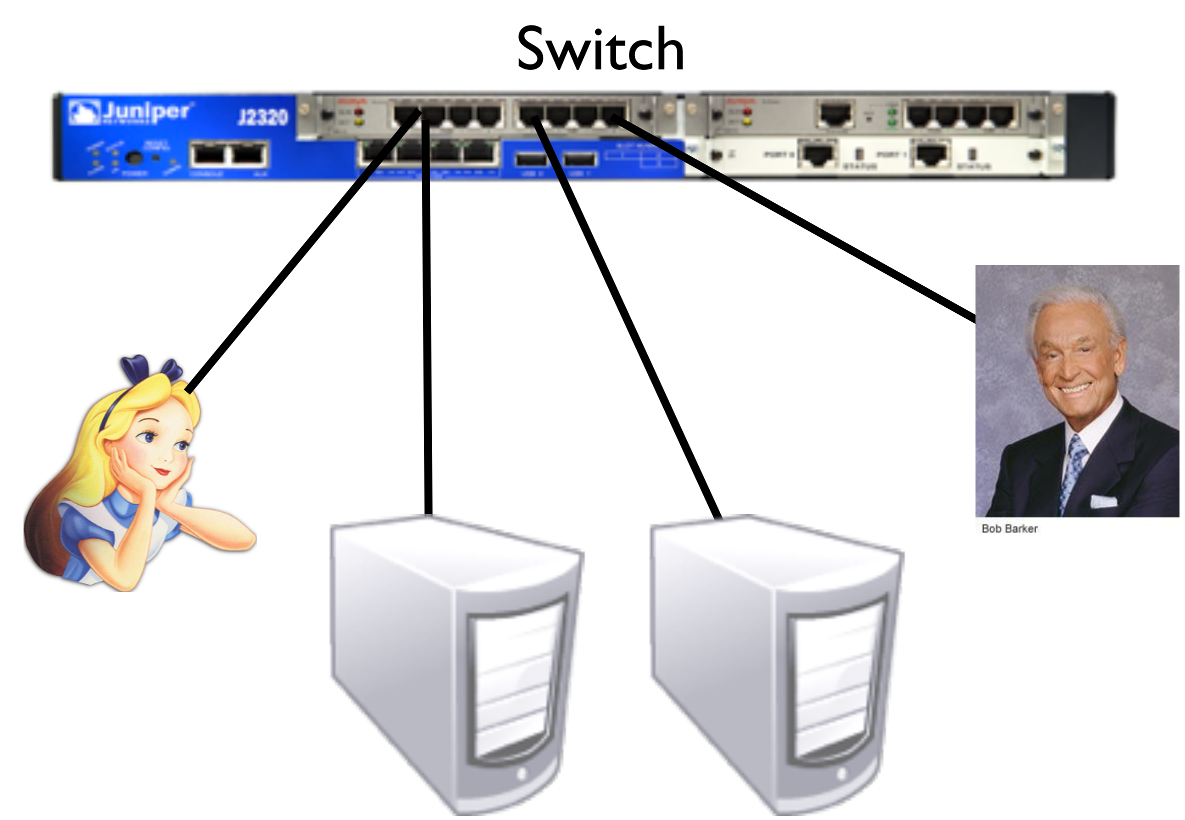
- RIP - Routing Information Protocol
  - Distance vector routing protocol used for the local network
  - Routers exchange reachability and "distance" vectors for all the sub-networks within (a typically small) domain
  - Use vectors to decide which route is best
- Problem: Data (vectors) are not authenticated
  - Forge vectors to cause traffic to be routed through adversary
  - or cause DoS

ARP Spoofing: Background: Ethernet Frames

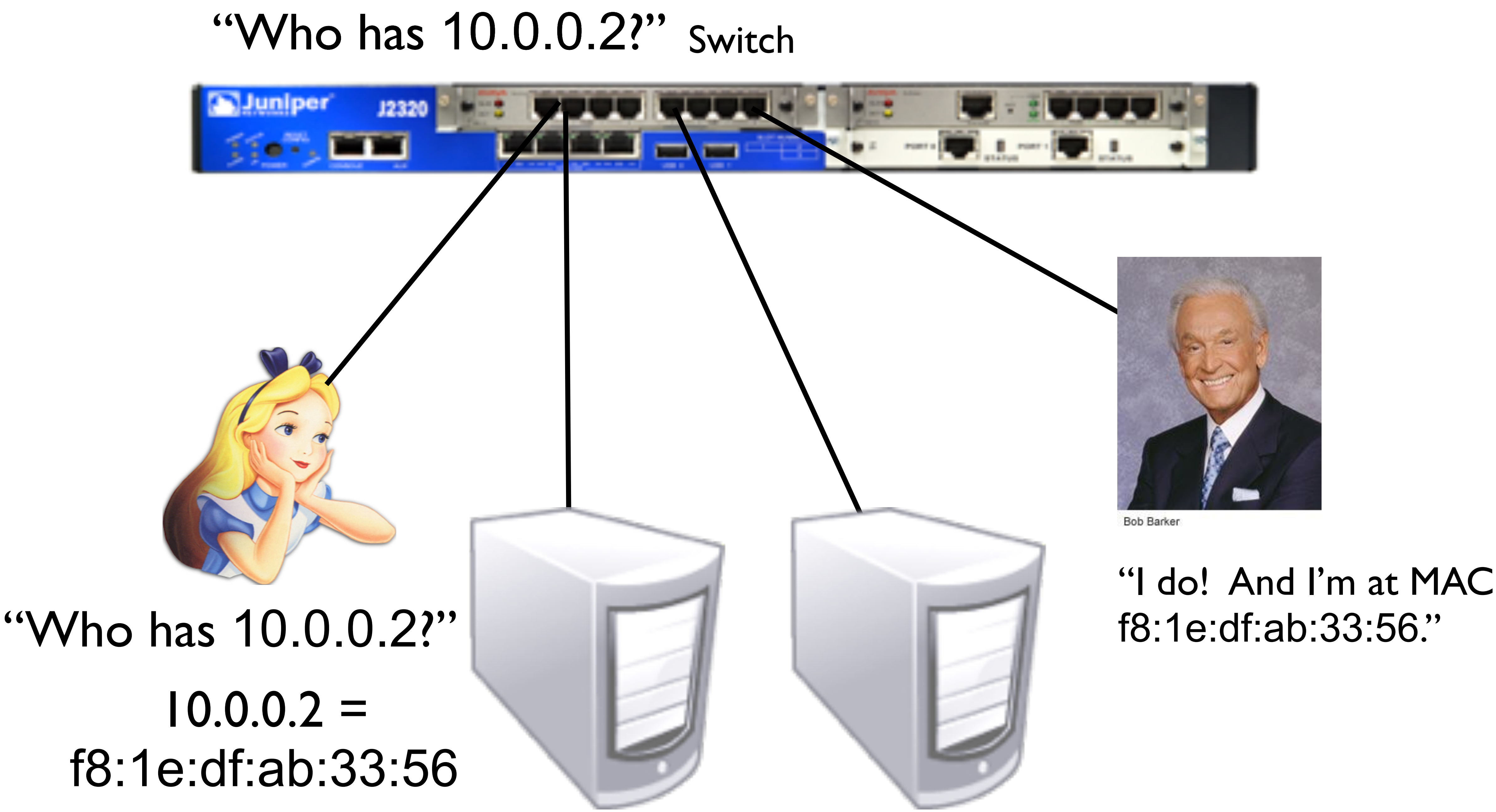


ARP Spoofing: Background: ARP

- **Address Resolution Protocol (ARP):** Locates a host's link-layer (MAC) address
- Problem: How does Alice communicate with Bob over a LAN?
  - Assume Alice (10.0.0.1) knows Bob's (10.0.0.2) IP
  - LANs operate at layer 2 (there is no router inside of the LAN)
  - Messages are sent to the switch, and addressed by a host's link-layer (MAC) address
- Protocol:
  - Alice broadcasts: "Who has 10.0.0.2?"
  - Bob responses: "I do! And I'm at MAC f8:1e:df:ab:33:56."



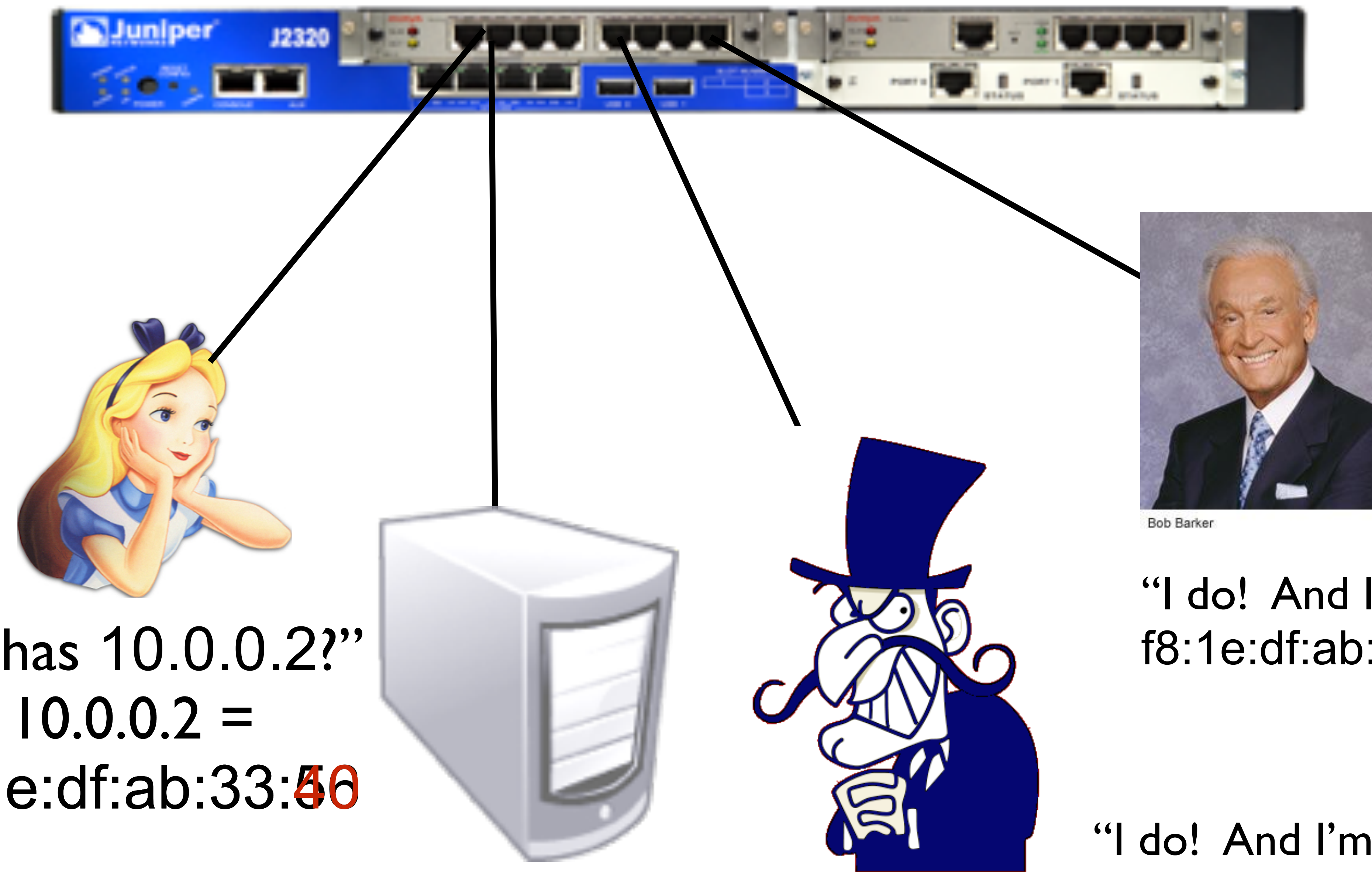
ARP Spoofing: Background: ARP



ARP Spoofing

- Each ARP response overwrites the previous entry in ARP table -- **last response wins**!
- Attack: Forge ARP response
- Effects:
  - Man-in-the-Middle
  - Denial-of-service
- Also called **ARP Poisoning** or **ARP Flooding**

ARP Spoofing: Background: ARP



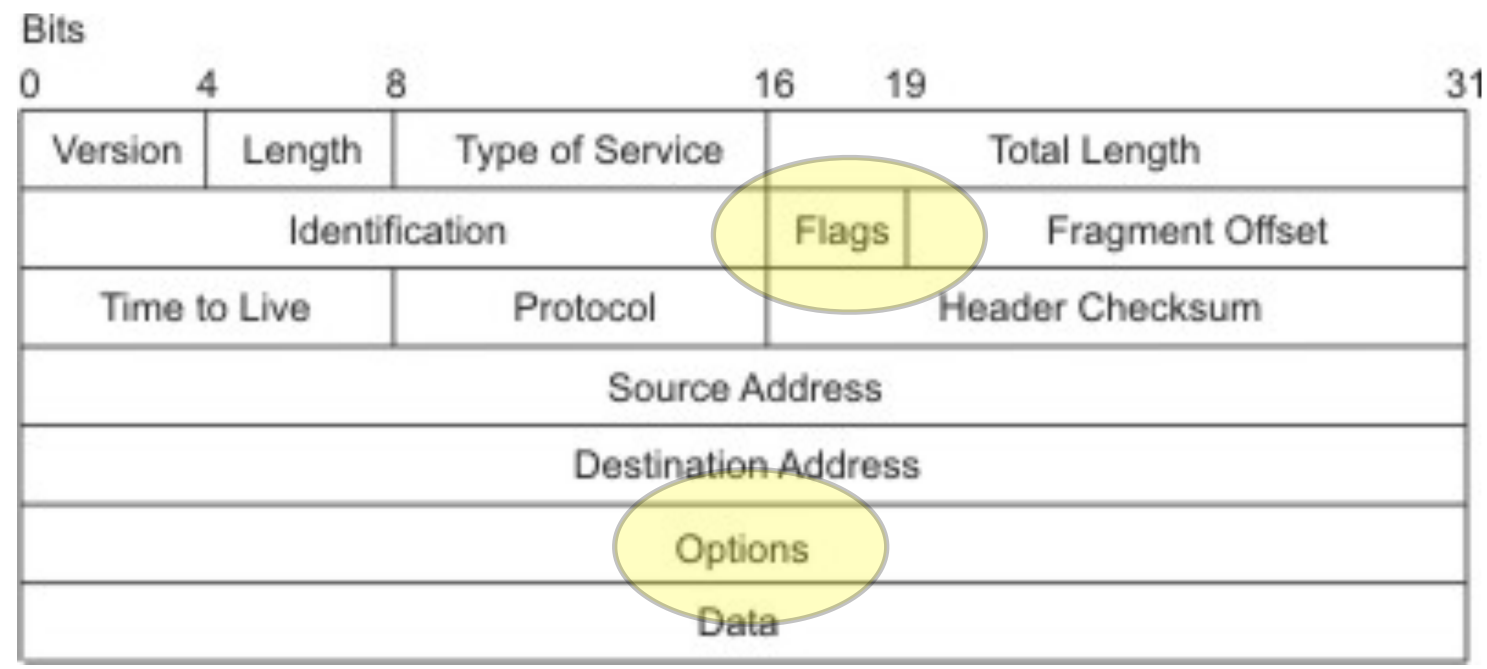
ARP Spoofing: Defenses

- Smart switches that remember MAC addresses
- Switches that assign hosts to specific ports

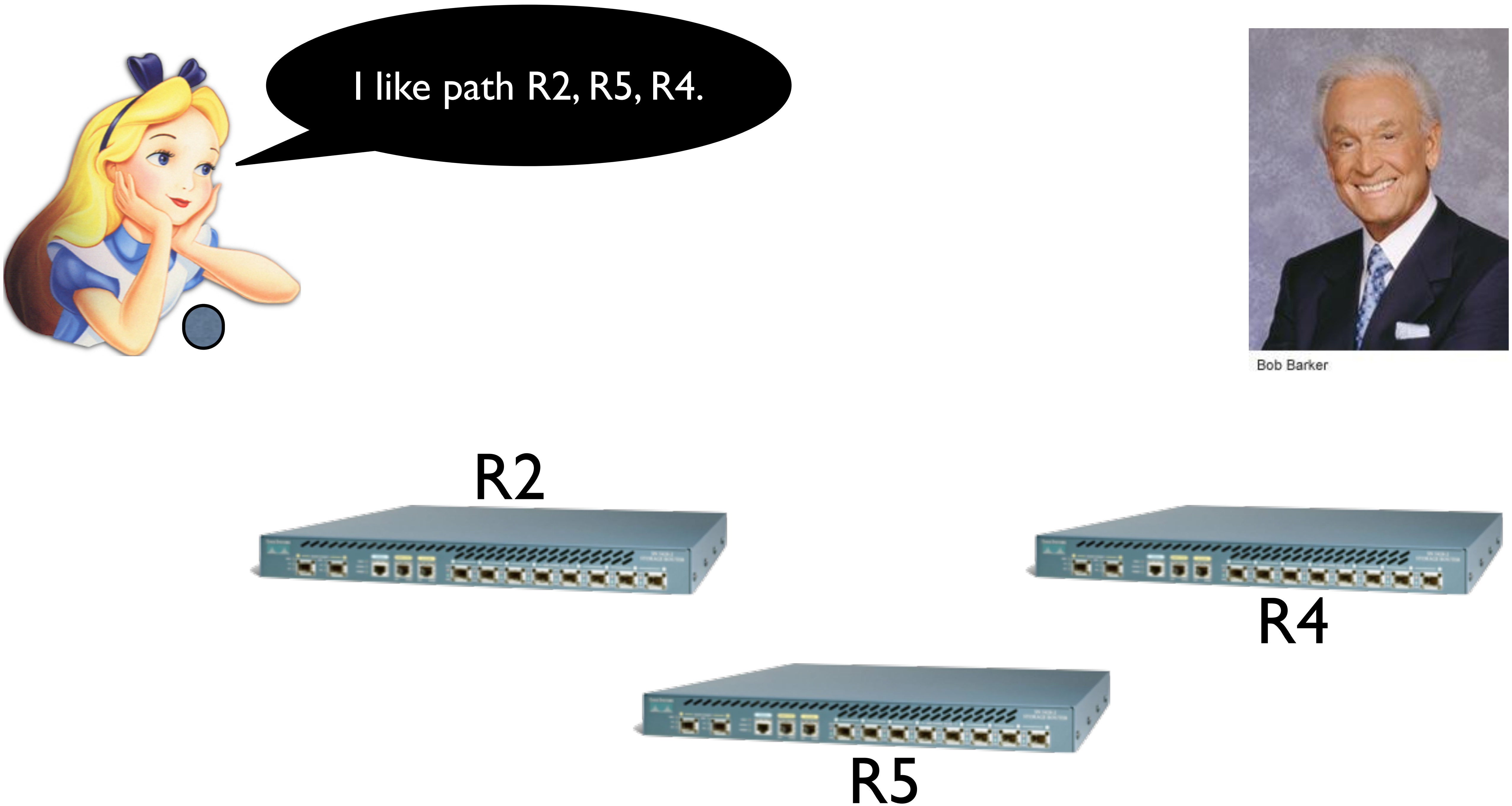
Troubles in troubleshooting

Source Routing

- Standard IP Packet Format (RFC791)
- Source Routing allows sender to specify route
  - Set flag in *Flags* field
  - Specify routes in *Options* field



Source Routing



Source Routing

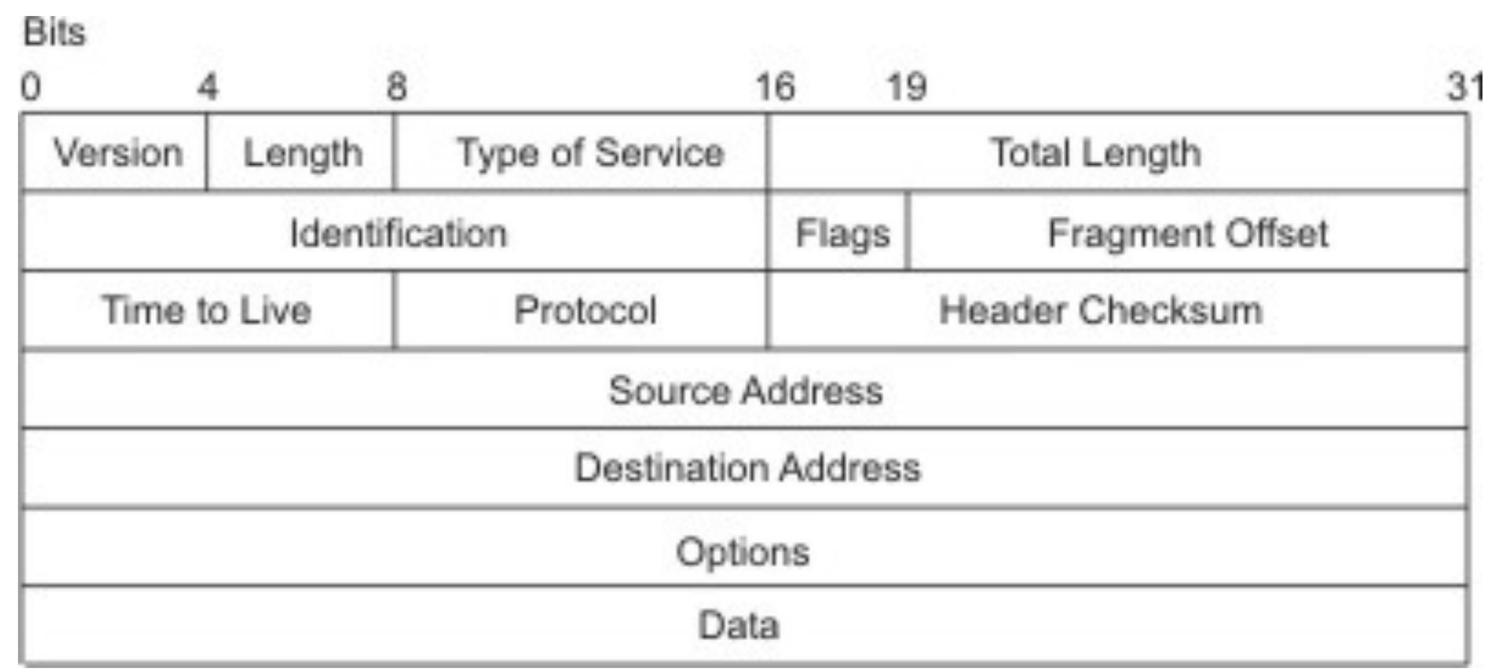
- Q: What are the security implications of Source Routing?
  - Spoofing?
  - Access control?
  - DoS?
- Q: What are the possible defenses?
  - A: Block packets with source-routing flag

Internet Control Message Protocol (ICMP)

- ICMP is used as a control plane for IP messages
  - Ping (connectivity probe)
  - Destination unreachable (error notification)
  - Time-to-live exceeded (error notification)
- Some ICMP messages cause clients to alter behavior
  - e.g., TCP RSTs on destination unreachable or TTL-exceeded
- ICMP messages are easy to spoof: no handshake
- Enables attacker to <u>remotely</u> reset others' connections
- Solution:
  - Verify/sanity check sources and content
  - Filter most of ICMP

Ping-of-Death: Background: IP Fragmentation

- 16-bit "Total Length" field allows $2^{16}-1=65{,}535$ byte packets
- Data link (layer 2) often imposes significantly smaller **Maximum Transmission Unit** (MTU) (normally 1500 bytes)
- Fragmentation supports packet sizes greater than MTU and less than 2^{16}
- 13-bit Fragment Offset specifies offset of fragmented packet, in units of 8 bytes
- Receiver reconstructs IP packet from fragments, and delivers it to Transport Layer (layer 4) after reassembly



Ping-of-Death

- Maximum packet size: 65,535 bytes
- Maximum 13-bit fragment offset is $(2^{13} - 1) * 8 = 65,528$
- In 1996, someone discovered that many operating systems, routers, etc. could be crash/rebooted by sending a **single** malformed packet
  - If packet with maximum possible offset has more than 7 bytes, IP buffers allocated with 65,535 bytes will be overflowed
  - ...causing crashes and reboots

65528

Server buffer | 65535 bytes | Othe

Packet fragment | 50 bytes | @ max offset

Ping-of-Death

- Maximum packet size: 65,535 bytes
- Maximum 13-bit fragment offset is $(2^{13} - 1) * 8 = 65,528$
- In 1996, someone discovered that many operating systems, routers, etc. could be crash/rebooted by sending a **single** malformed packet
  - If packet with maximum possible offset has more than 7 bytes, IP buffers allocated with 65,535 bytes will be overflowed
  - ...causing crashes and reboots
- Not really ICMP specific, but easy
  - % ping -s 65510 your.host.ip.address
- Most OSes and firewalls have been hardened against PODs
- This was a popular pastime of early hackers

Lessons Learned?

- The Internet was built for robust communication
- Smartness occurs at the end-hosts (see End-to-End Principle)
- Does this design support or hinder network security?