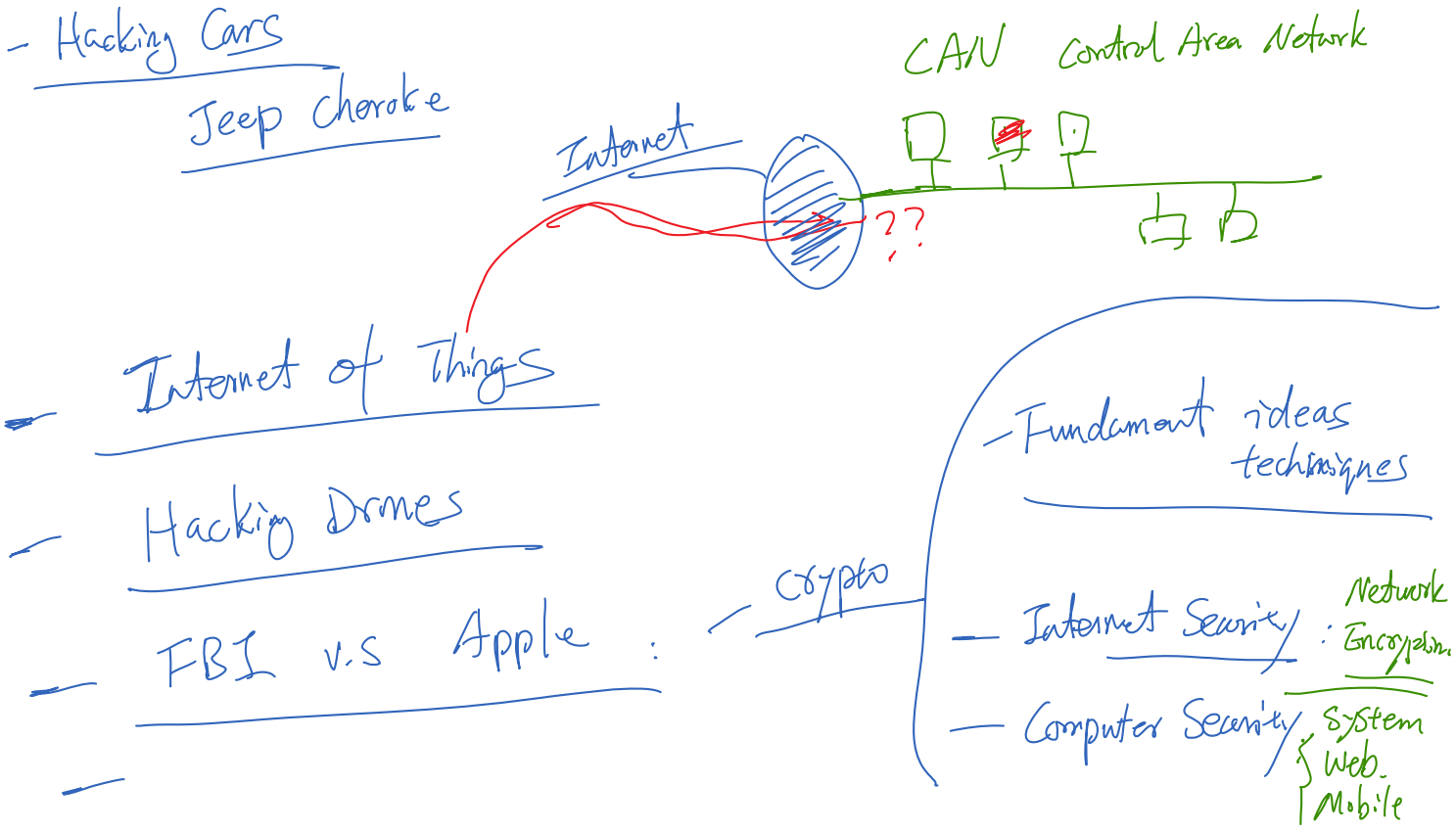
Stories Related to Internet Security

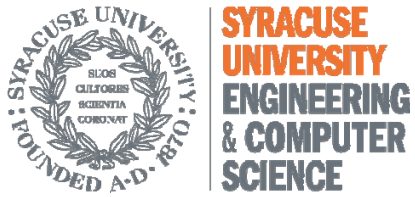
SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Stories Related to Internet Security

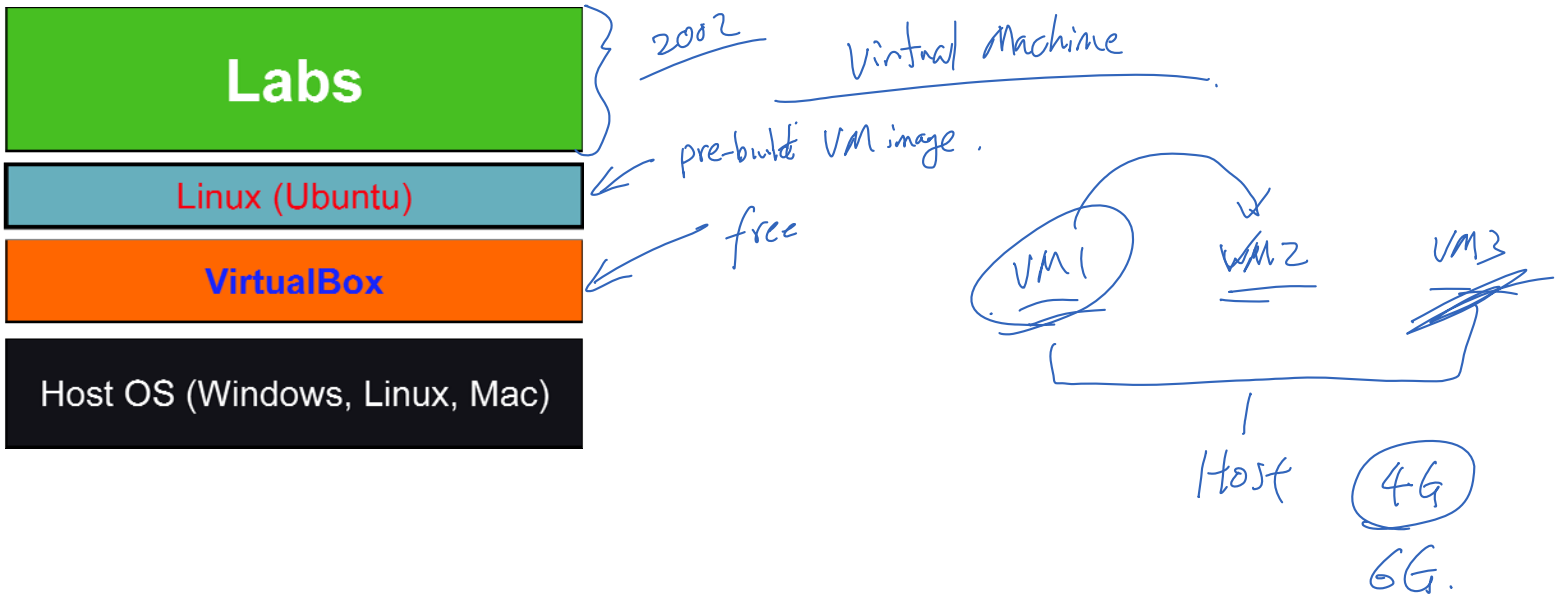


SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

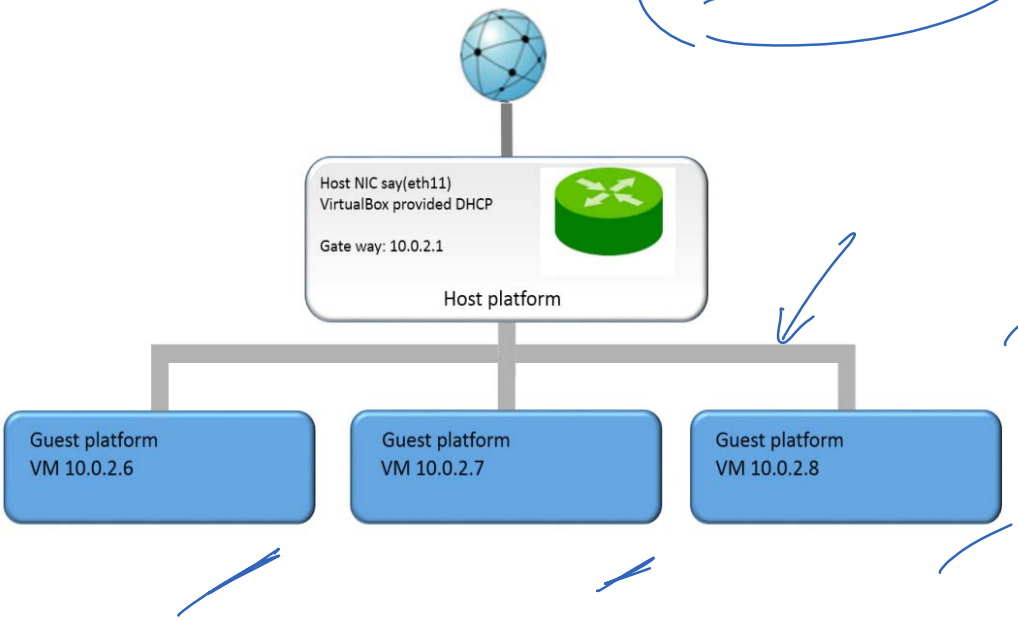
Hands-On Exercises



Hands-On Exercises: Lab Environment



Network Setup



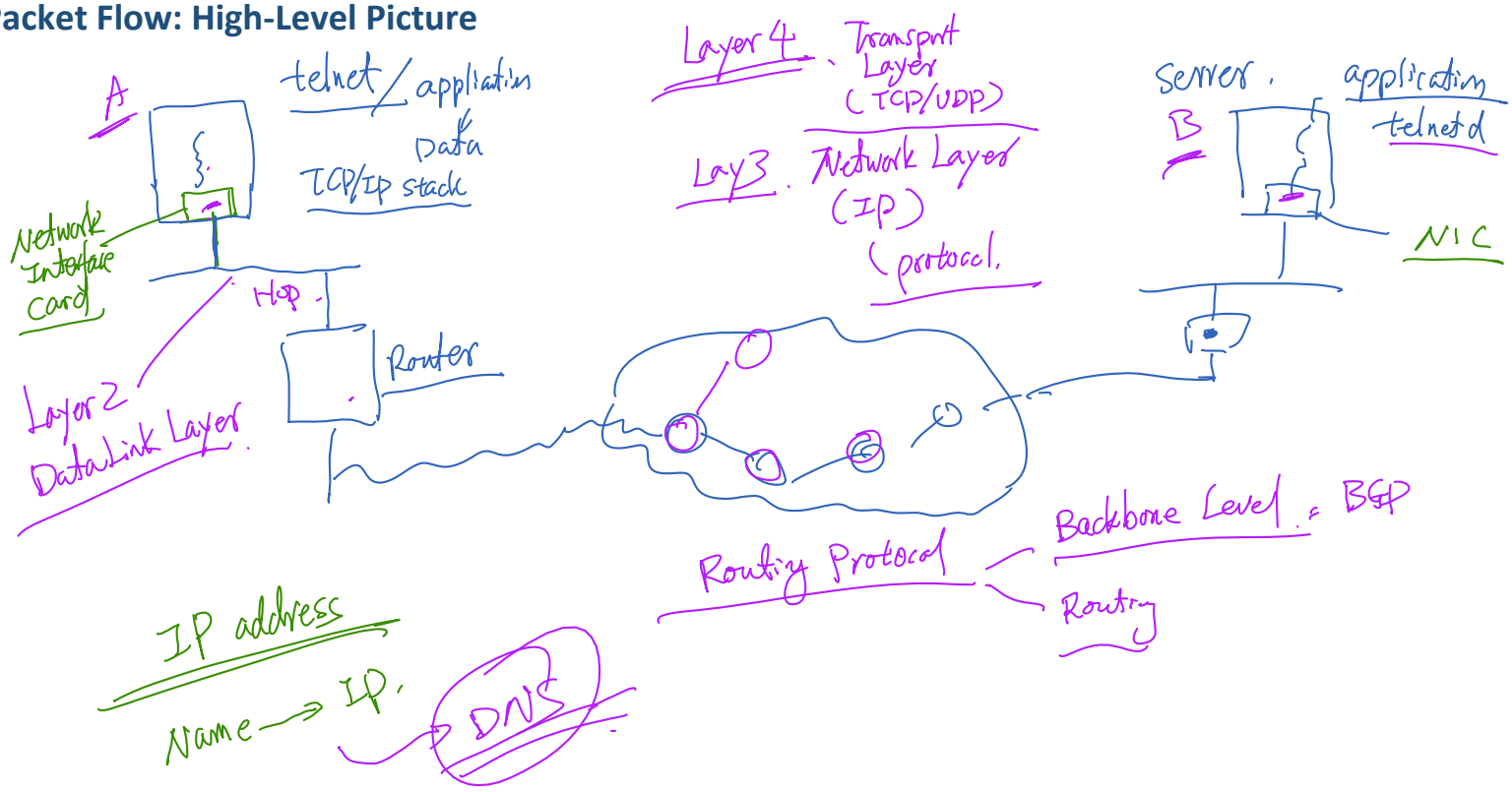
Sample Lab Exercises

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Packet Flow Over the Internet

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Packet Flow: High-Level Picture

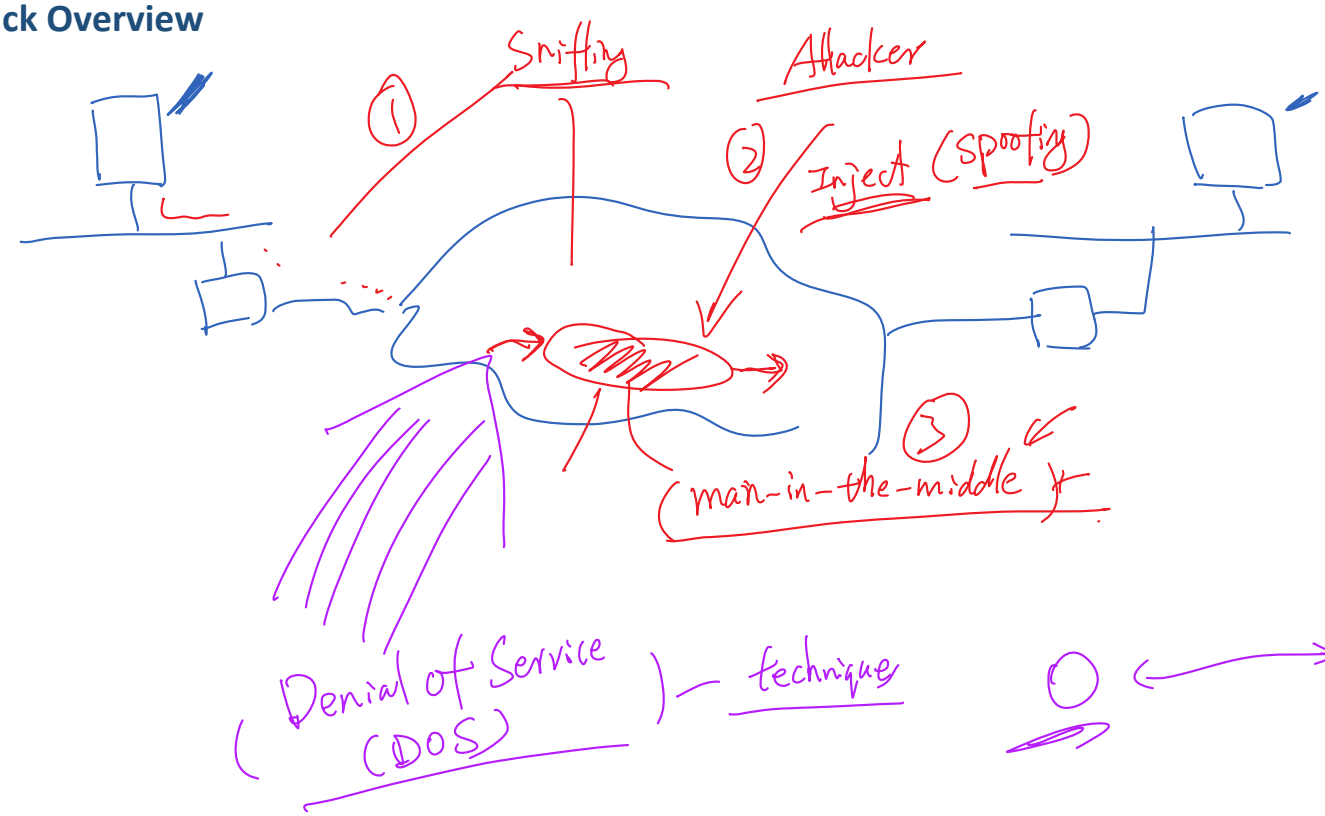


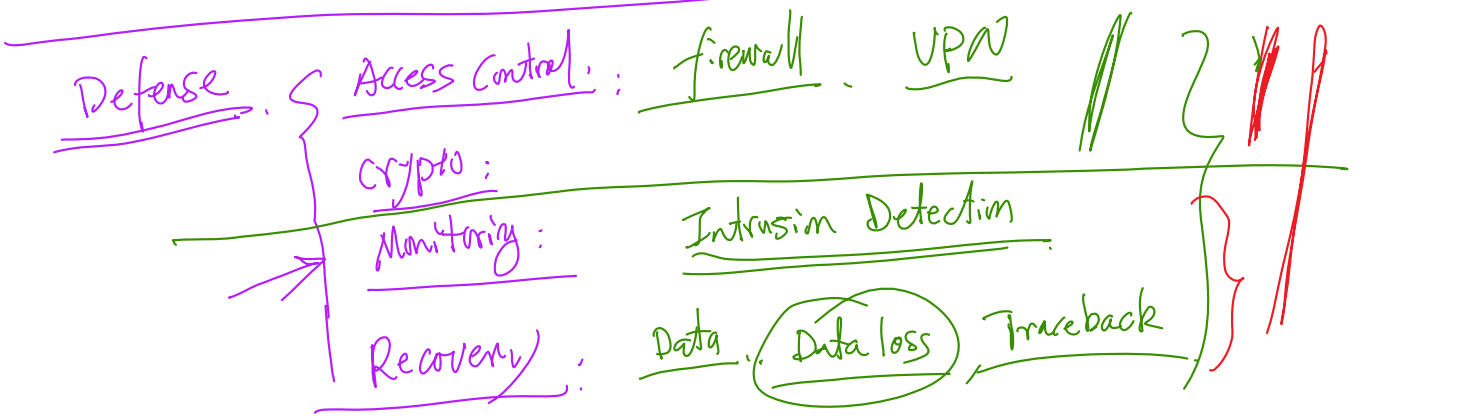
SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Attack Overview

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Attack Overview



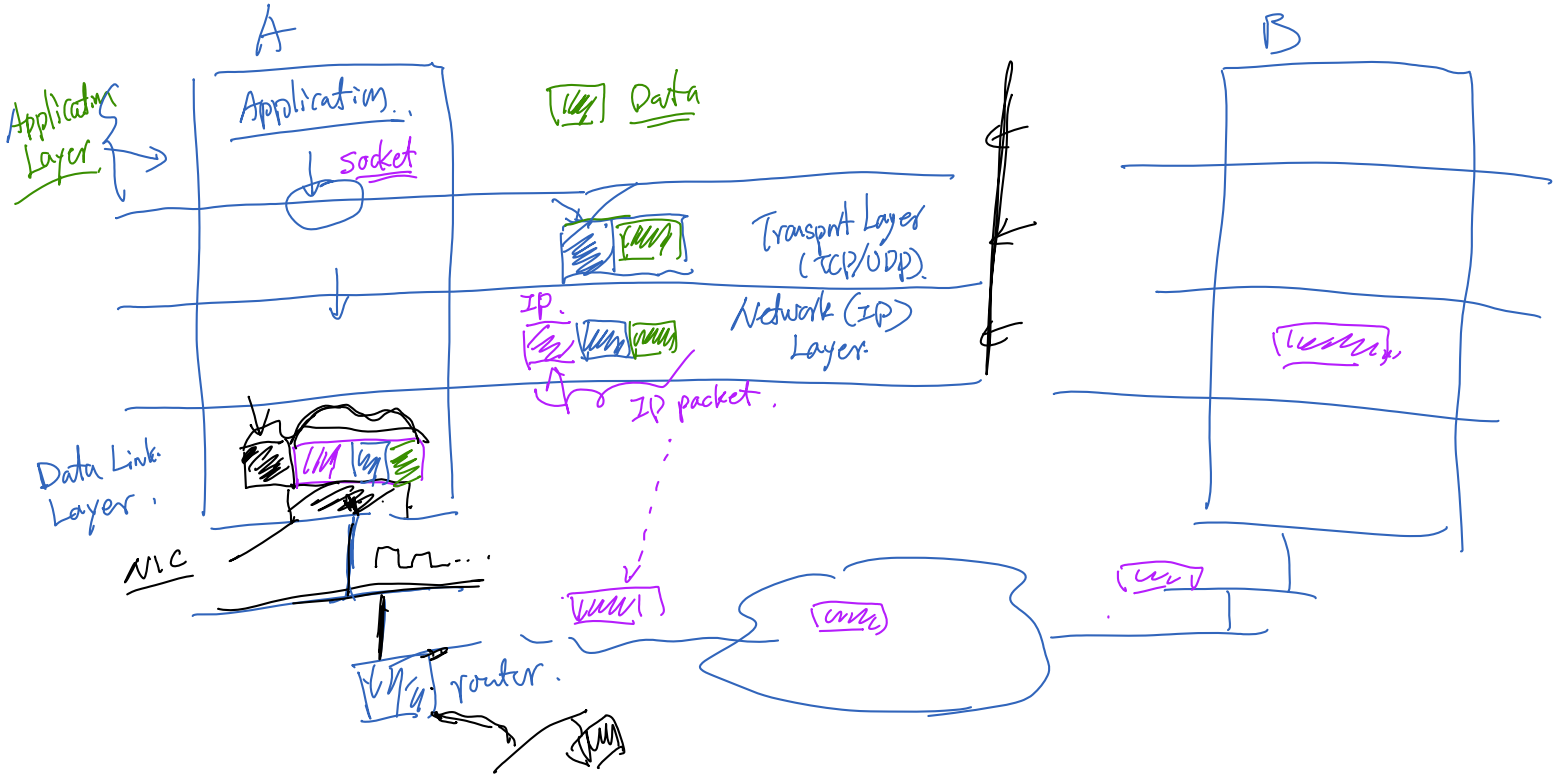


SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

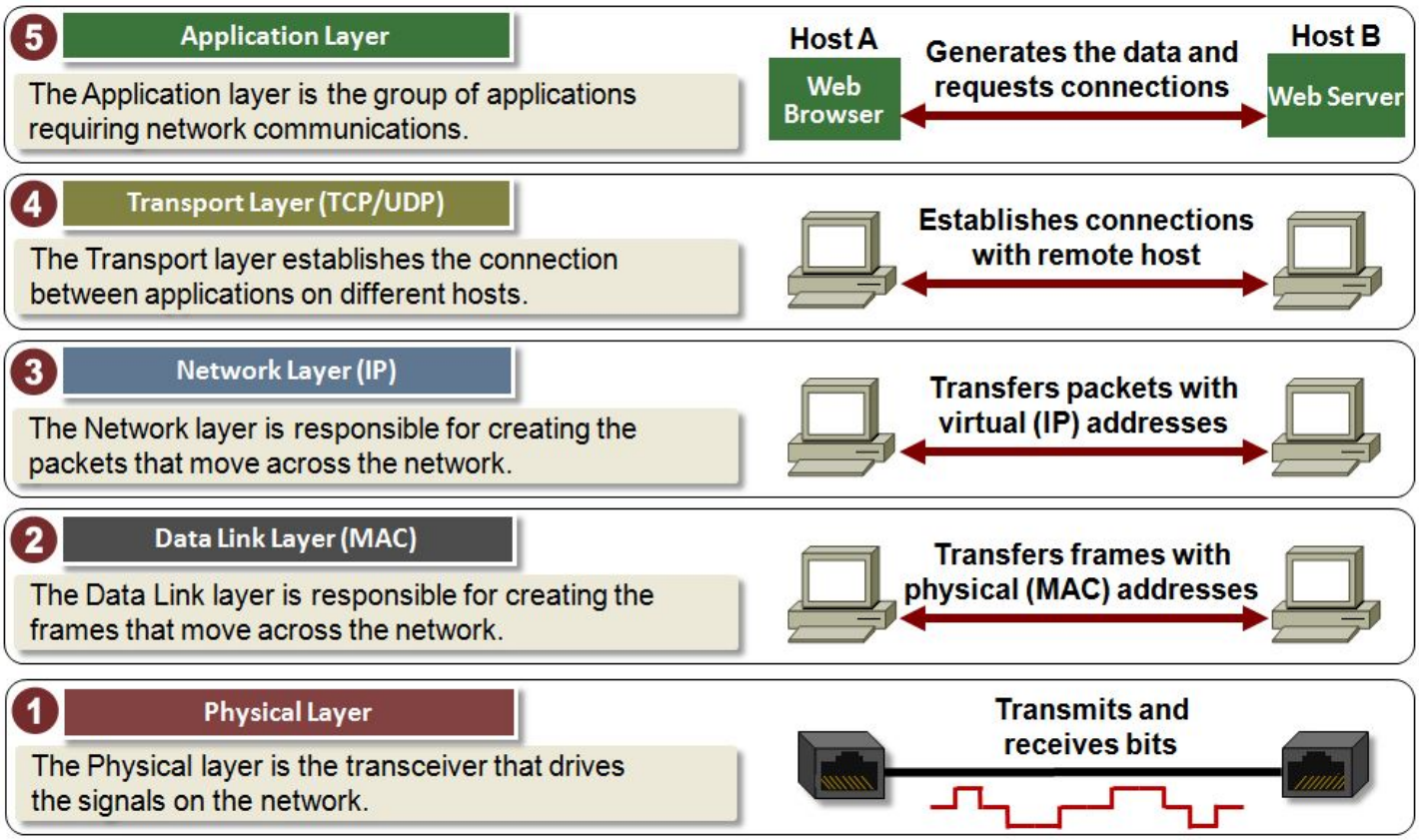
TCP/IP Layers

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Network Data Traverses Through Layers



TCP/IP Layers

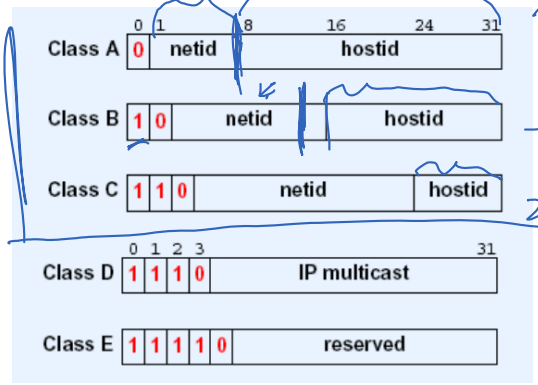


SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

IP Address

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

IP Address



2^{24}

Classful Scheme

2^{16}

128.230.. 2^{16}

2^{8}

32-bit IP.

2^{32}

Netmask

Classless Scheme.

netid

128.230.0.0/16

128.230.0.0/14

Netid

IP

2^{32}

IPV6

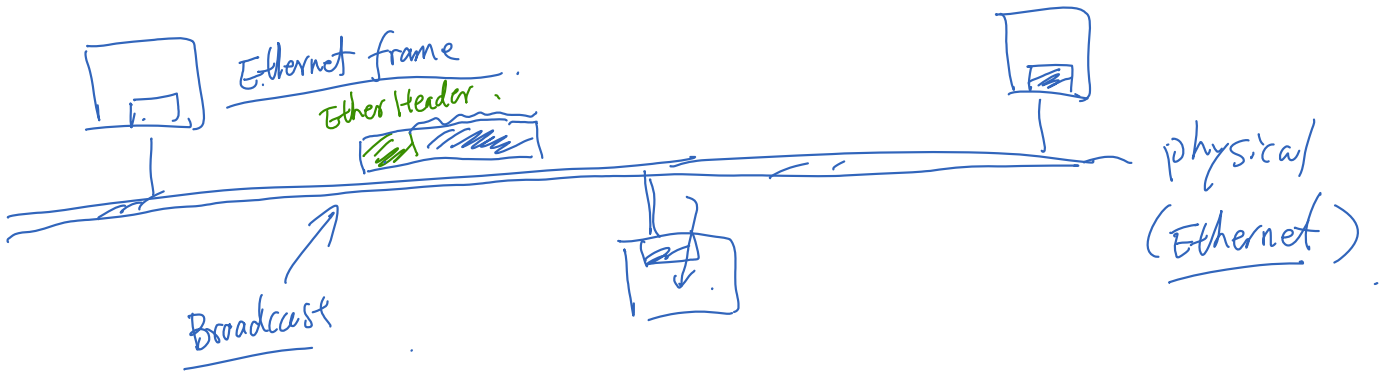
NAT

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

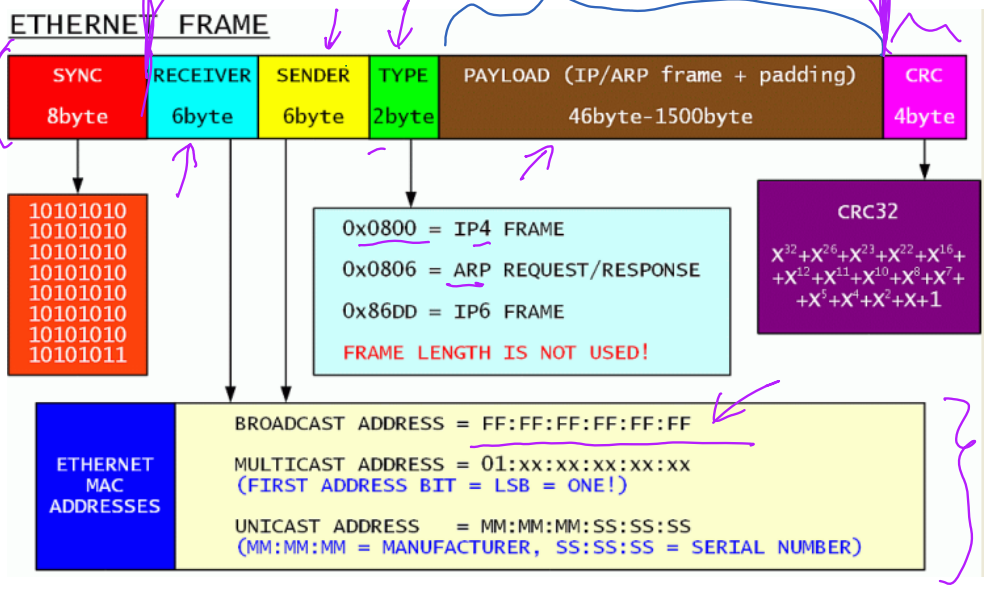
Data Link Layer, Ethernet

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Data Link Layer (MAC Layer)



Ethernet Frame



Hardware Address
(MAC)
NIC

MAC Address Example

```
$ ifconfig
eth16     Link encap:Ethernet  HWaddr 08:00:27:cf:eb:bd
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecf:ebbd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:35897 errors:0 dropped:0 overruns:0 frame:0
          TX packets:877 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14323226 (14.3 MB)  TX bytes:159911 (159.9 KB)

eth18     Link encap:Ethernet  HWaddr 08:00:27:c5:79:5f
          inet6 addr: fe80::a00:27ff:fec5:795f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32348 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27211 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2839116 (2.8 MB)  TX bytes:1830313 (1.8 MB)
```

Privacy Issue Related to MAC

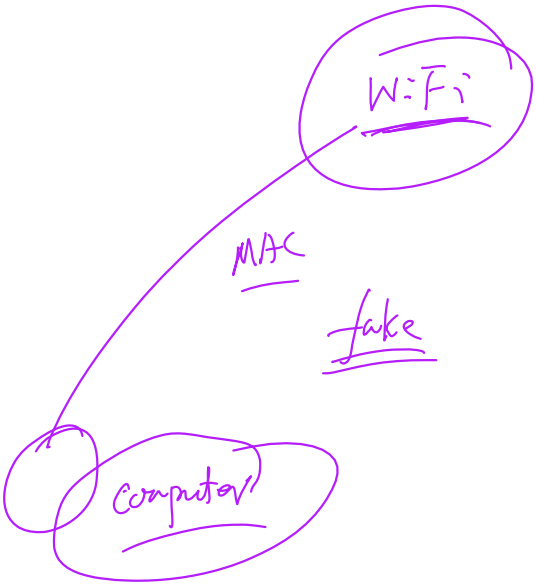
iOS 8 to stymie trackers and marketers with MAC address randomization

When searching for Wi-Fi networks, iOS8 devices can hide their true identities.

by **Lee Hutchinson** - Jun 9, 2014 10:56am EDT

Share Tweet Email 88

Quartz is reporting a change to how iOS 8-equipped devices search out Wi-Fi networks with which to connect. The new mobile operating system, which is on track for a release in the fall, gives iOS 8 devices the ability to identify themselves not with their unique burned-in hardware MAC address but rather with a random, software-supplied address instead.

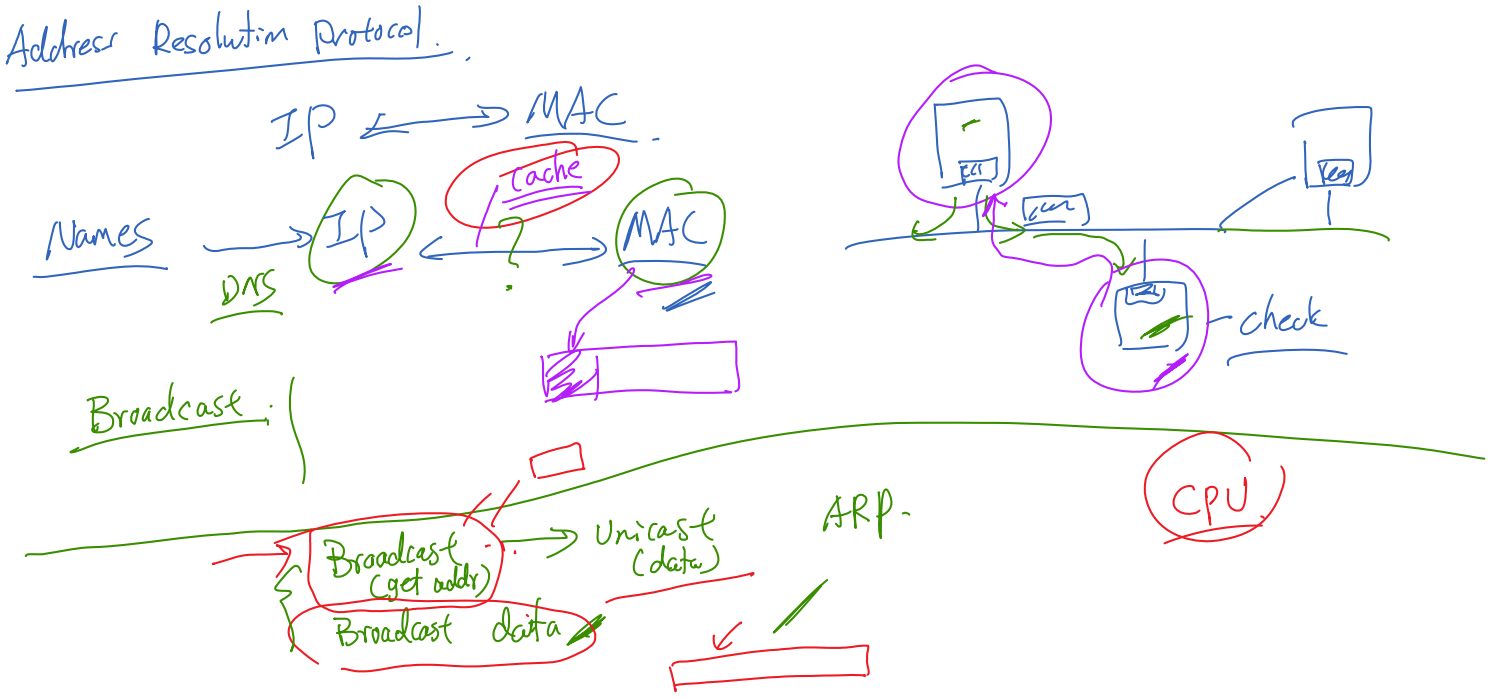


SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

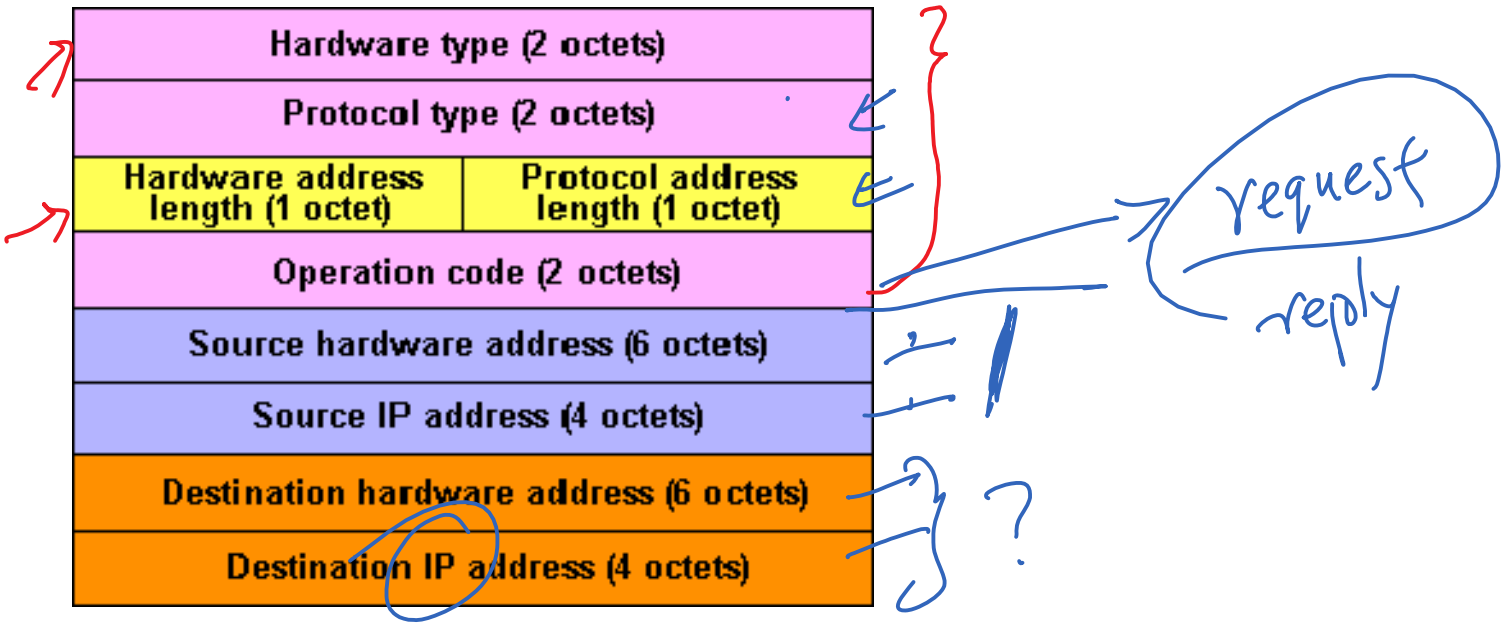
ARP Protocol

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

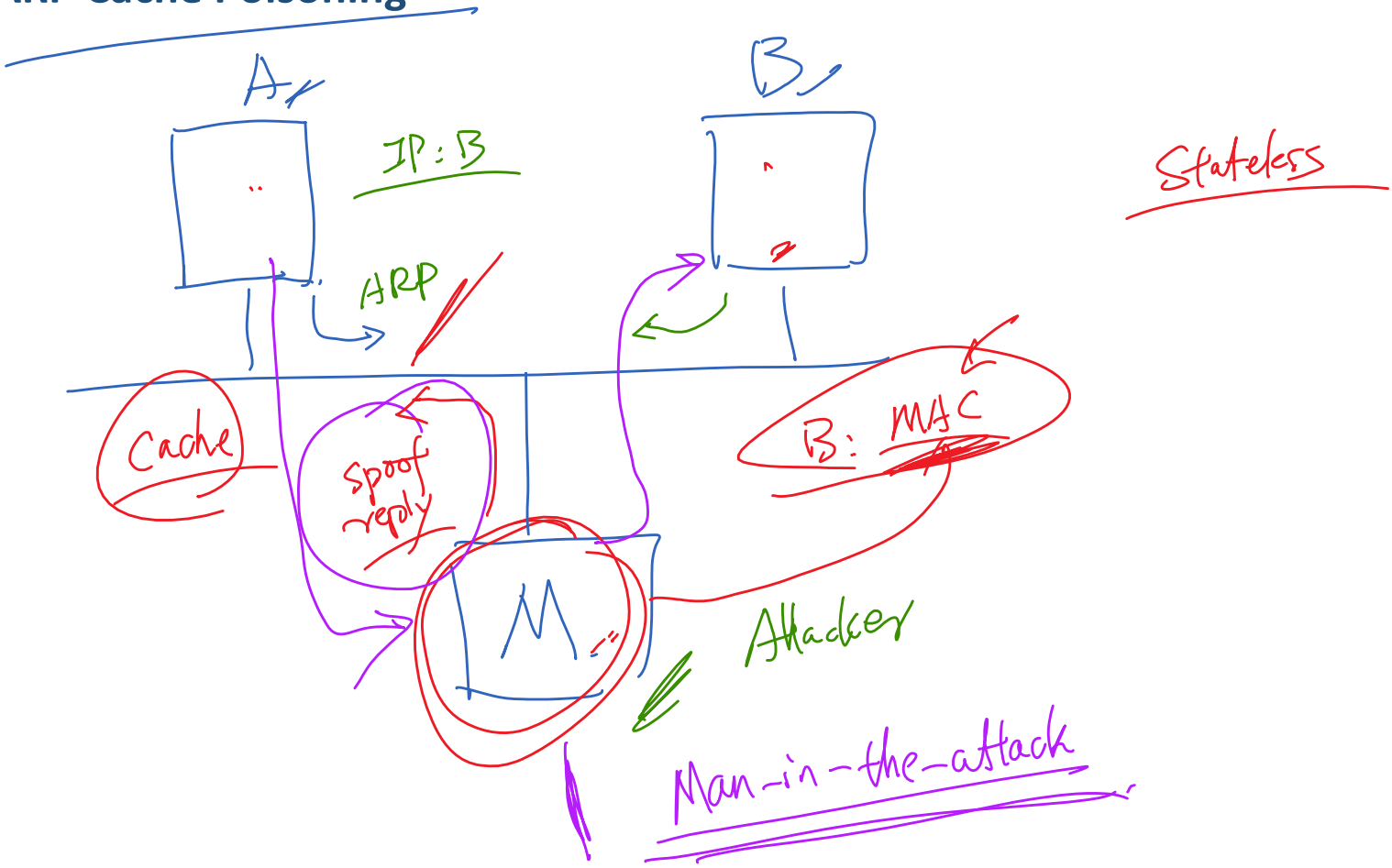
ARP: IP Address to Ethernet Address



ARP Format


Hardware type (2 octets)
Protocol type (2 octets)
Hardware address length (1 octet)
Protocol address length (1 octet)
Operation code (2 octets)
Source hardware address (6 octets)
Source IP address (4 octets)
Destination hardware address (6 octets)
Destination IP address (4 octets)
request
reply

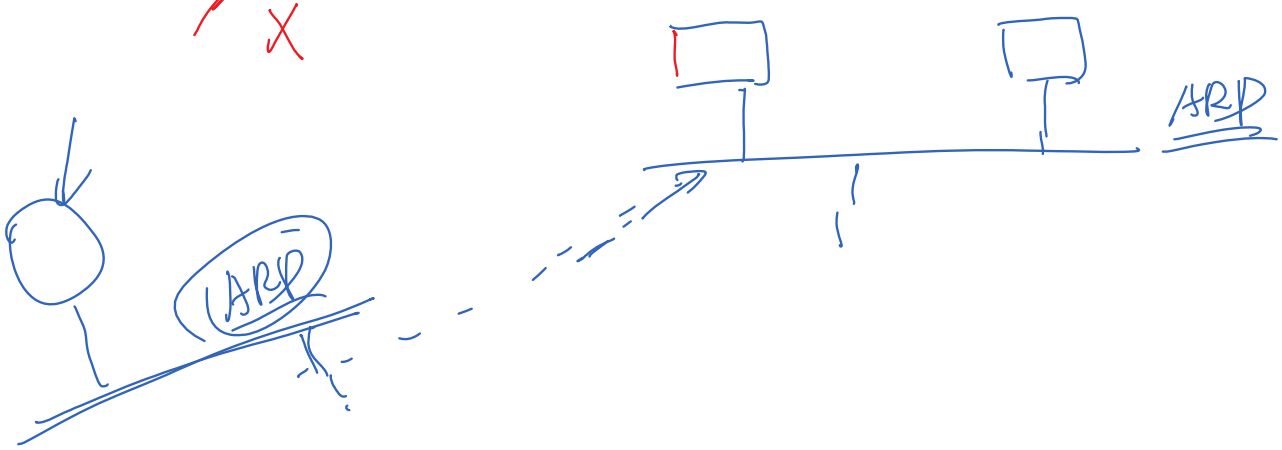
ARP Cache Poisoning



Question: ARP Cache Poisoning

Which of the following is true?

a. A computer in Russia can launch the ARP cache-poisoning attack on your computers in Syracuse.
b. The ARP cache-poisoning attack can achieve denial of service.
c. If the ARP does not use a cache, it is safe.



SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Summary

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Summary

- High-level picture of packet flow and attack overview
- TCP/IP layers
- IP address
- Data link layer
- ARP protocol and ARP cache-poisoning attack

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE