Network Attacks

CMSC 23200, Spring 2025, Lecture 7

Grant Ho

University of Chicago, 04/15/2025

Slides adapted from Blasé Ur, Peyrin Kao, Vern Paxson, and Borja Sotomayor

Logistics

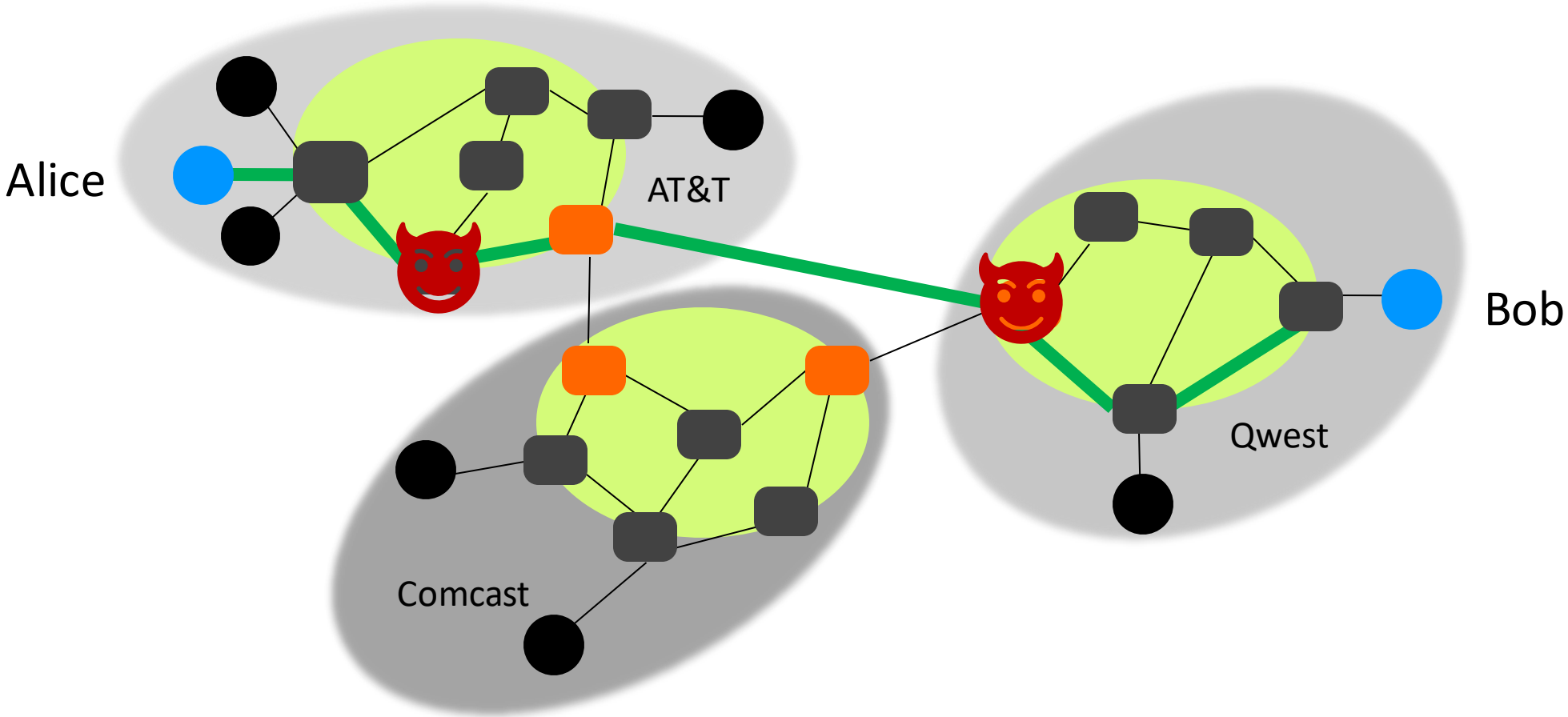
- Assignment 3 (Crypto) Due on Thursday (04/17) @ 11:59pm
- No Discussion Section This Week
- Final Exam Time: **Wednesday, May 28 @ 10am**
  - COMBINED TIME FOR BOTH SECTIONS

Network Threat Model: 3 Types of Attackers

Alice & Bob want to communicate over the Internet:
What kinds of attackers do they need to worry about?

	Can modify or delete packets	Can read packets	Can inject new packets
1) In-Path attacker (Man-in-the-middle)	✓	✓	✓

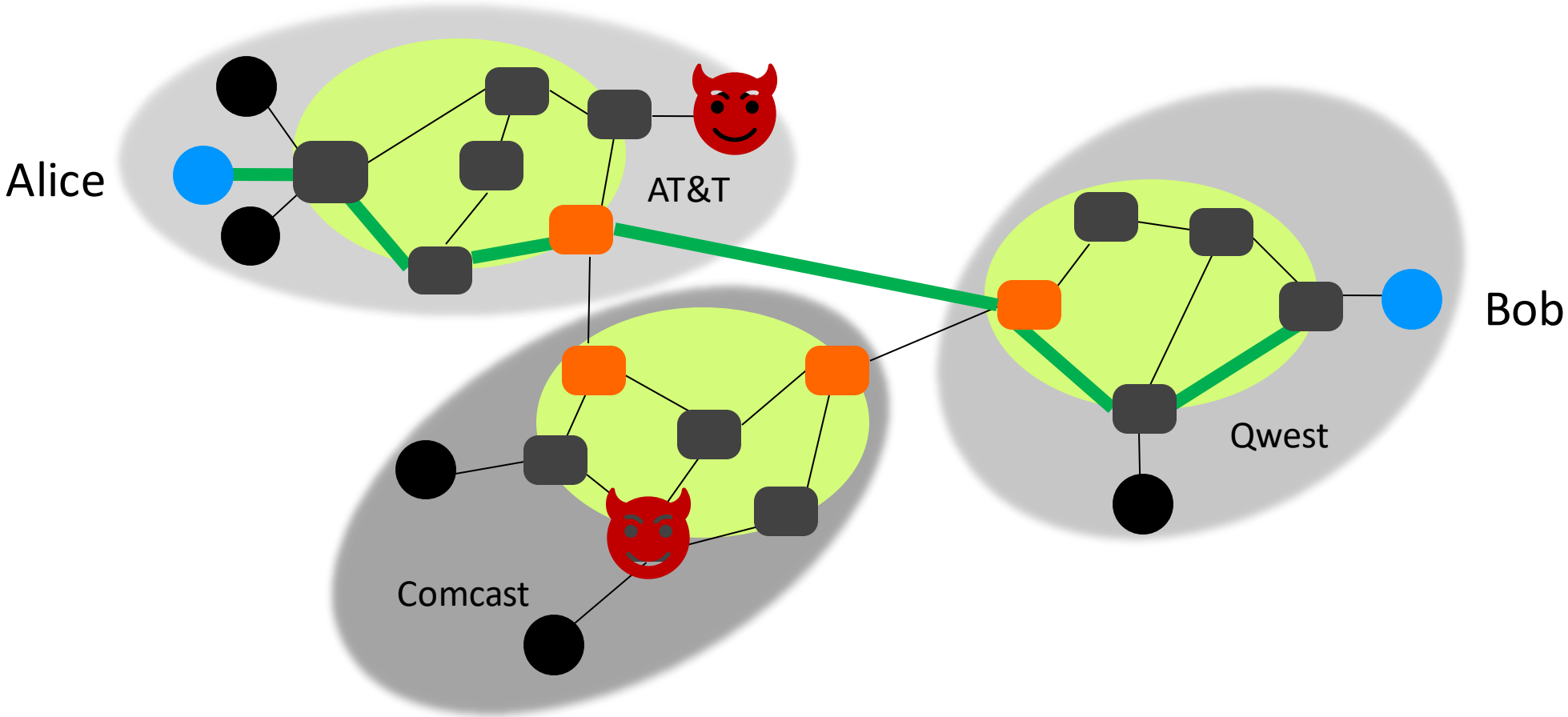
In-Path (MITM) Attacker Examples



Network Threat Model: 3 Types of Attackers

	Can modify or delete packets	Can read packets	Can inject new packets
1) In-Path attacker (Man-in-the-middle)	✓	✓	✓
3) Off-path attacker			✓

Off-Path Attacker Examples

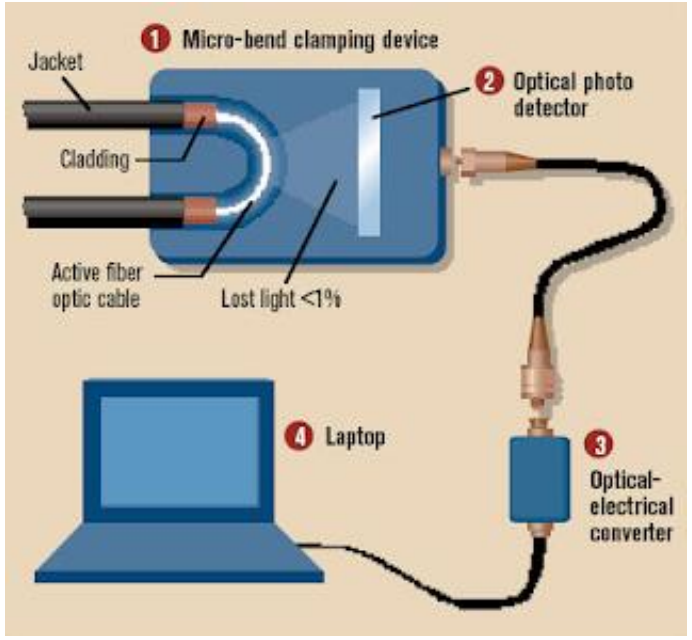


Network Threat Model: 3 Types of Attackers

	Can modify or delete packets	Can read packets	Can inject new packets
1) In-Path attacker (Man-in-the-middle)	✓	✓	✓
2) On-path attacker		✓	✓
3) Off-path attacker			✓

Real-World On-Path Attackers

- How might a real-life attacker read packets?
- Layer 1 attack: Use a special device to read bits being transmitted across space



Real-World On-Path Attackers

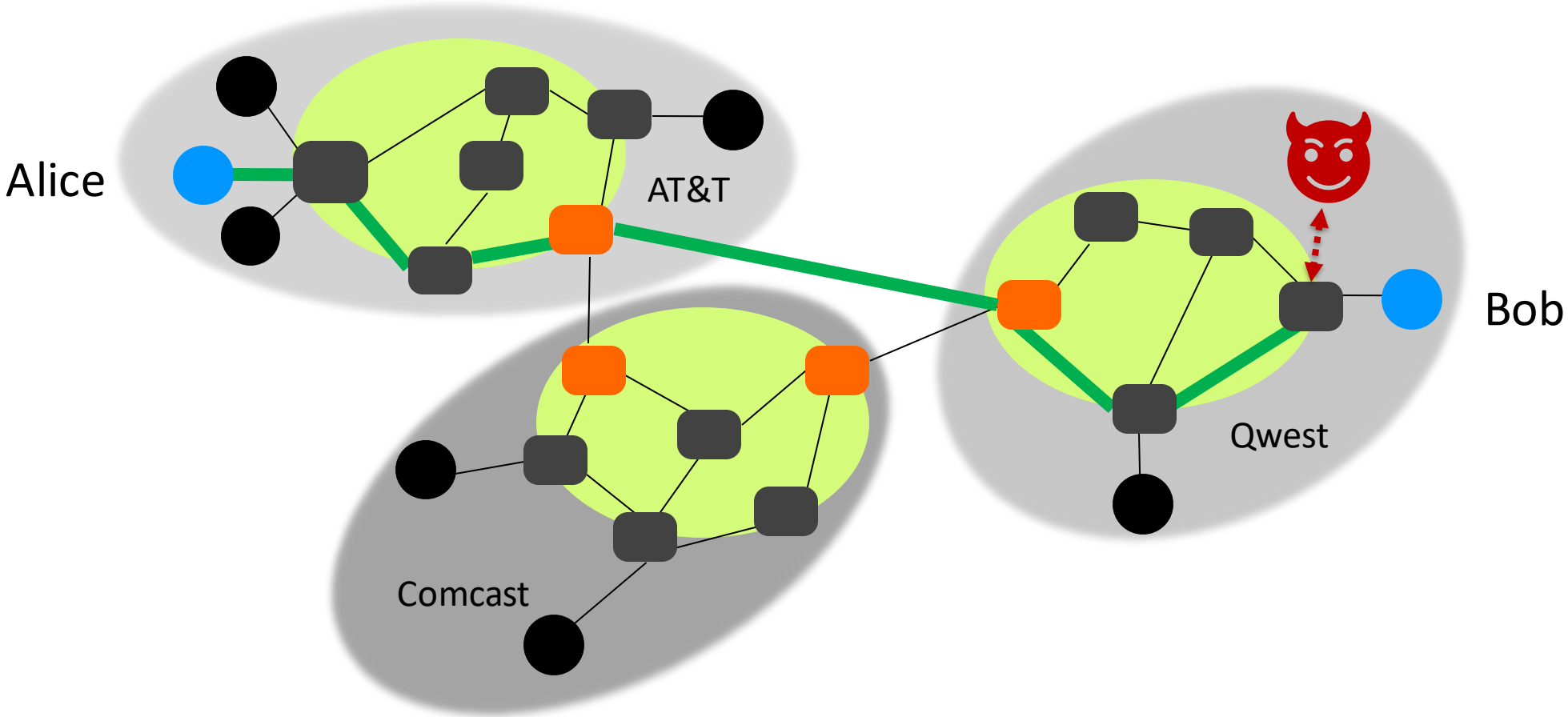
Military.com

Operation Ivy Bells

Matthew Carle *February 6, 2017*

In an effort to alter the balance of the Cold War, divers from the USS Halibut scoured the ocean floor for a five-inch diameter cable that carried secret Soviet communications between military bases. The divers found the cable and installed a listening device. Upon their return to the United States, the NSA analyzed the recordings and found that a surprising amount of sensitive Soviet information travelled through the lines without encryption. The original tap was later discovered by the Soviets and is now on exhibit at the KGB museum in Moscow.

On-Path Attacker Examples



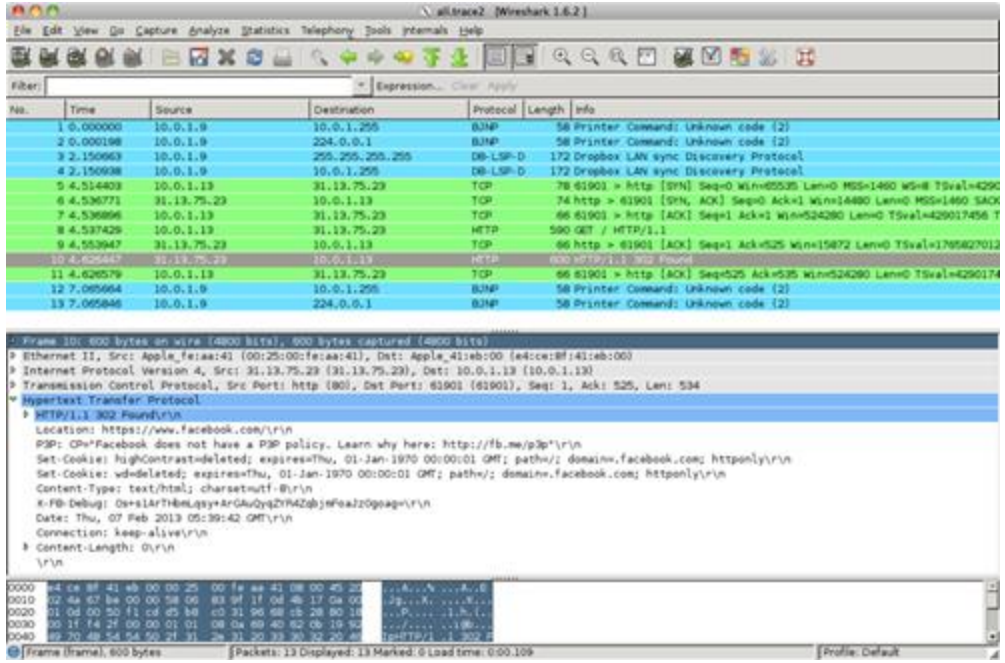
Real-World On-Path Attackers

- LAN (Local Area Network) is a network of connected machines
  - Any machine on LAN can send packets to other machines on the LAN
- Some LANs use **broadcast technologies** (e.g., Wifi)
  - Every packet gets sent to every machine on the LAN
  - Each machine agrees to ignore packets where the destination is a different machine, if they follow protocol
- A machine can break the agreement and read packets meant for other machines
  - This is called **promiscuous mode**

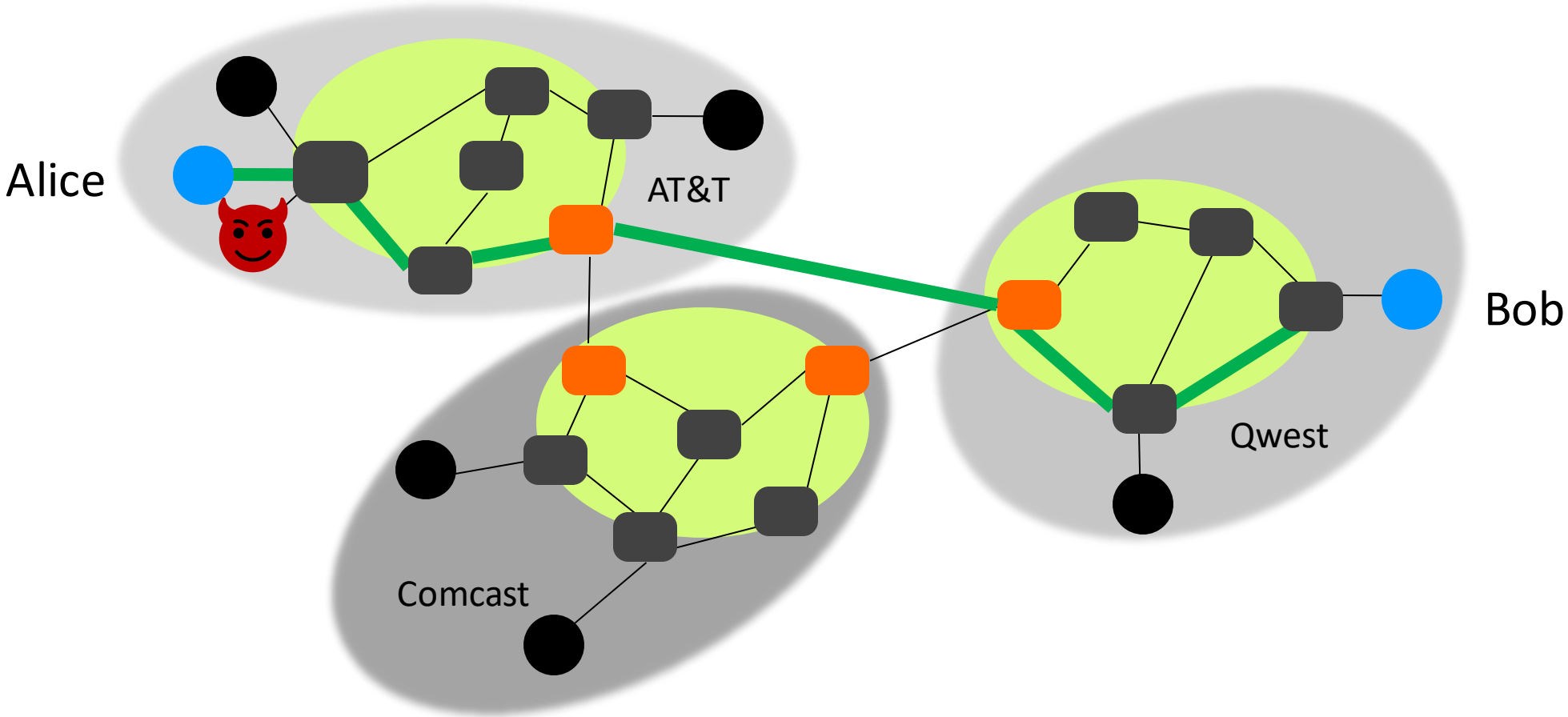
Real-World On-Path Attackers

- **`tcpdump`**: A program for reading packets on the local network
  - Uses promiscuous mode to read other machines' broadcast packets
- Wireshark: A graphical user interface (GUI) for analyzing **`tcpdump`** packets

```
demo 2 % tcpdump -r all.trace2
reading from file all.trace2, link-type EN10MB (Ethernet)
21:39:37.772367 IP 10.0.1.9.60627 > 10.0.1.255.canon-bjnp2: UDP, length 16
21:39:37.772565 IP 10.0.1.9.62137 > all-systems.mcast.net.canon-bjnp2: UDP, length 16
21:39:39.923030 IP 10.0.1.9.17500 > broadcasthost.17500: UDP, length 130
21:39:39.923305 IP 10.0.1.9.17500 > 10.0.1.255.17500: UDP, length 130
21:39:42.286770 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [S], seq 2
523449627, win 65535, options [mss 1460,nop,wscale 3,nop,nop,TS val 429017455 ecr 0,sack
OK,eol], length 0
21:39:42.309138 IP star-01-02-pao1.facebook.com.http > 10.0.1.13.61901: Flags [S.], seq
3585654832, ack 2523449628, win 14480, options [mss 1460,sackOK,TS val 1765826995 ecr 42
9017455,nop,wscale 9], length 0
21:39:42.309263 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [.], ack 1
, win 65535, options [nop,nop,TS val 429017456 ecr 1765826995], length 0
21:39:42.309796 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [P.], seq
1:525, ack 1, win 65535, options [nop,nop,TS val 429017456 ecr 1765826995], length 524
21:39:42.326314 IP star-01-02-pao1.facebook.com.http > 10.0.1.13.61901: Flags [.], ack 5
25, win 31, options [nop,nop,TS val 1765827012 ecr 429017456], length 0
21:39:42.398814 IP star-01-02-pao1.facebook.com.http > 10.0.1.13.61901: Flags [P.], seq
1:535, ack 525, win 31, options [nop,nop,TS val 1765827083 ecr 429017456], length 534
21:39:42.398946 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [.], ack 5
35, win 65535, options [nop,nop,TS val 429017457 ecr 1765827083], length 0
21:39:44.838031 IP 10.0.1.9.54277 > 10.0.1.255.canon-bjnp2: UDP, length 16
21:39:44.838213 IP 10.0.1.9.62896 > all-systems.mcast.net.canon-bjnp2: UDP, length 16
```



On-Path Attacker Examples



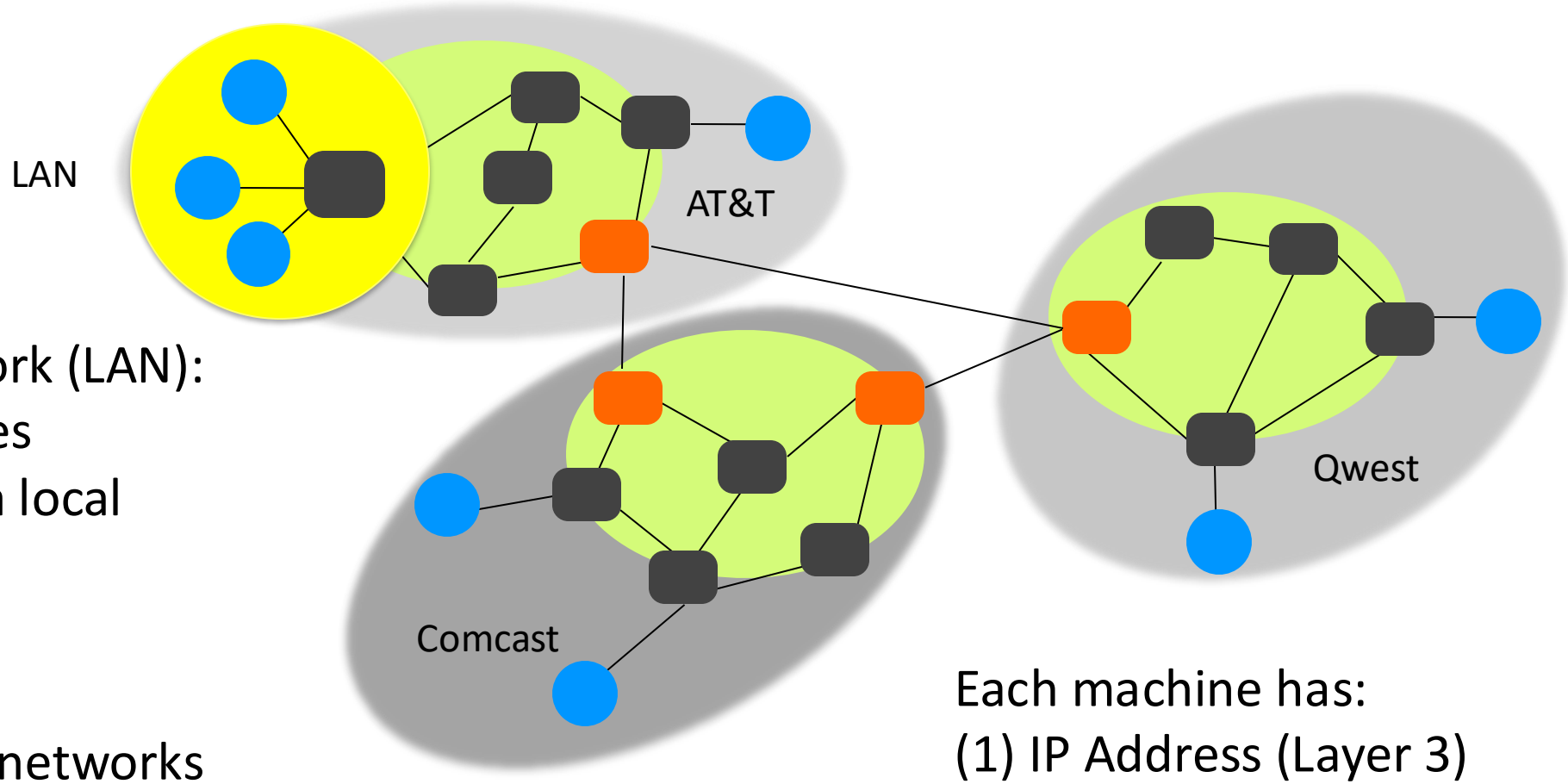
Network Attacks

- Attacks on confidentiality
  (e.g., eavesdropping, side channel information, scanning)
- Attacks on integrity
  (e.g., spoofing, packet injection)
- Attacks on availability
  (e.g., denial of service, or **DoS**)

Outline

- Networking Threat Models
- ARP/DHCP Security
- WPA2: Wifi security

Recall: The Internet From 10,000 Feet



Local Area Network (LAN):

- Set of machines connected in a local network

Internet (IP):

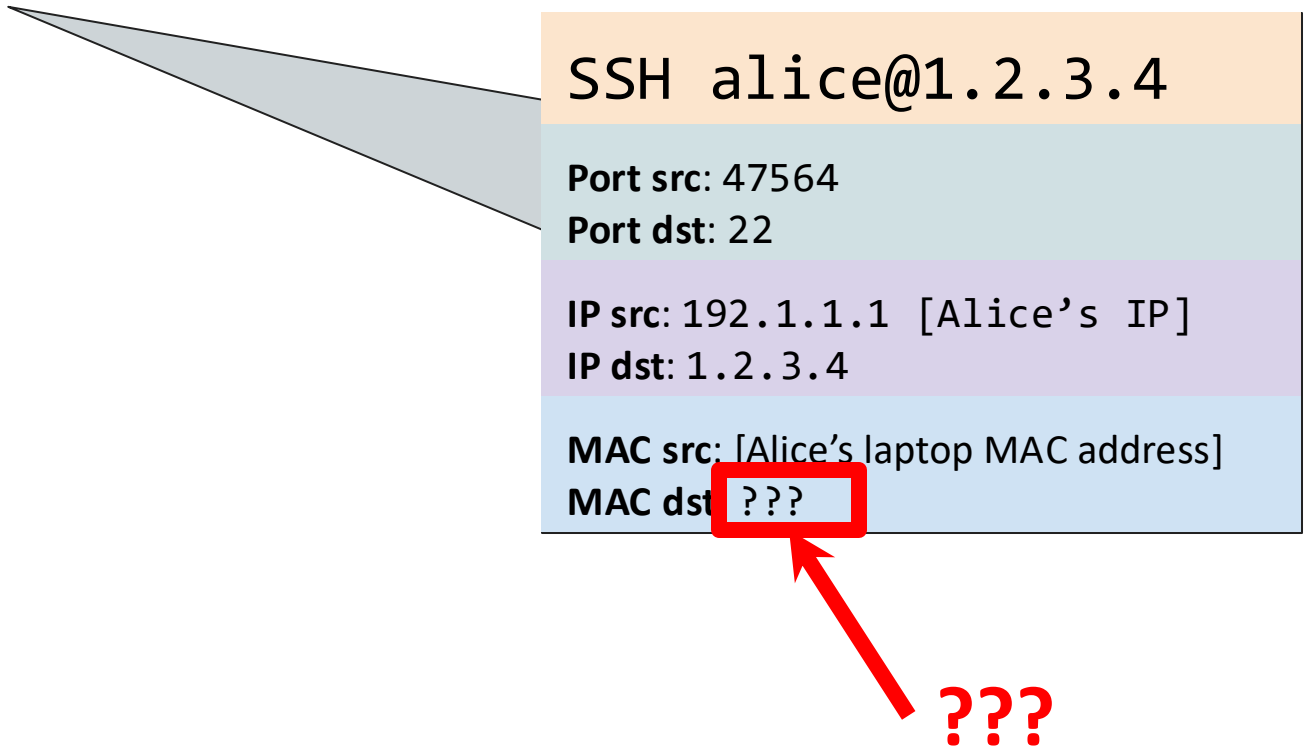
- Set of smaller networks connected via routers

Each machine has:
(1) IP Address (Layer 3)
(2) MAC Address (Layer 2)

Address Resolution Protocol (ARP)

The Problem: Alice knows Bob's IP address & wants to send him data (e.g., Alice performs ssh login to VM [Bob] @ IP address = `1.2.3.4`)

- What should she fill in for the Layer 2 header (MAC Address)?

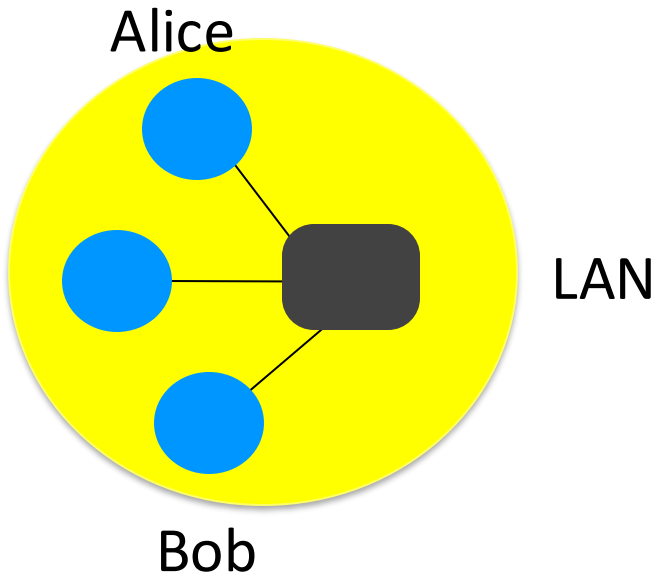


Address Resolution Protocol (ARP)

The Problem: Alice knows Bob's IP address & wants to send him data (e.g., Alice performs ssh login to VM [Bob] @ IP address = `1.2.3.4`)

- What should she fill in for the Layer 2 header (MAC Address)?

ARP: Translates IP addresses to MAC addresses



Address Resolution Protocol (ARP)

The Problem: Alice knows Bob's IP address & wants to send him data (e.g., Alice performs ssh login to VM [Bob] @ IP address = `1.2.3.4`)

- What should she fill in for the Layer 2 header (MAC Address)?

ARP: Translates IP addresses to MAC addresses

1. Alice checks her ARP cache to see if she already knows Bob's MAC address.
2. If Bob's MAC addr not in the cache, Alice **broadcasts** to everyone on the LAN: "What is the MAC address of **`1.2.3.4`**?"
3. Bob responds by sending a message only to Alice: "My IP is **`1.2.3.4`** and my MAC address is **`ca:fe:f0:0d:be:ef`**."
   Everyone else does nothing.
4. Alice caches Bob's MAC address & uses it.

Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC

Alice

Bob

Charlie

Dave

Router

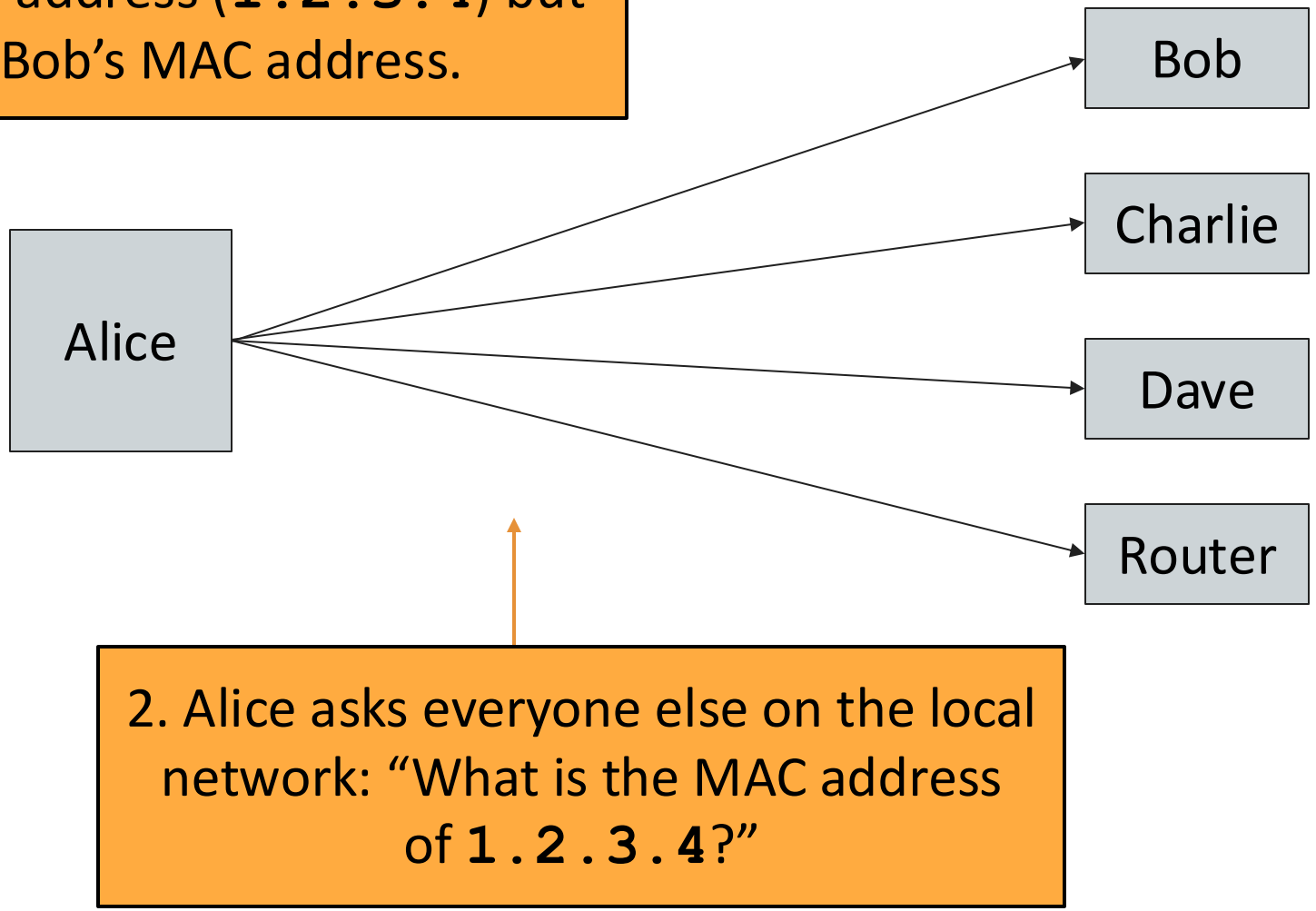
1. Alice checks her cache to see if she already knows the MAC address corresponding to `1.2.3.4`.

Not in the cache: she must make a request to find out.

Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

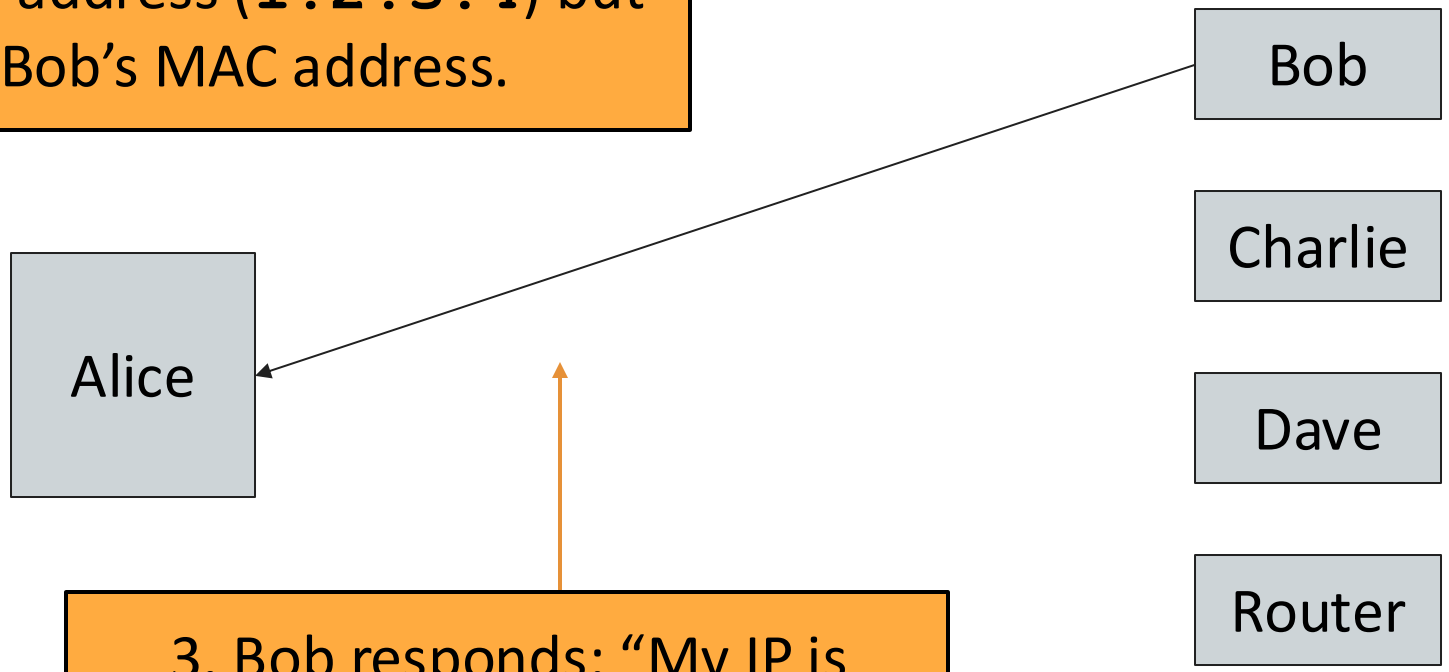
Alice's cache	
IP	MAC



Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC



Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC
`1.2.3.4`	`ca:fe:f0:0d:be:ef`

Alice

Bob

Charlie

Dave

Router

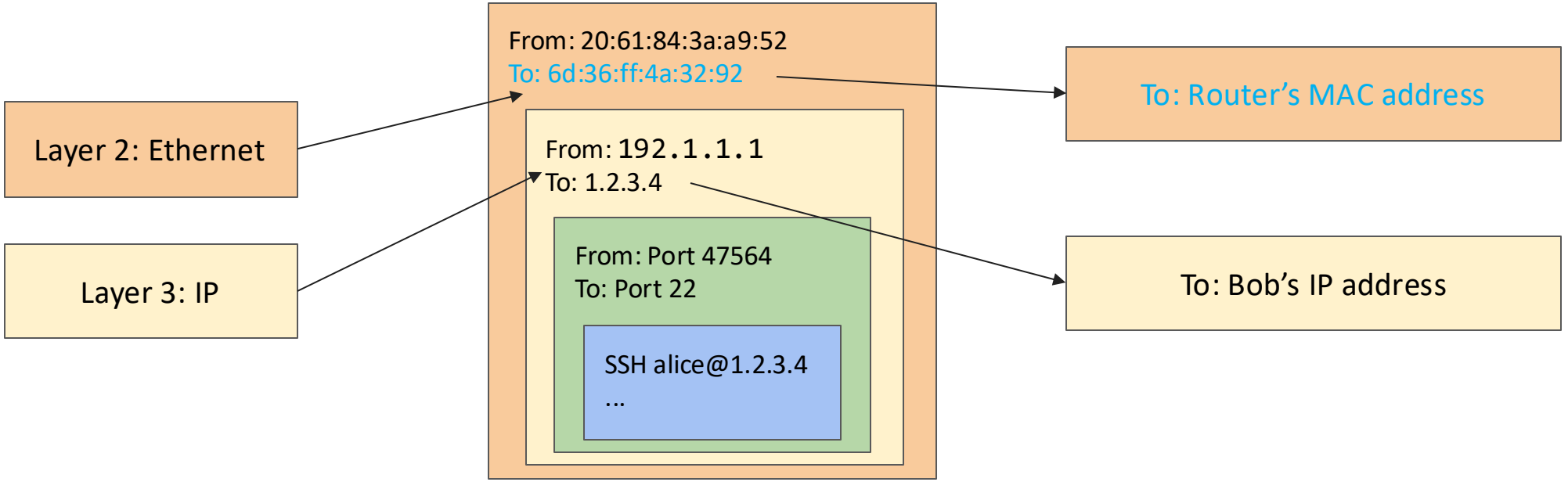
4. Alice adds Bob's MAC address to her cache.

NOTE: All received ARP replies are cached, even if no request was sent!!

Address Resolution Protocol (ARP)

If Bob is outside of the LAN, the router responds w/ its own MAC address

- If Alice wants to send a packet to Bob, she sends the packet to the router
- The router can forward the packet to other LANs to reach Bob



Spoofing Attacks

- Anybody can send their own packets through the network
- **Spoofing**: Lying about the identity of a packet's sender
  - The attacker can lie about source addresses in the packet header
  - Example: Mallory sends a message and says the message is from Bob
- All 3 types of attackers can spoof packets
  - However, some spoofing attacks may be harder if the attacker can't read or modify packets

Spoofing Attacks on ARP

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC

Alice

Bob

Charlie

Mallory

Router

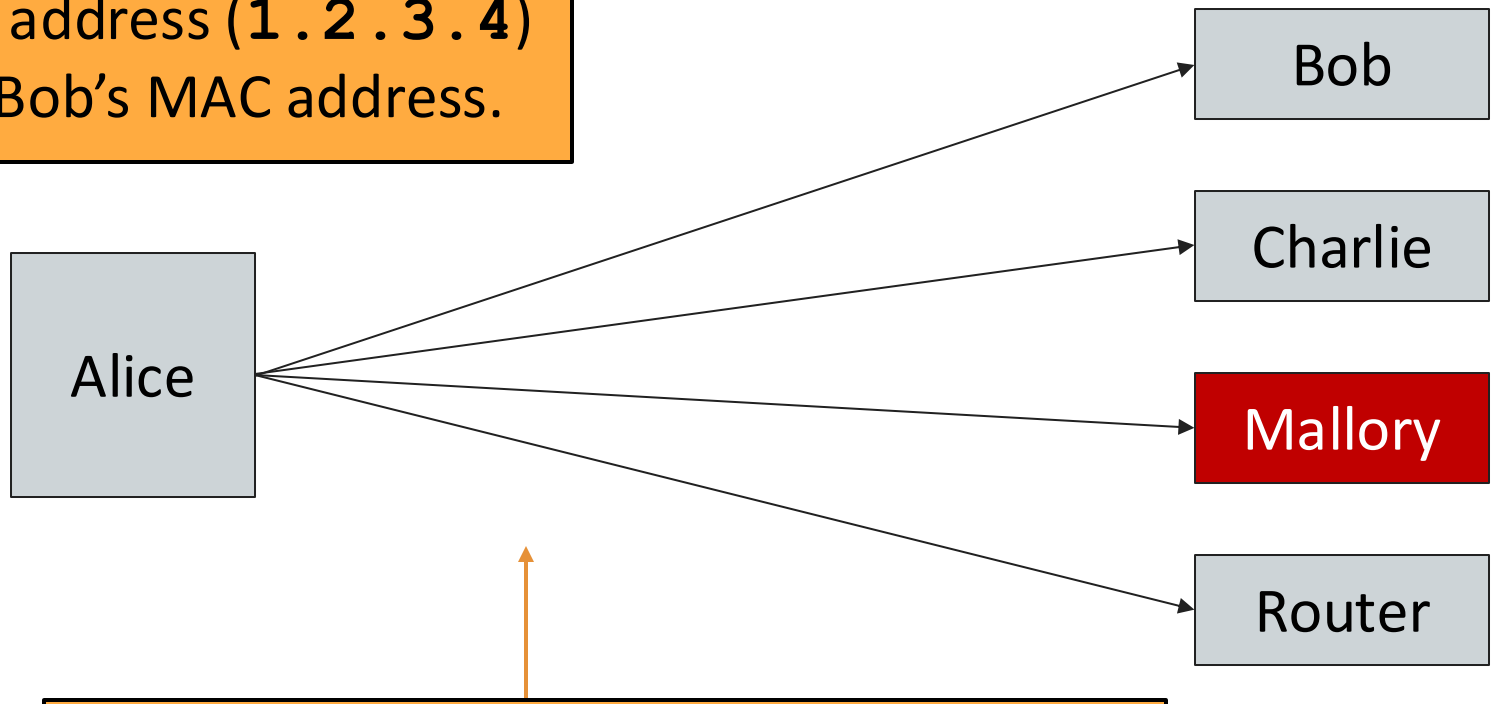
1. Alice checks her cache to see if she already knows the MAC address corresponding to `1.2.3.4`.

Since her cache is empty, she must make a request to find out.

Attacks on ARP

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC

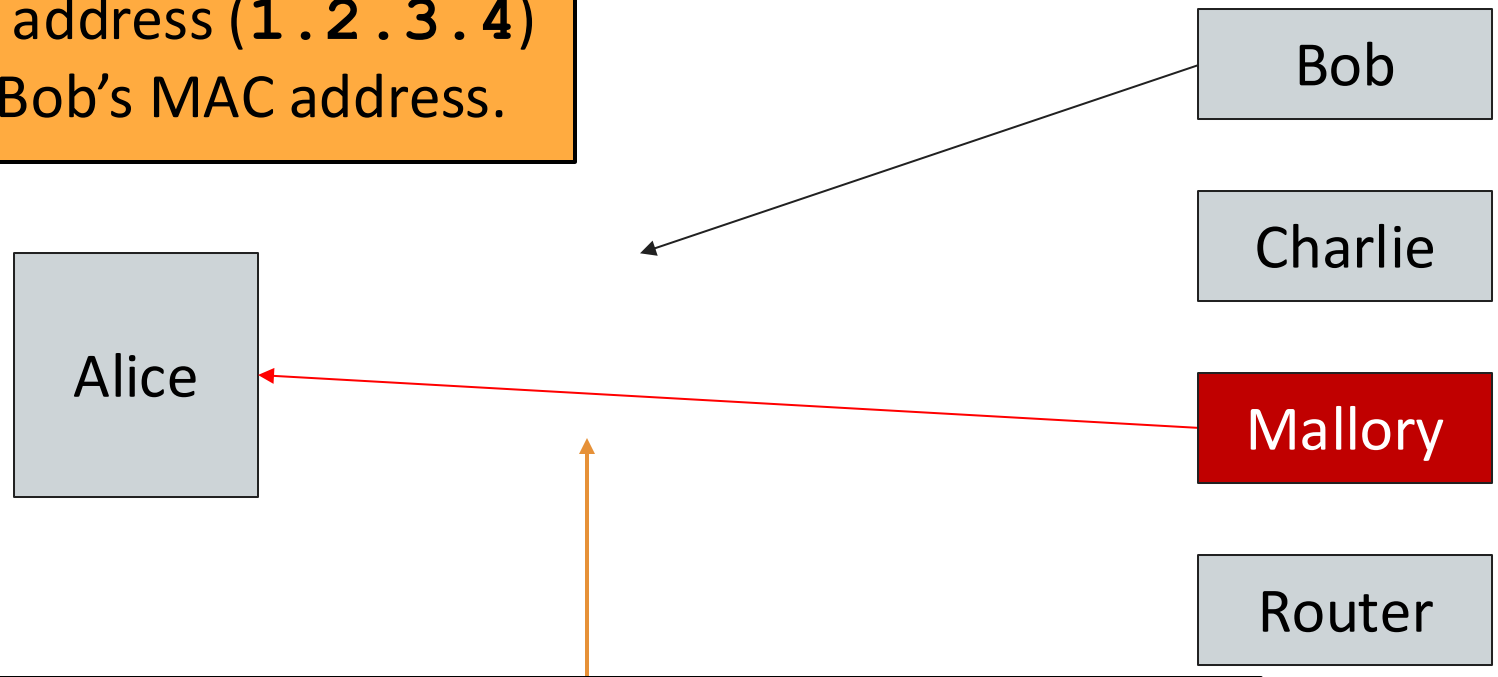


2. Alice asks everyone else on the local network: "What is the MAC address of `1.2.3.4`?"

Attacks on ARP

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC



3. Before Bob's response can arrive, Mallory sends a malicious response: "My IP is `1.2.3.4` and my MAC address is `66:66:66:66:66:66`."

Attacks on ARP

Alice knows Bob's IP address (**`1.2.3.4`**) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC
`1.2.3.4`	`66:66:66:66:66:66`

Alice

Bob

Charlie

Mallory

Router

4. Alice adds Mallory's malicious MAC address to her cache for Bob's IP addr!

Attack: ARP Spoofing

- Alice has no way of verifying the ARP response
- Alice is only expecting one machine to respond, so she will accept the first response
  - **Race condition**: As long as the attacker responds faster, the requester will accept the attacker's response

- ARP spoofing requires Mallory to be in the same LAN as Alice
- ARP spoofing lets Mallory become a man-in-the-middle (MITM)
  - Alice thinks that Bob's MAC address is **`66:66:...:66`** (Mallory's MAC address)
  - When Alice sends a message to Bob, she is actually sending the msg to Mallory
  - Mallory can modify the message and then send the modified message to Bob

ARP Spoofing: Defenses

- Repeater Hubs vs. Switches

- Use **switches** to avoid broadcasts and ARP requests
  - When Alice wants to msg Bob, she sends the msg to a switch on the LAN
  - The switch maintains a cache of IP <-> MAC mappings
  - If Bob's MAC address in the cache, the switch sends the msg directly to Bob
  - Otherwise, the switch broadcasts the message
- Benefits of switches
  - Efficiency: Fewer broadcast requests
  - Security: Reduces the number of messages broadcast to the entire LAN & isolation: can create "virtual" VLANs in software (guest Wifi vs. main Wifi)

Dynamic Host Configuration Protocol (DHCP)

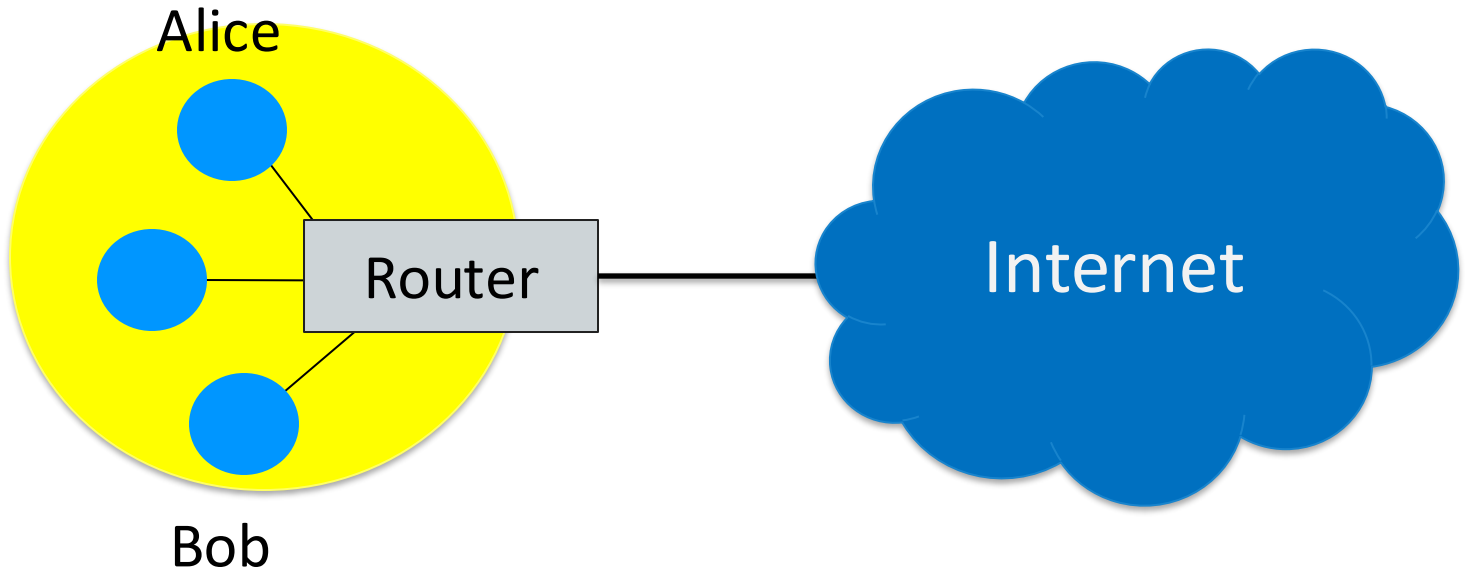
Coffee Shop

You go to a Coffee shop and want to use the Wifi

Wait… I don't have an IP address to send/recv data. *How do I get one?*

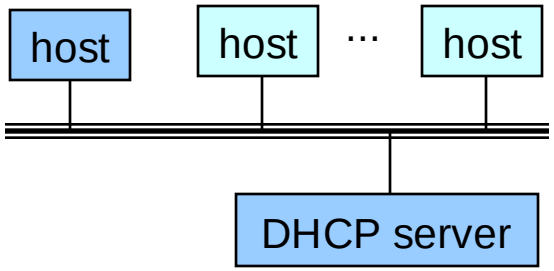
DHCP: Initial Network Configuration

- To connect to a network, a user needs:
  - An IP address so that other people can contact the user
  - The IP address of the router (gateway) so that the user can contact machines outside of the LAN
  - The IP address of the DNS server (future lectures)



DHCP: Initial Network Configuration

- New host connecting to network doesn't have an IP address yet
  - So, host doesn't know what source address to use
- Host doesn't know *who to ask* for an IP address
  - So, host doesn't know what destination address to use
- Solution: *shout* to "**discover**" server that can help
  - Broadcast a server-discovery message (layer 2)
  - DHCP Server(s) sends a reply offering an address & config details



DHCP = Dynamic Host Configuration Protocol

Steps of the DHCP Handshake (Protocol)

1. **Client Discover:** The client broadcasts a request for a configuration
2. **DHCP Offer**: Any DHCP server can respond with a configuration offer
   - Usually only one DHCP server responds, but can be multiple
   - The offer includes an IP address for the client & additional info (DNS server + gateway)
   - The offer also has an expiration time (how long the user can use this configuration)
3. **Client Request**: The client broadcasts which configuration it has chosen
   - If multiple DHCP servers made offers, the ones that weren't chosen discard their offer
   - The chosen DHCP server gives the offer to the client
4. **DHCP Acknowledgement**: The chosen server confirms that its configuration has been given to the client

Dynamic Host Configuration Protocol (DHCP)

Alice's configuration	
My IP	???
DNS Server	???
Gateway	???

Alice

Bob

DHCP Server 1

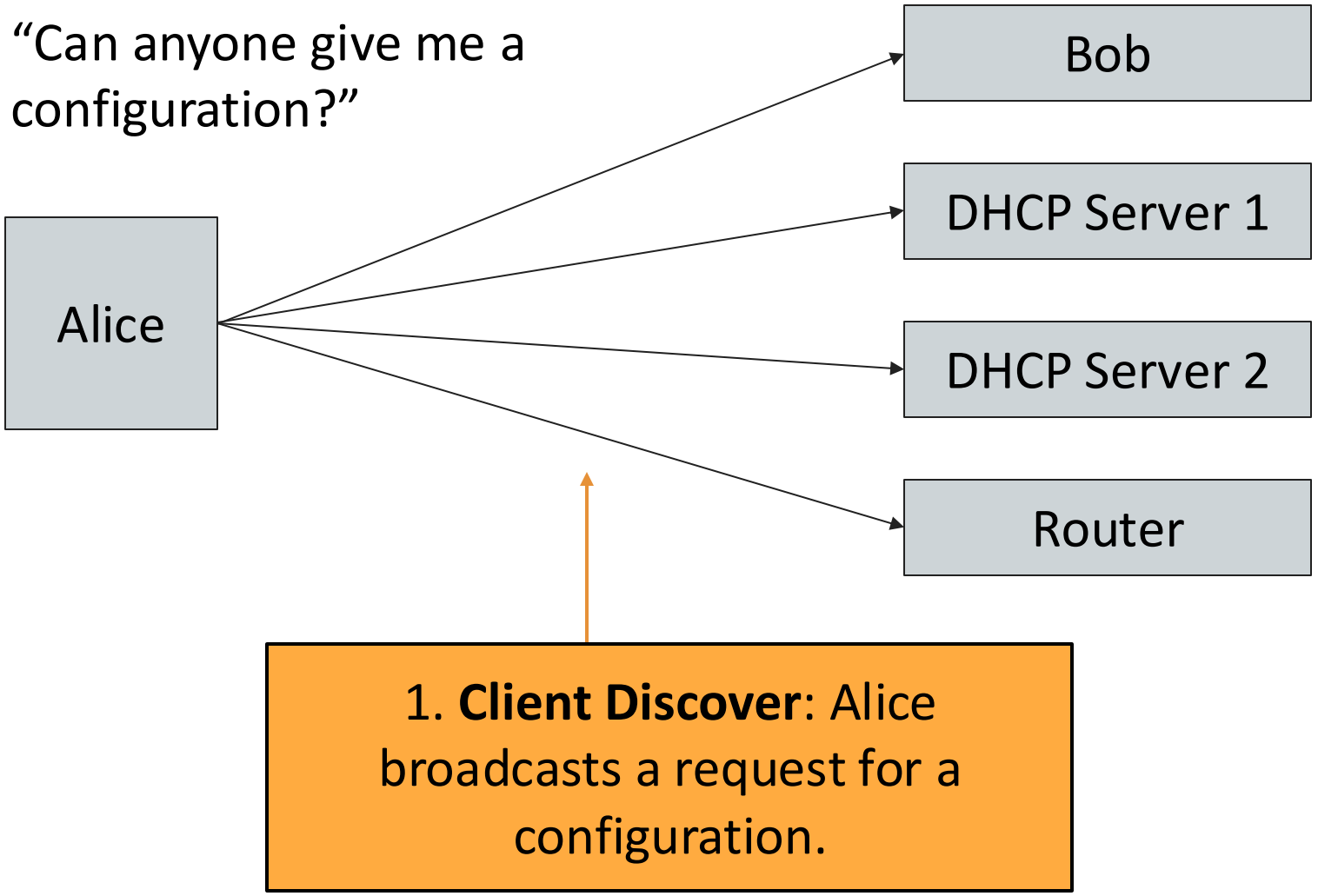
DHCP Server 2

Router

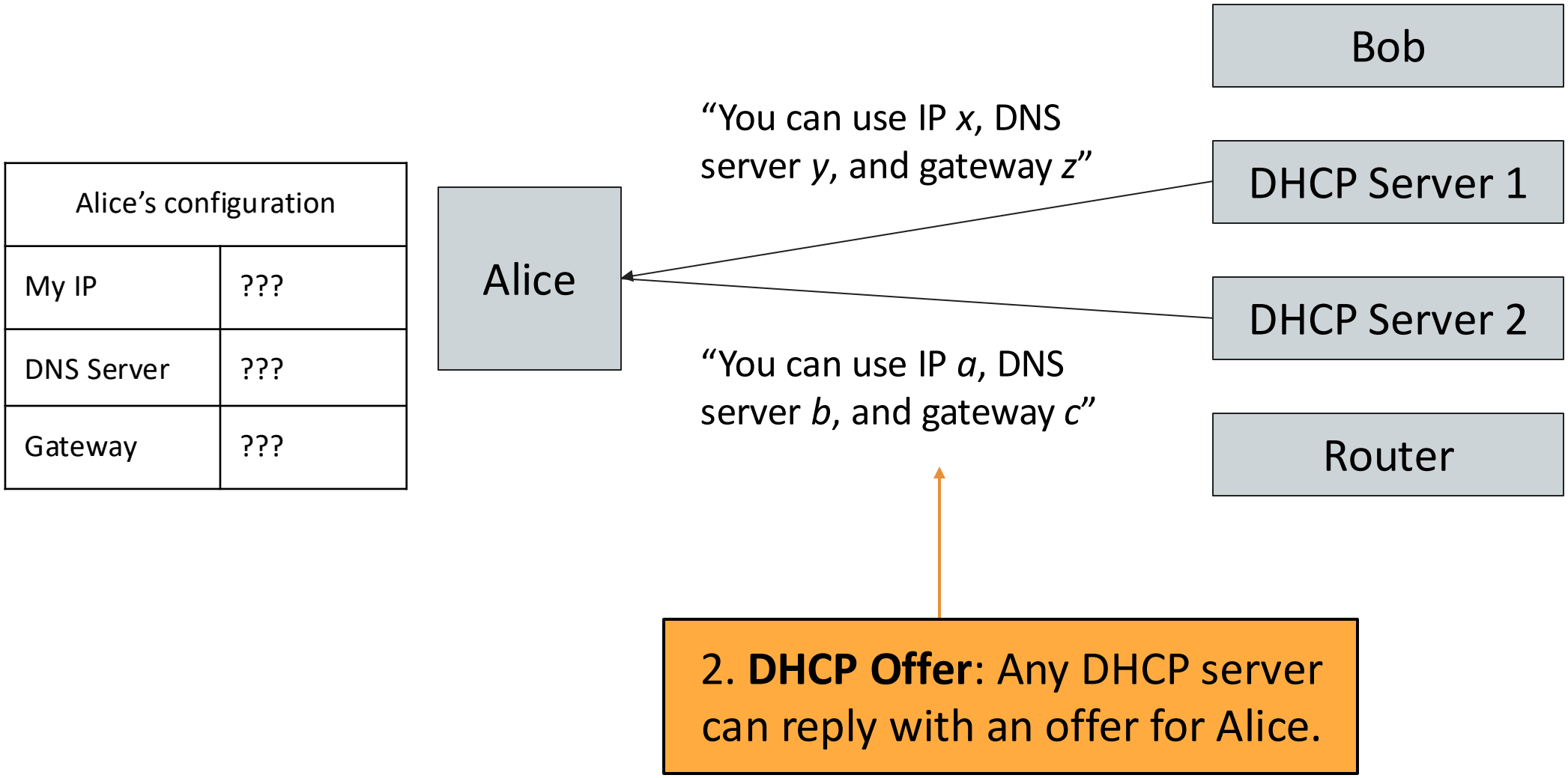
Alice wants to connect to the network, but she's missing a configuration.

Dynamic Host Configuration Protocol (DHCP)

Alice's configuration	
My IP	???
DNS Server	???
Gateway	???

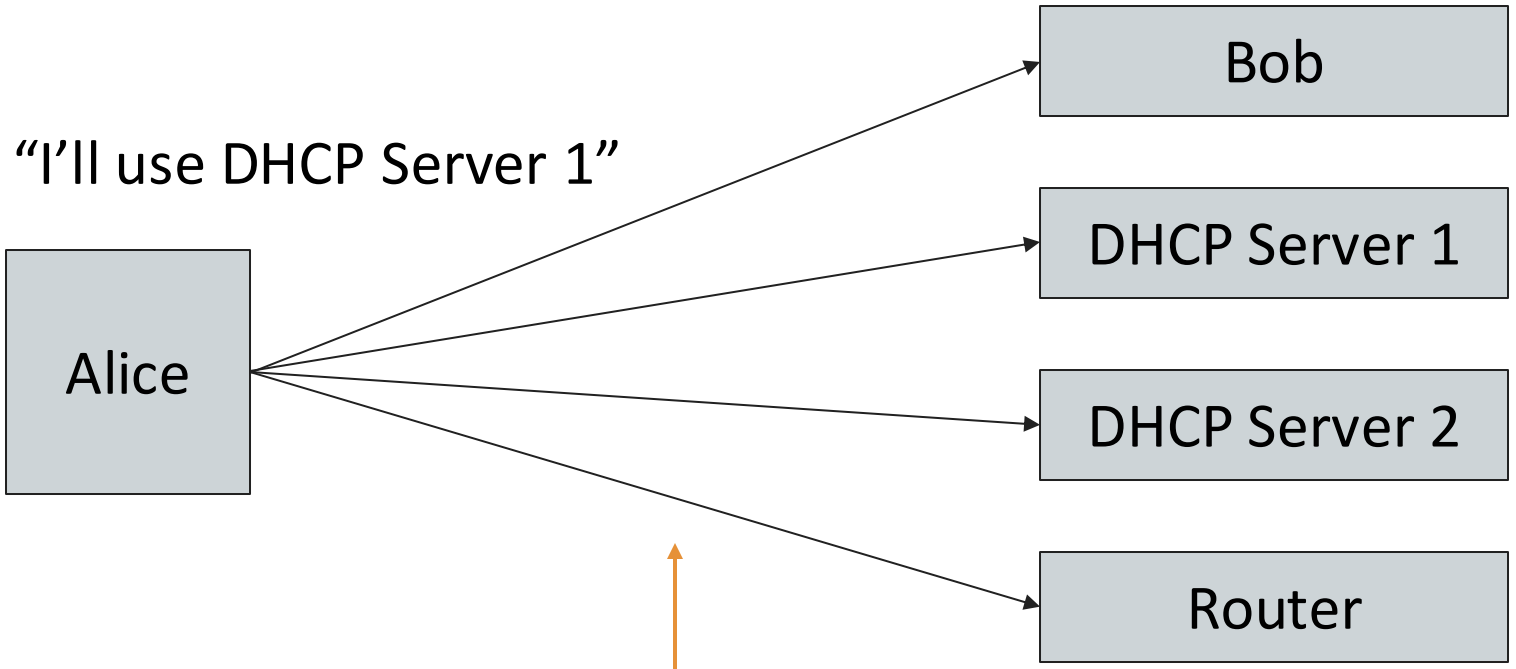


Dynamic Host Configuration Protocol (DHCP)



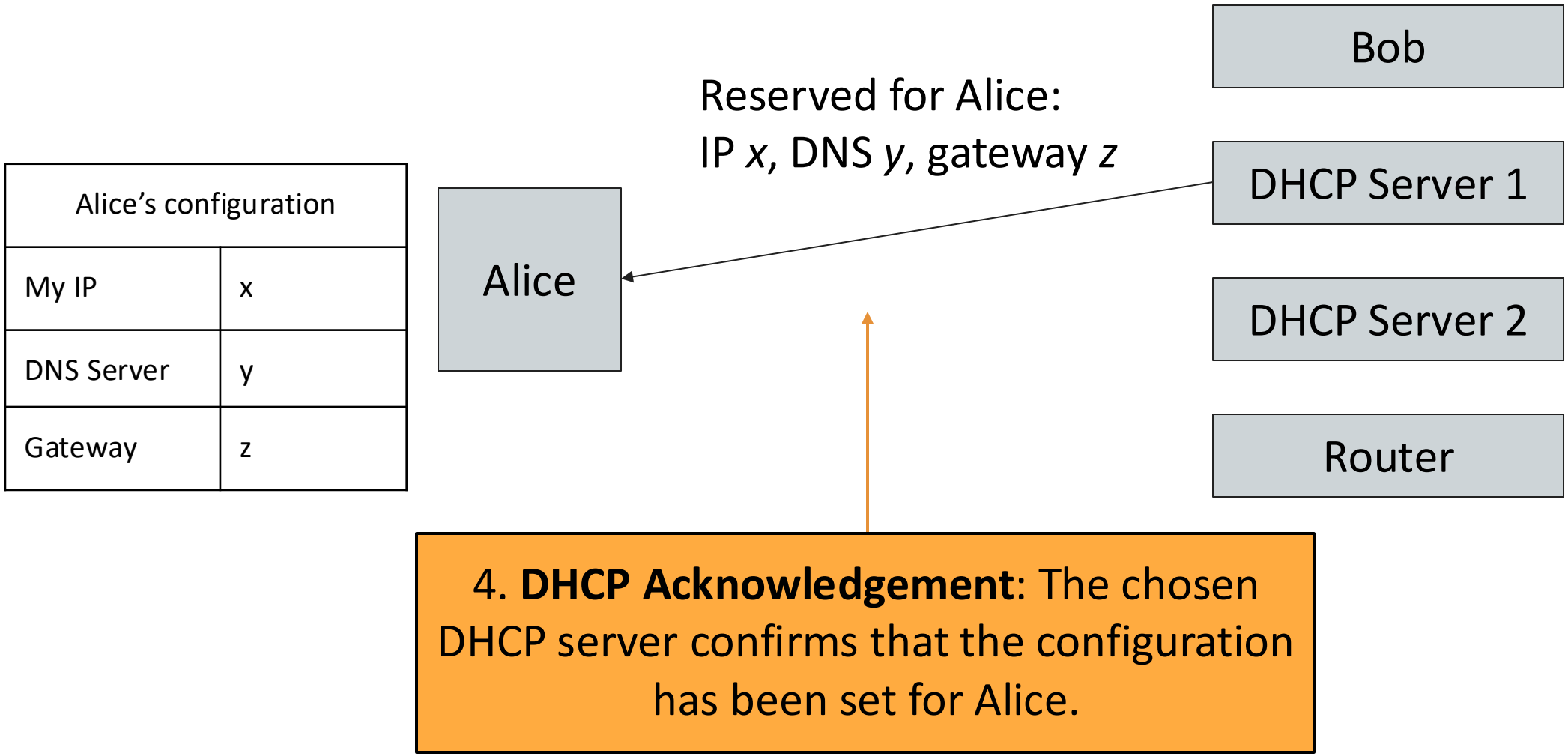
Dynamic Host Configuration Protocol (DHCP)

Alice's configuration	
My IP	???
DNS Server	???
Gateway	???



3. **Client Request**: Alice broadcasts which configuration she has chosen.

Dynamic Host Configuration Protocol (DHCP)



DHCP Attacks

Alice has no way of verifying the DHCP response

- Spoofing: Any attacker on the local network can claim to have a configuration

Alice usually expects only one DHCP server to respond, so she will accept the first response

- **Race condition**: If attacker responds faster, Alice accepts the attacker's response

DHCP attacks require Mallory to be in the same LAN as Alice

DHCP attacks let Mallory become a man-in-the-middle (MITM) attacker

- e.g., Mallory claims the gateway router's address is Mallory's address
  - When Alice tries to send a msg to rest of Internet, she actually sends it to Mallory
  - Mallory can modify the message before sending it to its destination

ARP and DHCP

- The attacks on ARP and DHCP are very similar
  - Spoofing: The attacker claims to have an answer
  - Race condition: The requester accepts the first response. As long as the attacker's response arrives first, it is accepted
- Main vulnerabilities
  - Broadcast protocols: Requests are sent to everyone on the LAN, so the attacker can see every request
  - No trust anchor: There is no way to verify that responses are legitimate

DHCP Defenses

- DHCP attacks are hard to defend against
- No root of trust: When we first connect, there's nobody we can trust
- Instead, we rely on defenses provided in higher layers (e.g., TLS, coming up in a future lecture)

Outline

- Networking Threat Models
- ARP/DHCP Security
- WPA2: Wifi security

Wi-Fi

- **ARP & DHCP:** Protocols for getting configuration / address info once a machine has joined a LAN
- **Wi-Fi**: layer 2 protocol that wirelessly connects machines in a LAN (sending packets b/t machines on a LAN)
  - Alternative is Ethernet, which uses wires to connect machines in a LAN
- Parts of a Wi-Fi network
  - **Access point**: A machine that will help you connect to the network
  - **SSID**: The name of the Wi-Fi network
  - Password: Optionally, a password to secure Wi-Fi communications

WPA2: Wi-Fi Security

- **Wi-Fi Protected Access 2** (**WPA2**): A protocol for securing Wi-Fi network communications with cryptography

- Design goals
  - Everyone with the Wi-Fi password can join the network
  - An attacker who ***does not know the Wi-Fi password*** cannot read or tamper with data sent over Wi-Fi
  - Messages sent over the network are encrypted with keys

WPA Handshake (Symmetric Key Sharing)

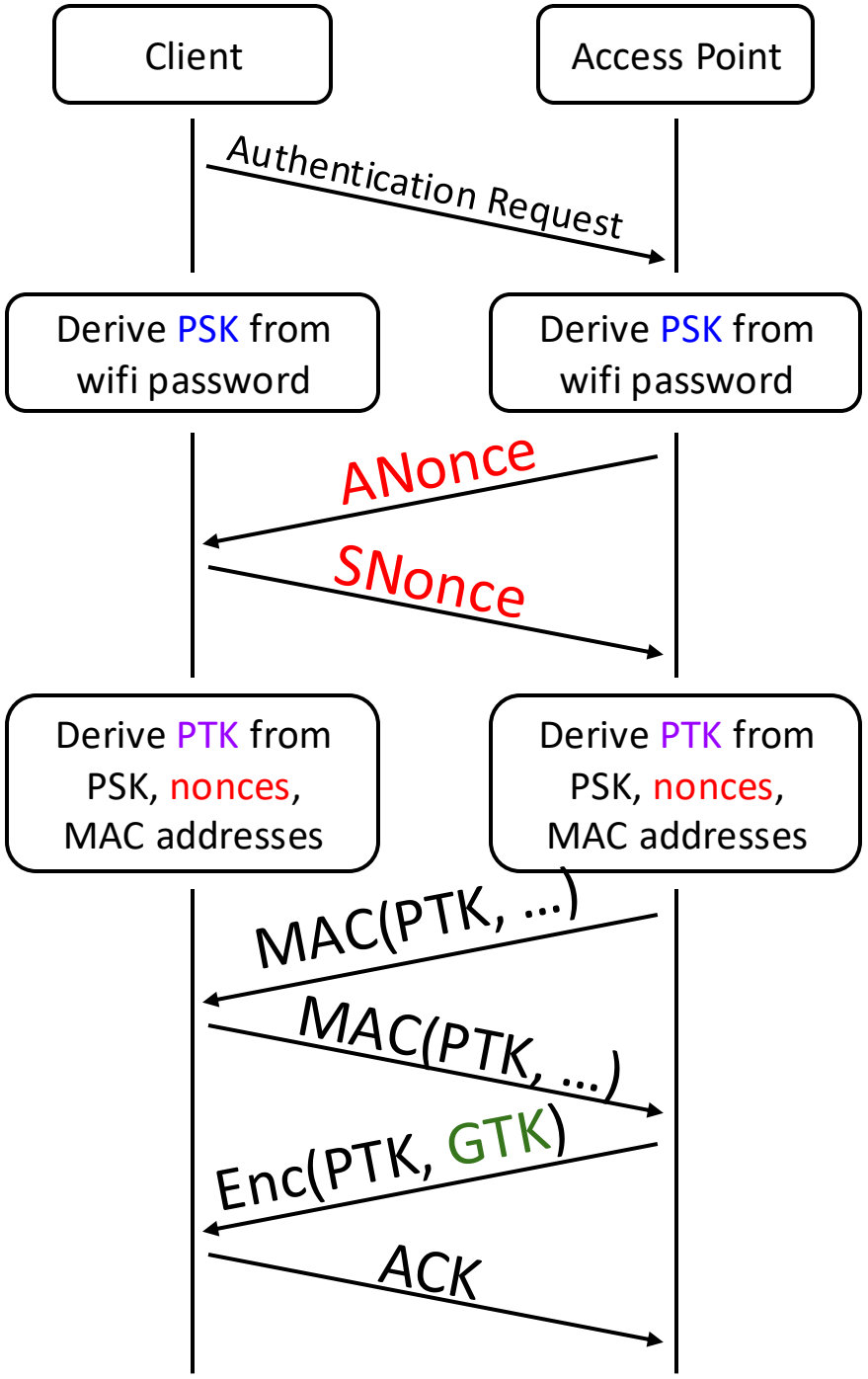
Password: $secret!

Client

Access Point

WPA Handshake (Symmetric Key Sharing)

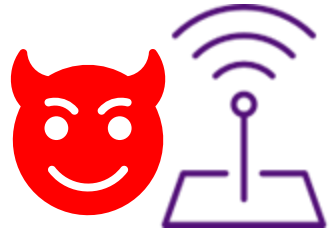
1. The client sends an authentication request to the access point
2. Both use the password to derive the *PSK* (pre-shared key)
3. Both exchange random nonces
4. Both use the *PSK*, nonces, and MAC addresses to derive the *PTK* (pairwise transport keys)
5. Both exchange MACs to ensure no one has tampered with the nonces, and that the PTK was correctly derived
6. The access point encrypts and sends the *GTK* (group temporal key) to the client, used for broadcasts that anyone can decrypt
7. The client acknowledges receiving the GTK



WPA Handshake: Establishing Shared Secret Key

- Both sides derive secret keys (*PTK*) for communication
  - Wi-Fi password → PSK
  - PSK + nonces + MAC addresses → PTK
  - The PTK is used to encrypt and authenticate all future communication
  - Note: The PTK is different for every user, because of the nonces
- The access point encrypts and sends the *GTK* to the client
  - The GTK is used for messages broadcast to the entire network (e.g., ARP, DHCP, etc.)
  - Everyone on the network uses the same GTK

WPA-PSK Attacks



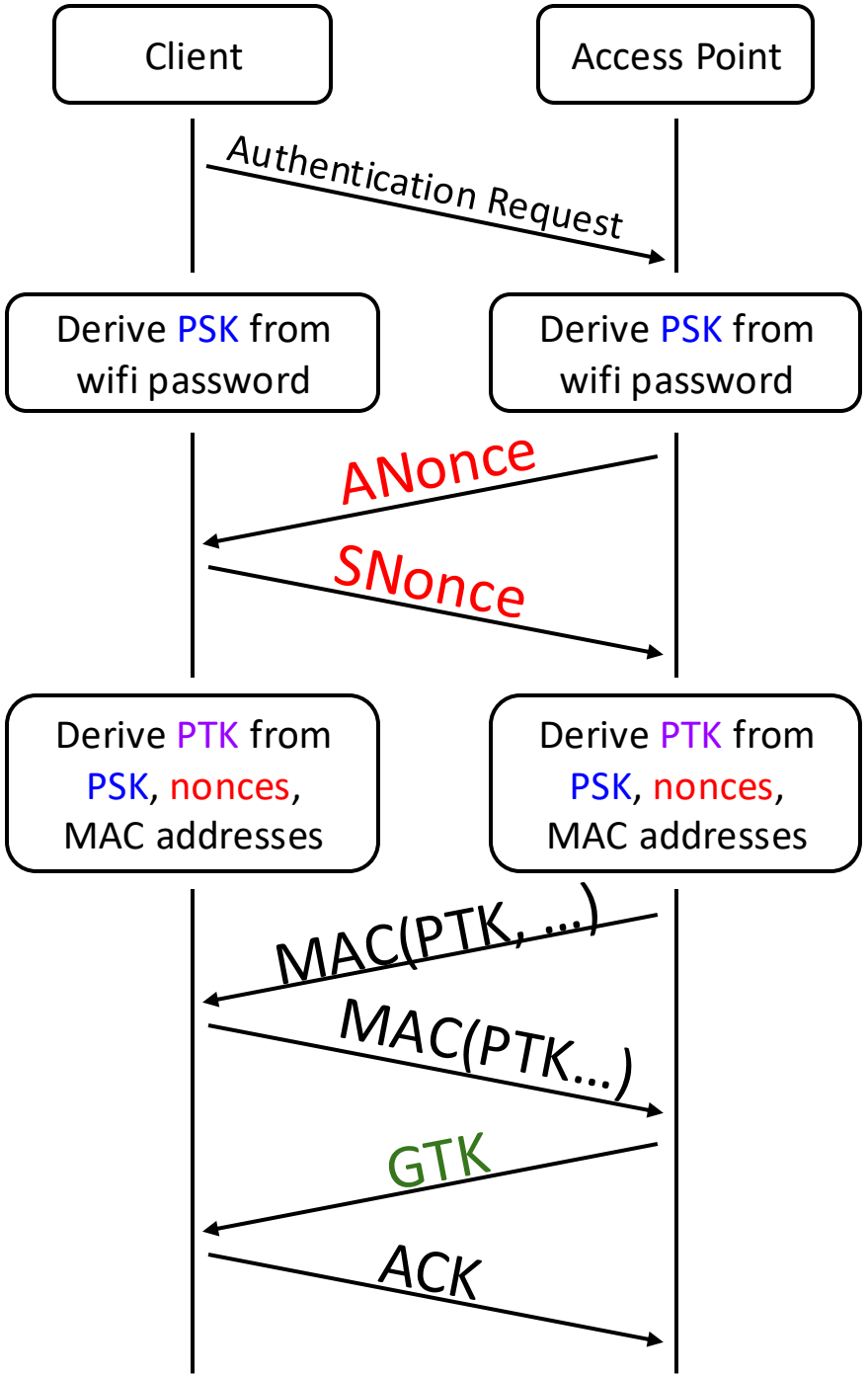
SSID: ORDWifi
Password: $secret!

Rogue Access Point (AP):
Pretend to be a valid AP, once client connects -> MITM Attacker

WPA-PSK Attacks

Eavesdropper already on Wi-Fi:

- All Wi-Fi msg's are broadcast
- Attacker can derive all keys & therefore decrypt/MAC everything correctly:
  - Wi-Fi password → *PSK*
  - Nonces are broadcast → *PTK*

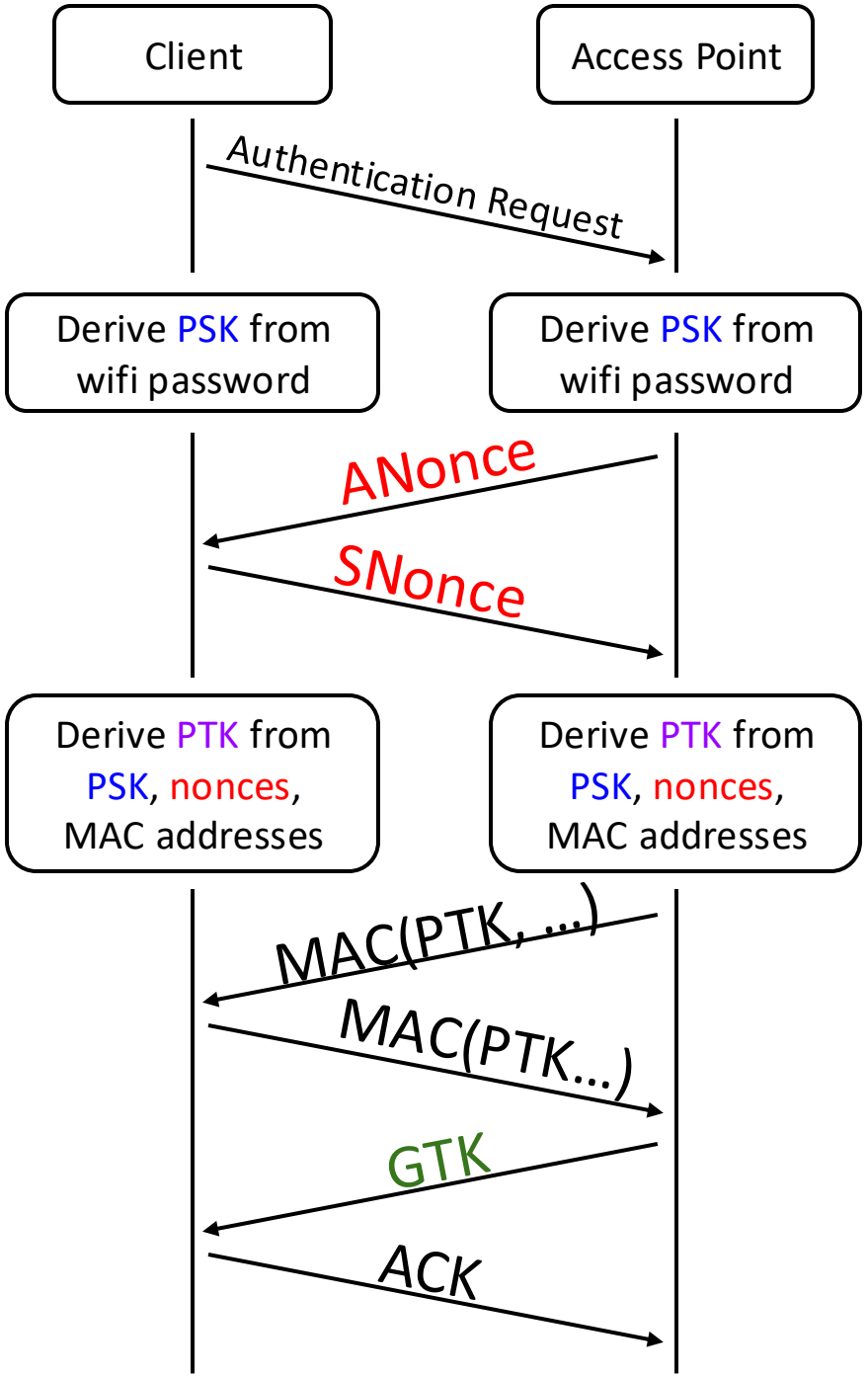


WPA-PSK Attacks

What about an attacker who doesn't know the Wi-Fi password?

Offline brute-force attack: People tend to choose bad passwords -> attacker can store past info to check if they guessed it

- Nonces are sent unencrypted, and client and AP MAC addresses are public
- Eavesdropper guesses a password and derives:
  - Wi-Fi password → *PSK*
  - *PSK* + nonces + MAC addresses → *PTK*
  - Eavesdropper checks: MAC from the guess matches the MAC that was sent?



WPA-Enterprise

- Core issue: Every client starts w/ the same *PSK* to derive *PTK*
  - Fix: Have each user use their own unique username + password
  - This is the model that eduroam use!
- Instead of using a PSK from common password, use a key generated (unique per user) randomly by an auth server
  - Authentication server has a digital certificate to prove legitimacy
  - Your machine first forms a secure channel to the authentication server, which lets you enter your username and password
  - If the username + password correct, auth server sends a one-time key to use instead of a PSK to both the client and the AP (over a separate secure channel)
- The rest of the handshake proceeds normally

WPA-Enterprise Attacks

- WPA Enterprise defends against the previous attacks
  - **Rogue AP attack**: The APs must authenticate themselves to the server, which the attacker can't do
  - **Other Wi-Fi users:** Every user has unique PSK & derives unique session keys (PTK's)
  - **Brute-force attack**: The generated PSK replacement is long and random, too long to brute-force
- However, it is still vulnerable to attacks such as ARP or DHCP spoofing

Outline

- Networking Threat Models
- ARP/DHCP Security
- WPA2: Wi-Fi security