CMSC414 Computer and Network Security

Low Level Network Attacks

Yizheng Chen | University of Maryland
surrealyz.github.io

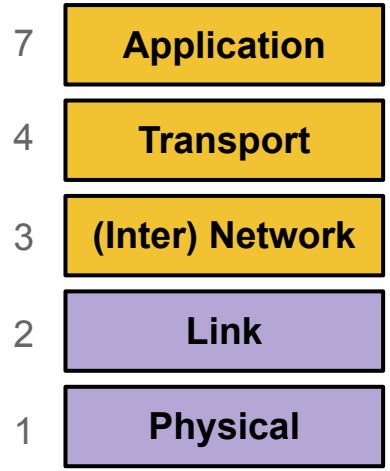
Apr 23, 2024

Credits: original slides from instructors and staff from CS161 at UC Berkeley. Blue slides will not be tested.

Last Time: Intro to Networking

- Internet: A global network of computers
  - Protocols: Agreed-upon systems of communication

- OSI model: A layered model of protocols
  - Layer 1: Communication of bits
  - Layer 2: Local frame delivery
    - Ethernet protocol
    - MAC addresses (6-byte)
  - Layer 3: Global packet delivery
    - IP protocol
    - IP addresses (4-byte or 16-byte)
  - Layer 4: Transport of data
  - Layer 7: Applications and services



Today: Low-Level Network Attacks

- Threat Model: Network Attackers
  - Man-in-the-middle attacker
  - On-path attacker
  - Off-path attacker
- ARP: Translate IP addresses to MAC addresses
- WPA: Communicate securely in a wireless local network
- DHCP: Get configurations when first connecting to a network

Types of Network Attackers

- Threat model: There are 3 types of attackers we'll consider

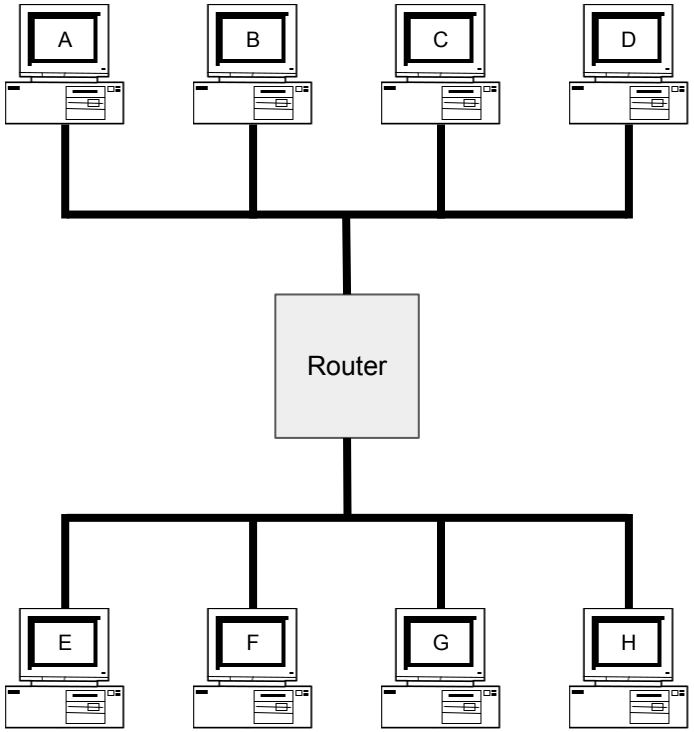
	Can modify or delete packets	Can read packets
Man-in-the-middle attacker	✓	✓
On-path attacker		✓
Off-path attacker		

Spoofing

- Anybody can send their own packets through the network
- **Spoofing**: Lying about the identity of the sender
  - Example: Mallory sends a message and says the message is from Alice
  - The attacker can lie about the *source address* in the packet header
- All types of attackers can spoof packets

Review: Layer 2 and Layer 3

- Local area network (LAN): A set of machines connected in a local network
  - The MAC identifies devices on layer 2
- Internet protocol (IP): Many LANs connected together with routers
  - The IP identifies devices on layer 3

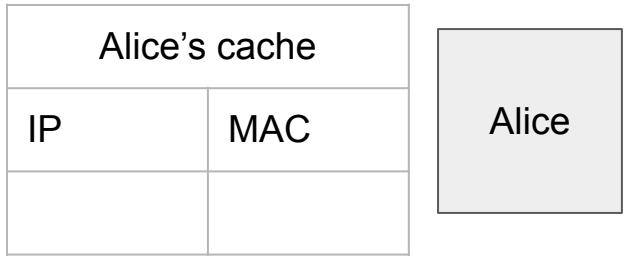


Address Resolution Protocol (ARP)

- **ARP**: Translates layer 3 IP addresses to layer 2 MAC addresses
  - Example: Alice wants to send a message to Bob on the local network, but Alice only knows Bob's IP address (`1.2.3.4`). To use layer 2 protocols, she must learn Bob's MAC address.

Address Resolution Protocol (ARP)

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



Alice

Bob

Charlie

Dave

Router

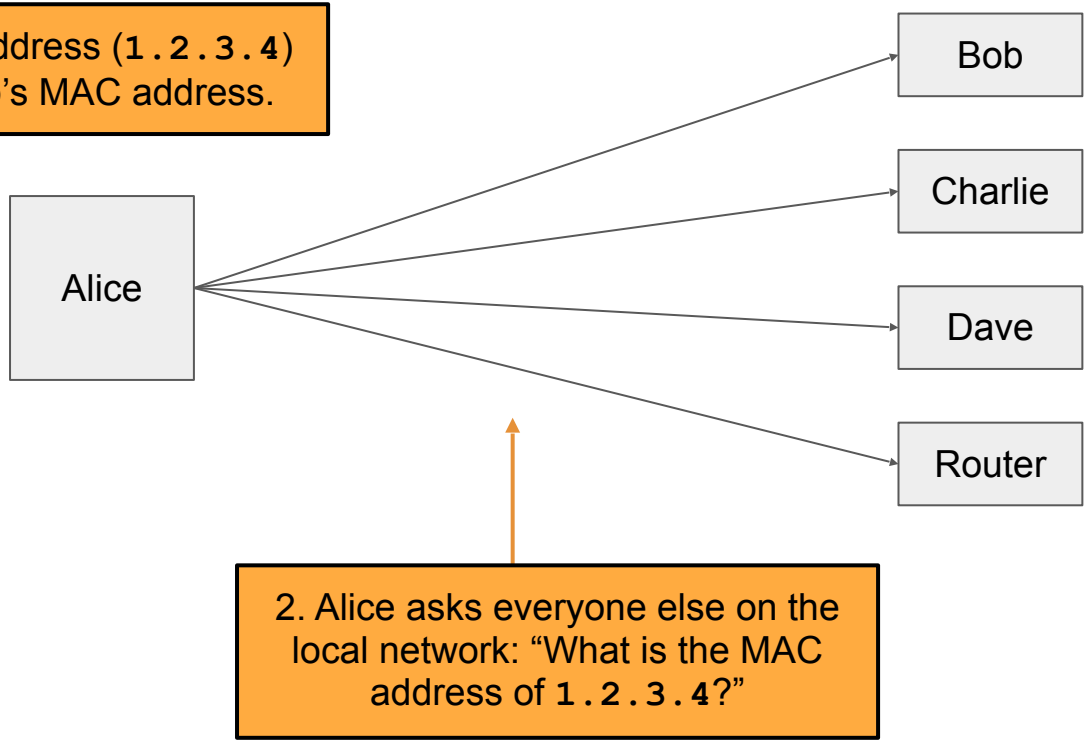
1. Alice checks her cache to see if she already knows the MAC address corresponding to `1.2.3.4`.

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

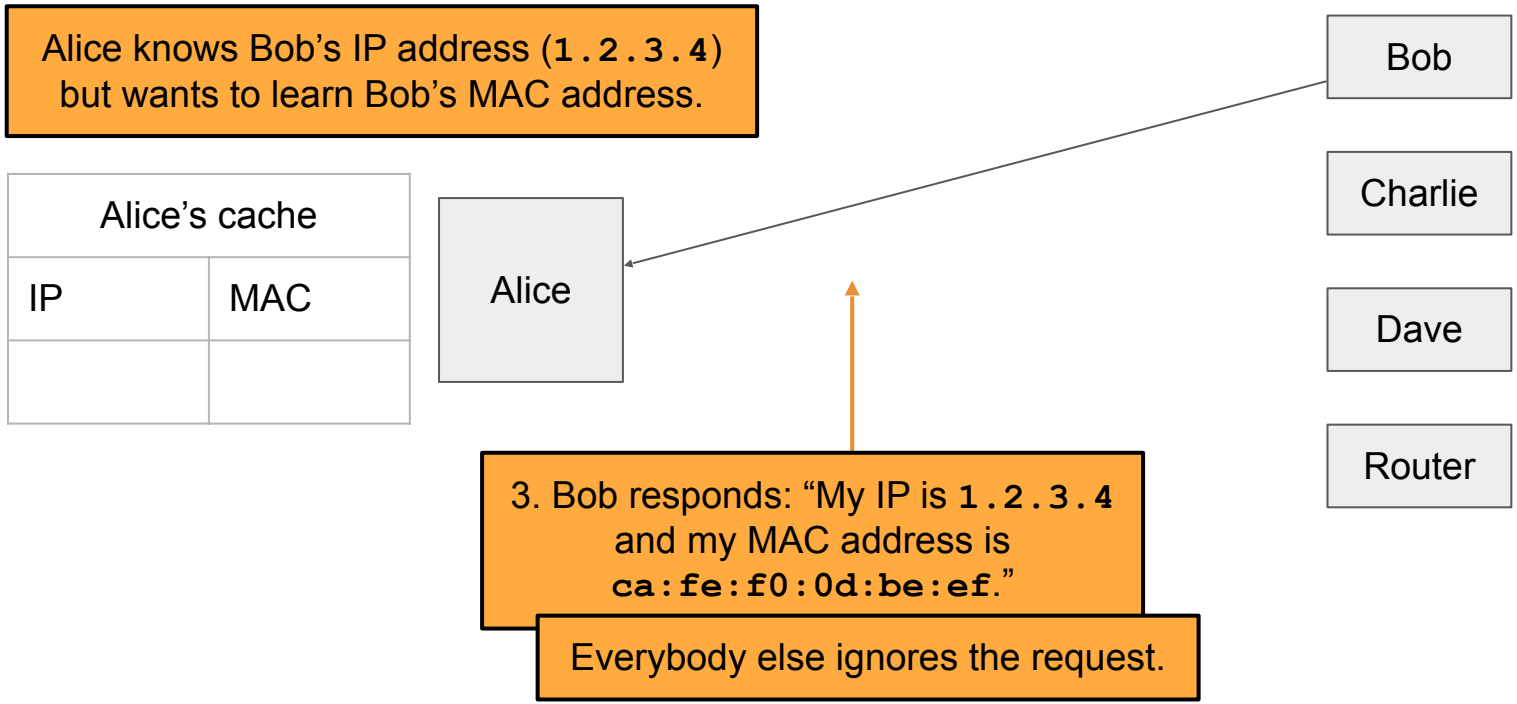
Address Resolution Protocol (ARP)

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)



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.

Address Resolution Protocol (ARP)

- Steps of the protocol
  1. Alice checks her cache to see if she already knows Bob's MAC address.
  2. If Bob's MAC address is 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.

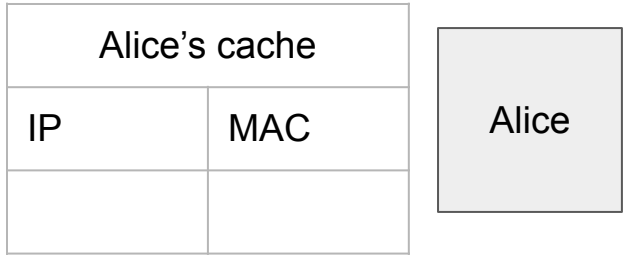
Address Resolution Protocol (ARP)

- If Bob is outside of the LAN, the router will respond with its 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
  - Alternatively, if Alice knows what addresses belong to the LAN, she will request the router's IP

- All received ARP replies are cached, even if no request was sent

Attacks on ARP

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



Alice

Bob

Charlie

Mallory

Router

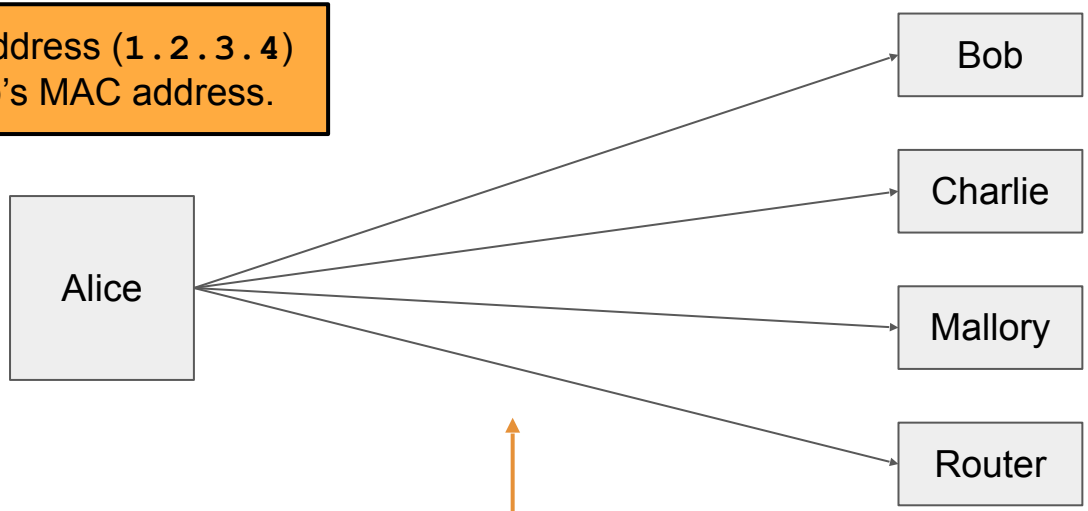
1. Alice checks her cache to see if she already knows the MAC address corresponding to `1.2.3.4`.

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

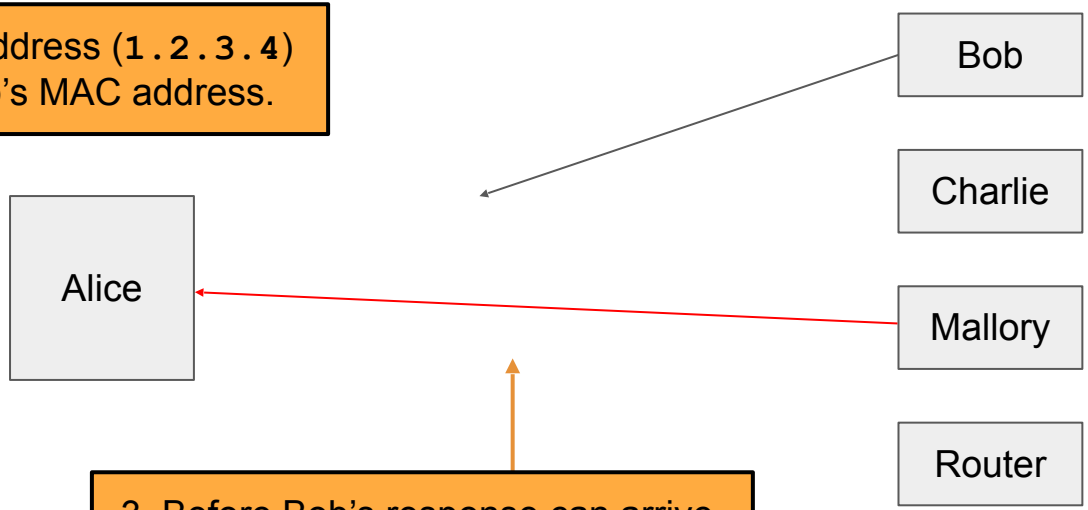


2. Alice asks everyone else on the local network: "What is the MAC address of `1.2.3.4`?"

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 address to her cache.

Attack: ARP Spoofing

- Alice has no way of verifying the ARP response
  - Spoofing: Any attacker on the network can claim to have the requested IP address
- 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) attacker
  - When Alice sends a message to Bob, she is actually sending the message to Mallory
  - Mallory can modify the message and then send the modified message to Bob
  - Alice thinks that Bob's MAC address is `66:66:66:66:66:66` (Mallory's MAC address)

ARP Spoofing: Defenses

- Use **switches** to avoid broadcasts and ARP requests
  - When Alice wants to send a message to Bob, she sends the message to a switch on the LAN
  - The switch maintains a cache of IP/MAC mappings
  - If Bob's MAC address is in the cache, the switch sends the message directly to Bob
  - Otherwise, the switch broadcasts the message

- Benefits of switches
  - Security: Reduces the number of messages broadcast to the entire LAN
  - Efficiency: Fewer broadcast requests means more requests can be sent per second
  - Isolation: Smarter switches implement virtual local area networks (VLANs), which split a LAN into several isolated parts
    - One part of the VLAN cannot directly interact with other parts of the VLAN

- Tools like **`arpwatch`** track ARP responses and make sure that there is no suspicious activity

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 DNS server to look up IPs of domain names
  - The IP address of the router (gateway) to contact machines outside of the LAN

- The first time a user connects, they don’t have this information yet
  - The user also doesn’t know who to ask for this information

- **DHCP** gives the user a configuration when they first join the network

Dynamic Host Configuration Protocol (DHCP)

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

Alice

Bob

DHCP Server 1

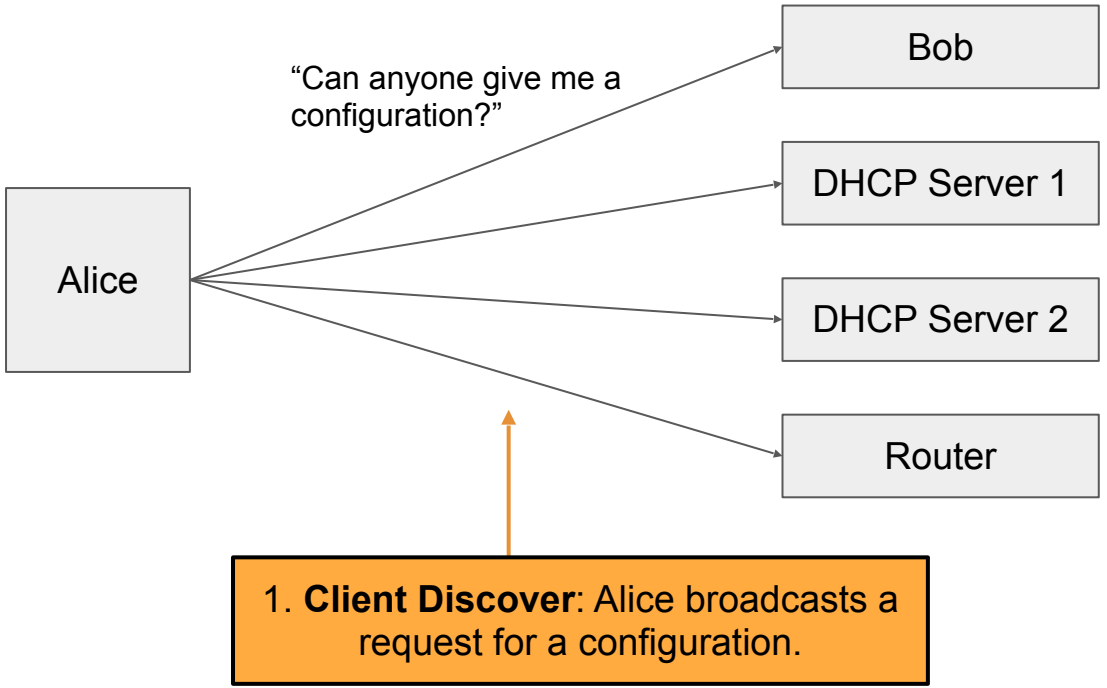
DHCP Server 2

Router

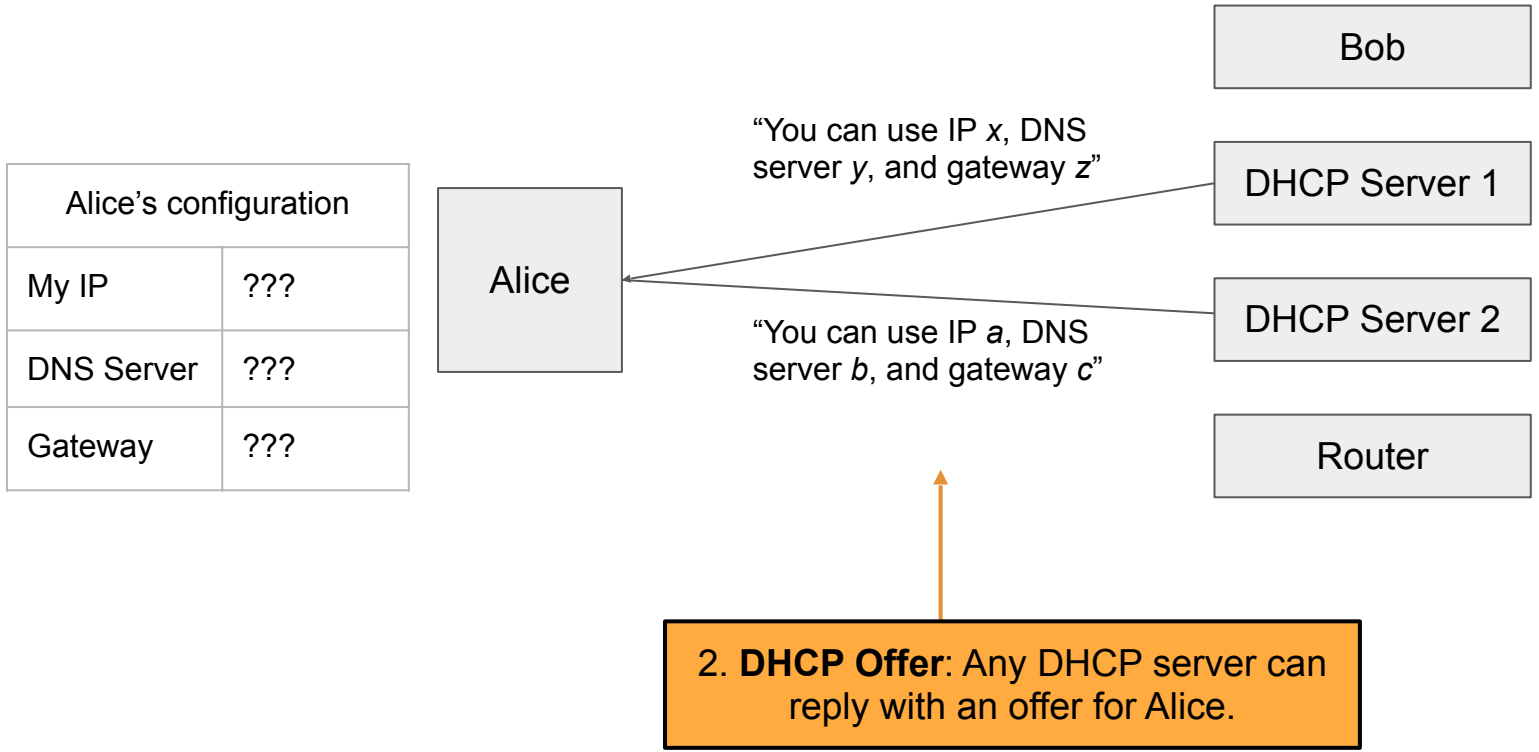
Alice wants to connect to the network, but she's missing a configuration.

Dynamic Host Configuration Protocol (DHCP)

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

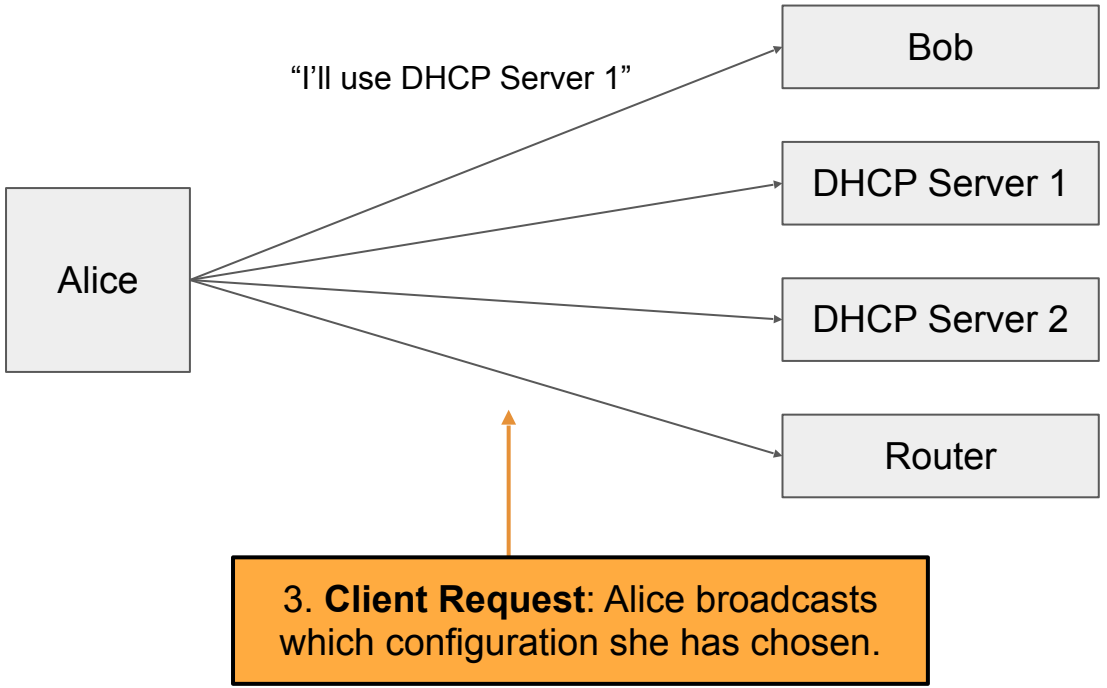


Dynamic Host Configuration Protocol (DHCP)

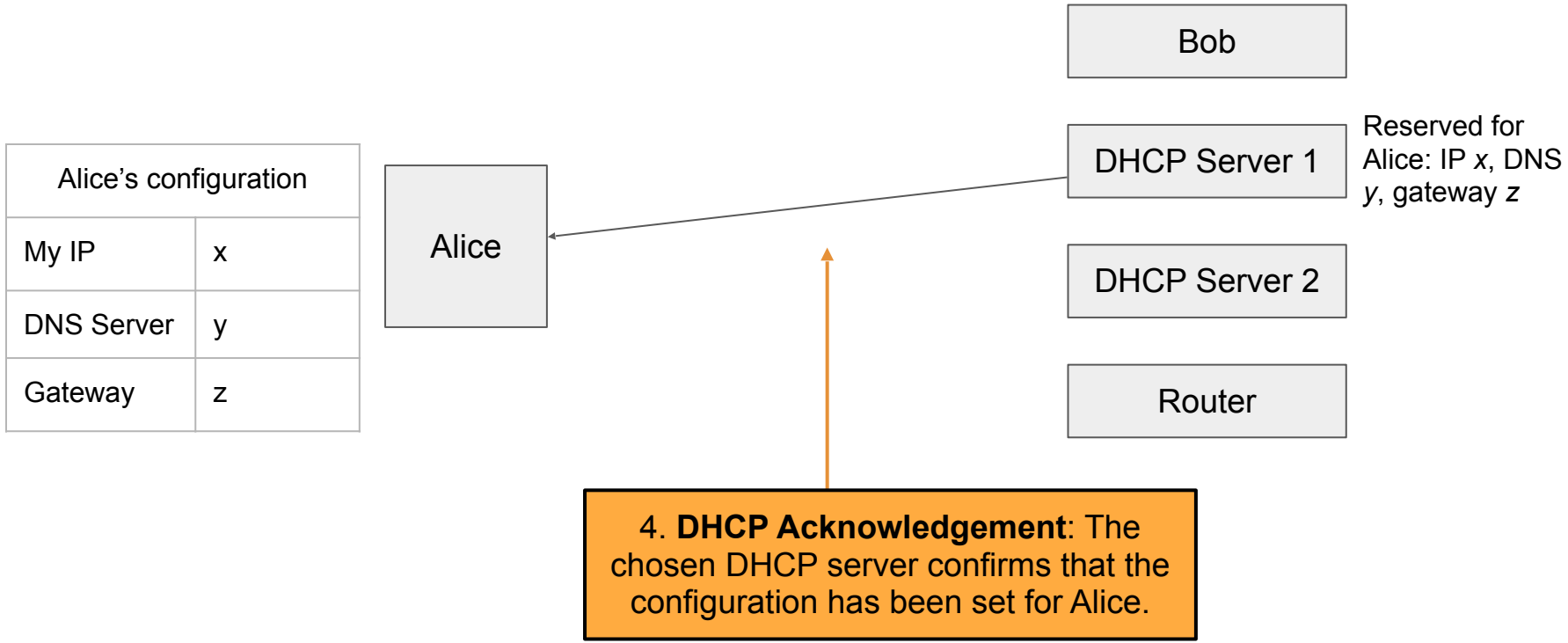


Dynamic Host Configuration Protocol (DHCP)

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



Dynamic Host Configuration Protocol (DHCP)



Steps of the DHCP Handshake

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
    - The offer includes an IP address for the client, the DNS server's IP address, and the (gateway) router's IP address
    - 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 were not 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

DHCP Attacks

- Alice has no way of verifying the DHCP response
  - Spoofing: Any attacker on the 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**: As long as the attacker responds faster, Alice will accept 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
  - Mallory claims the gateway router's address is Mallory's address
    - When Alice sends a message to the rest of the Internet, she actually sends it to Mallory
    - Mallory can modify the message before sending it to its destination
  - Mallory can also claim the DNS server's address is Mallory's address

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 is 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

Wi-Fi

- **Wi-Fi**: A layer 2 protocol that wirelessly connects machines in 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** (service set identifier): The name of the Wi-Fi network
  - Password: Optionally, a password to secure Wi-Fi communications

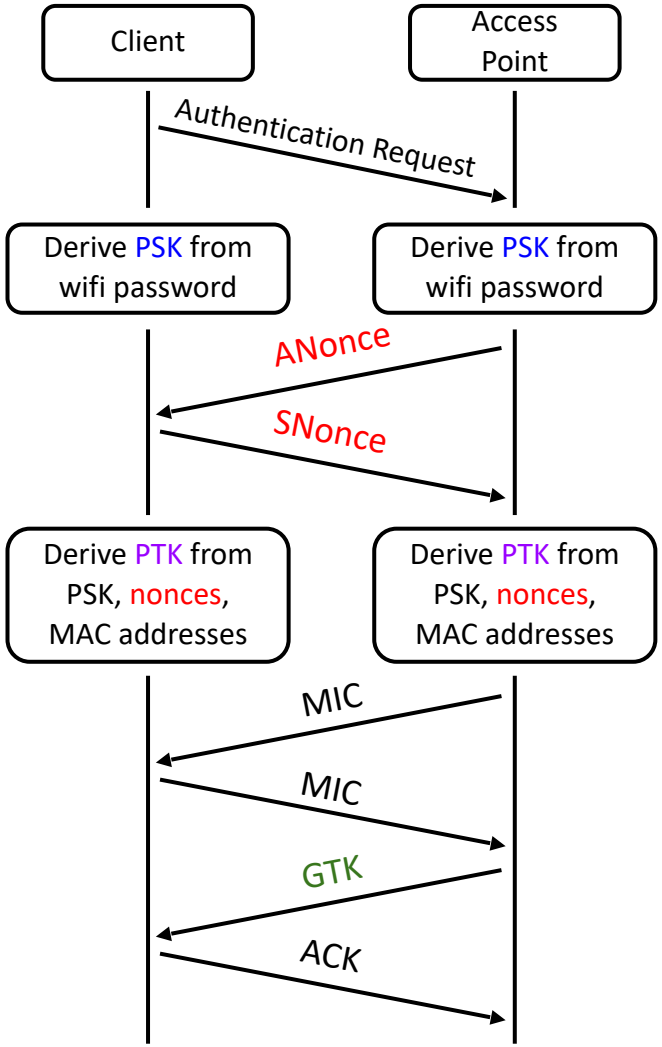
WPA2

- **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
  - Messages sent over the network are encrypted with keys
  - An attacker who does not know the Wi-Fi password cannot learn the keys

WPA Handshake

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 MICs (Message Integrity Check, these are MACs from the crypto unit) 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



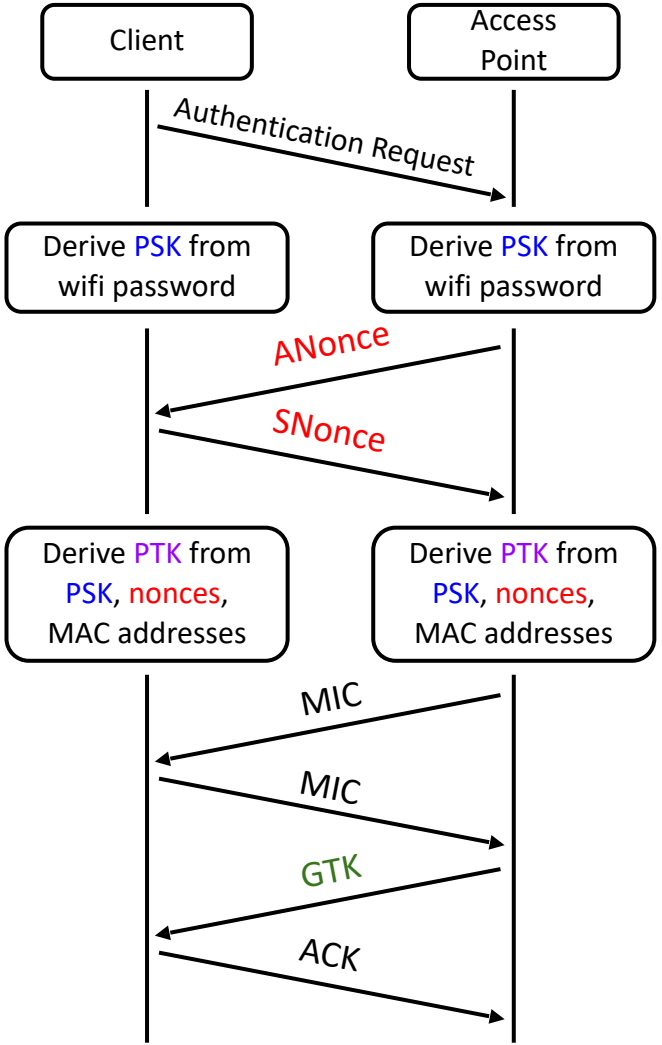
WPA Handshake

- Both sides derive secret keys 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
  - Everyone on the network uses the same GTK

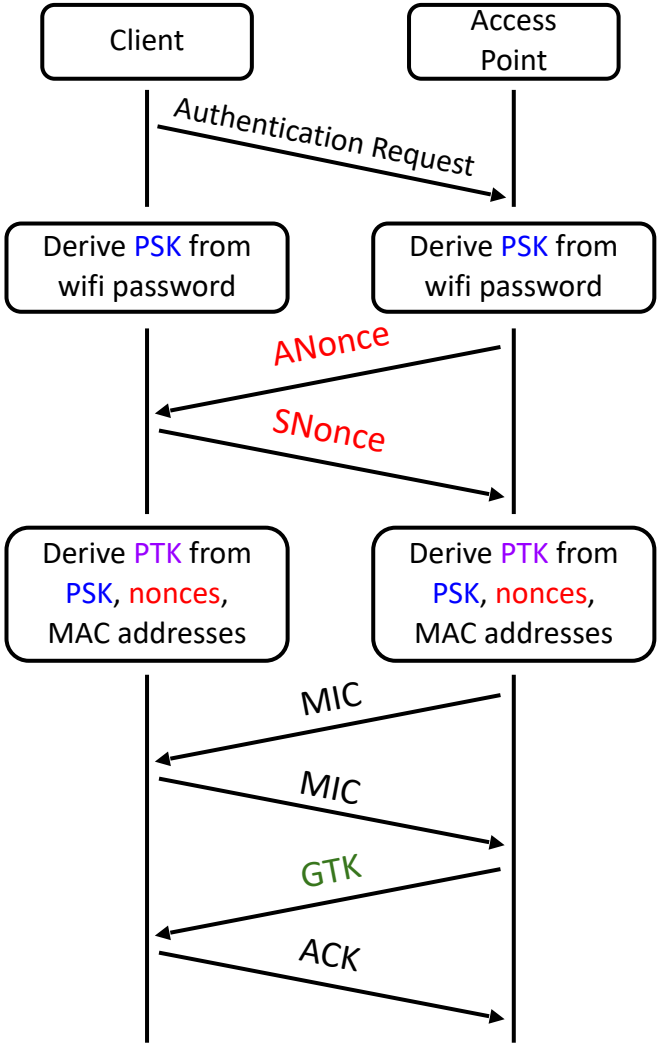
WPA-PSK Attacks

- **Rogue AP**: Pretend to be an AP, and offer your own *ANonce* to the client
  - If you know the password/PSK, you can complete the handshake with the client and become a MITM!



WPA-PSK Attacks

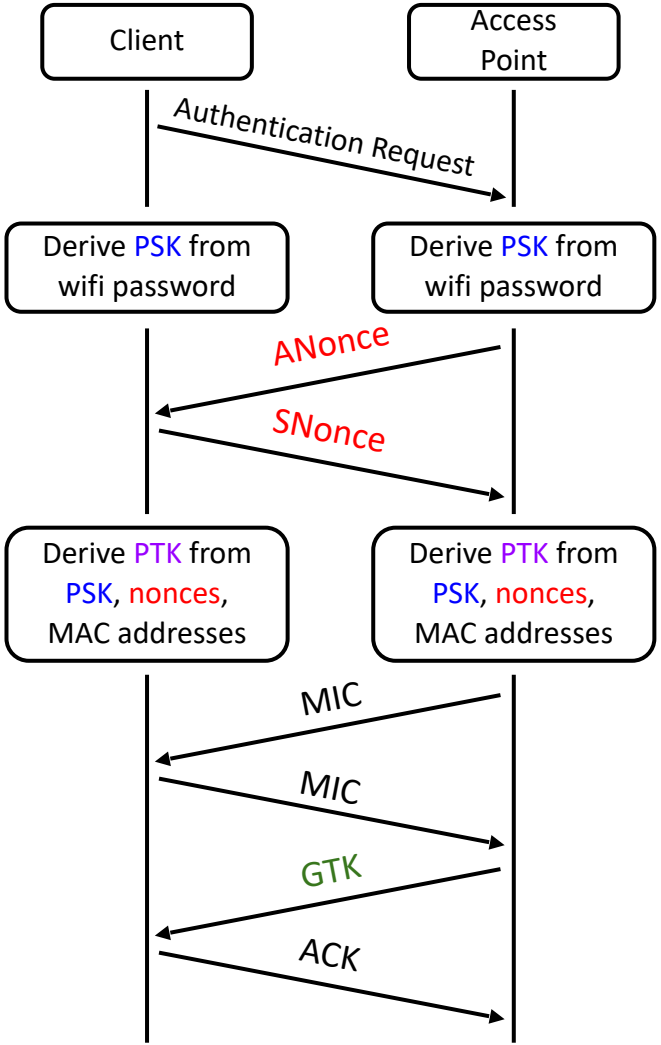
- **Offline brute-force attack**: People tend to choose bad passwords, and you have enough information to know if you guessed the password correctly
  - Nonces are sent unencrypted, and client and AP MAC addresses are public
  - Eavesdropper guesses a password and derives:
    - Wi-Fi password → *PSK*
    - *PSK* + nonces + MAC addresses → *PTK*
    - Eavesdropper checks that the MIC from the guess matches the MIC that was sent



WPA-PSK Attacks

- **Forward Secrecy:** Compromising a long-term key should not compromise past session keys

- **No forward secrecy**: An eavesdropper who records the values of *ANonce* and *SNonce* can derive the key if they later learn the password or *PSK*
  - Compare to Diffie-Hellman: An eavesdropper can't learn the key even if the record g^a and g^b and later compromise Alice's computer



WPA-Enterprise

- Core issue: Every client starts with the same *PSK* to derive the *PTK*
  - Fix: Have each user use their own username and password, instead
    - This is the model that eduroam use!

- Instead of using a PSK, use a randomly generated key by an authentication server
  - For your client to trust the authentication server, you accept a digital certificate
  - Form a secure channel to the authentication server, which lets you enter your username and password
  - If the username and password are correct, the authentication server sends a one-time key to use instead of a PSK to both the client and the AP (also over a 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 authentication server, which the attacker can't do
  - **Brute-force attack**: The generated PSK replacement is long and random, too long to brute-force
  - **Forward secrecy**: The generated PSK replacement is used once and then discarded, so no information is retained that allows the PTK to be recovered later

- However, it is still vulnerable to higher-layer attacks such as ARP or DHCP spoofing
  - WPA is really a layer 1 protocol, so it can't provide defenses for this!

Summary

- Classes of attackers:
  - Off-path: Can’t see, modify, or drop packets
  - On-path: Can see packets, but can’t modify or drop packets
  - MITM: Can see, modify, and drop packets

- ARP: A protocol to translate local IP addresses to MAC addresses
  - Ask everyone on the network, “Who has the IP 1.2.3.4?”
  - Attack: The attacker can respond instead of the true device with 1.2.3.4, and packets will get routed to the attacker!
  - Defense: Switches
  - Defense: Rely on higher layers

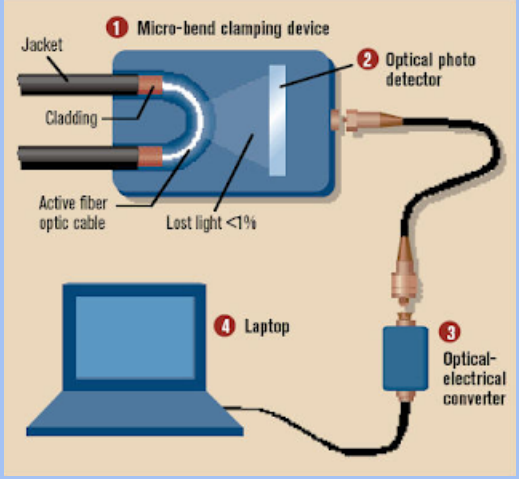
- DHCP: A protocol for a new client to receive a network configuration
  - Ask everyone on the network, “What is the network configuration to use?”
  - Attack: The attacker can respond with a malicious configuration
  - Defense: Rely on higher layers

Summary

- WPA: A protocol to encrypt Wi-Fi connections at layer 1
  - Messages between the client and the AP are encrypted with keys
  - Handshake uses MICs (cryptographic MACs) to verify that both parties have the same PSK and nonces
  - WPA-PSK: Use a password to derive a PSK, which is used in a handshake to arrive at a key
    - Attack: Attacker can pretend to be an AP
    - Attack: Brute-force the password after recording a handshake
    - Vulnerability: No forward secrecy
  - WPA-Enterprise: Use a third party to provide a one-time “replacement PSK,” used in the same handshake
    - Solves the attacks on WPA-PSK

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

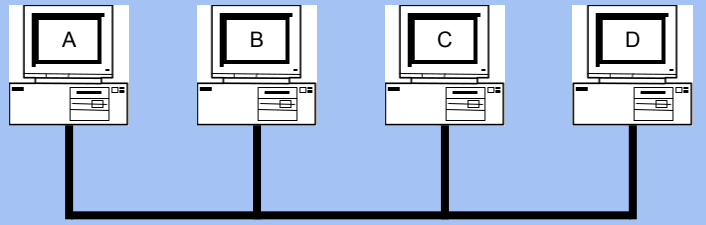
Operation Ivy Bells

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.

Real-World On-Path Attackers

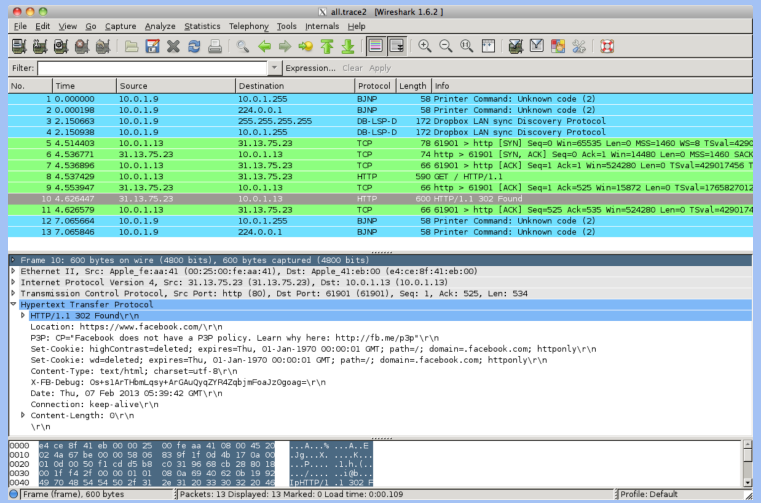
- Layer 2 attack: Read packets sent across the local area network (LAN)
- Recall: A LAN is a network of connected machines
  - Any machine on the LAN can send packets to any other machine on the LAN
- Some LANs use **broadcast technologies**
  - Every packet gets sent to every machine on the LAN
  - Each machine agrees to ignore packets where the destination is a different machine
- A machine can break the agreement and read packets meant for other machines
  - This is called **promiscuous mode**
  - May require root access on the machine



Real-World On-Path Attackers

- **`tcpdump`**: A program for reading packets on the local network
  - Uses promiscuous mode to read other machines' packets in broadcast techonlogies
- 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
```



Real-World On-Path Attackers

- Some layer 2 (Ethernet) devices can be configured to also send a copy of every packet to the attacker
- The attacker could also use this device to modify packets (man-in-the-middle attack)
- Example: DualComm DCGS-2005
  - Newer model: ETAP-2003R
  - Cost: $200
  - Powered with USB (no extra power supply needed)