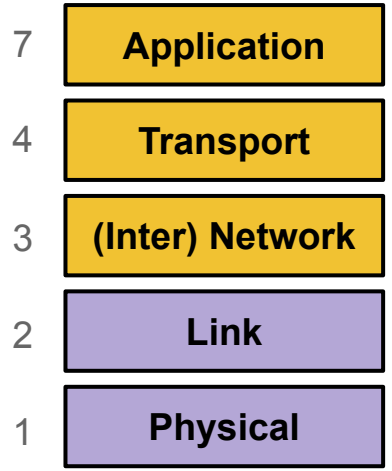
Low Level Network Attacks

CS 161 Fall 2022 - Lecture 17

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: The most common Layer 2 protocol
    - MAC addresses: 6-byte addressing system used by Ethernet
  - Layer 3: Global packet delivery
    - IP: The universal Layer 3 protocol
    - IP addresses: 4-byte (or 16-byte) addressing system used by IP
  - Layer 4: Transport of data (more on this next time)
  - Layer 7: Applications and services (the web)



Last Time: ARP

- 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

Today: Low-Level Network Attacks

- WPA: Communicate securely in a wireless local network
- DHCP: Get configurations when first connecting to a network

Dynamic Host Configuration Protocol (DHCP)

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 (we'll see this soon)
  - The IP address of the router (gateway) so that the user can 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

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

Dynamic Host Configuration Protocol (DHCP)

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

Alice

Bob

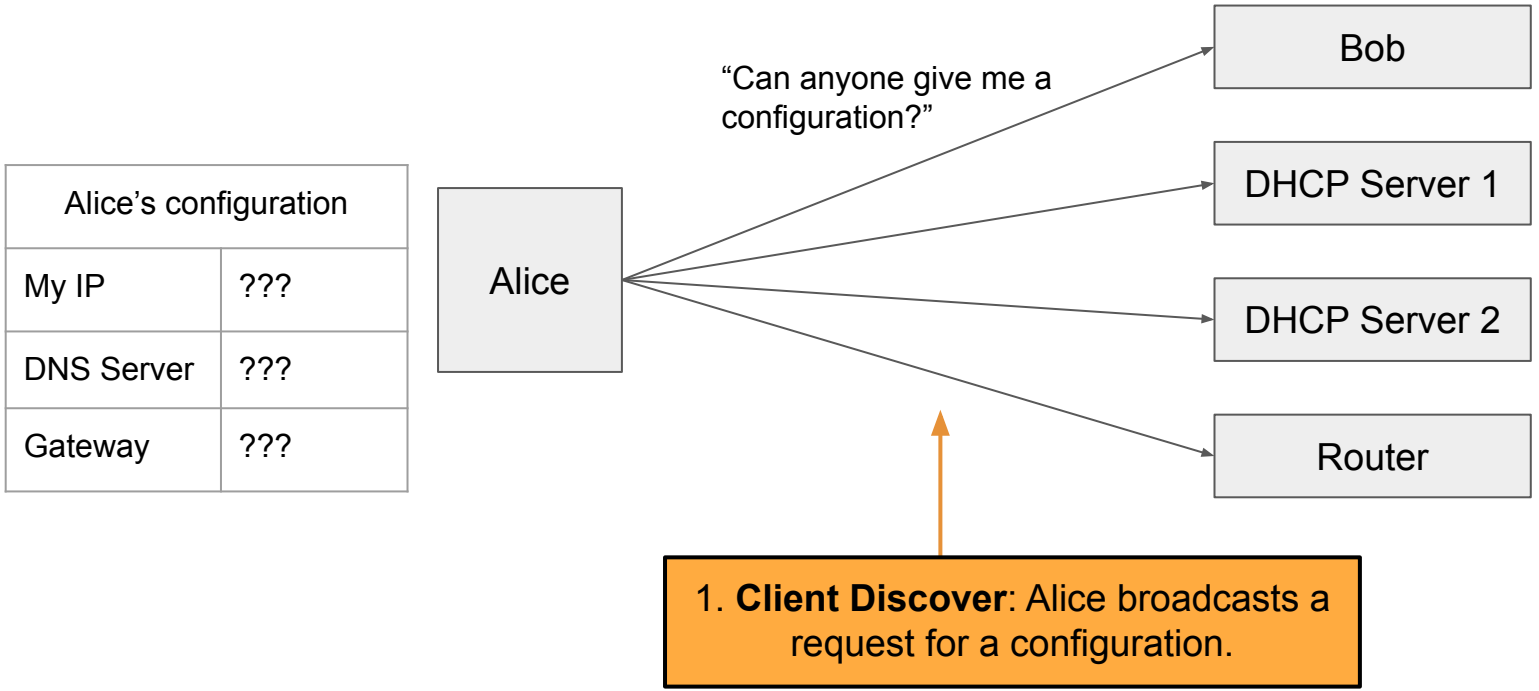
DHCP Server 1

DHCP Server 2

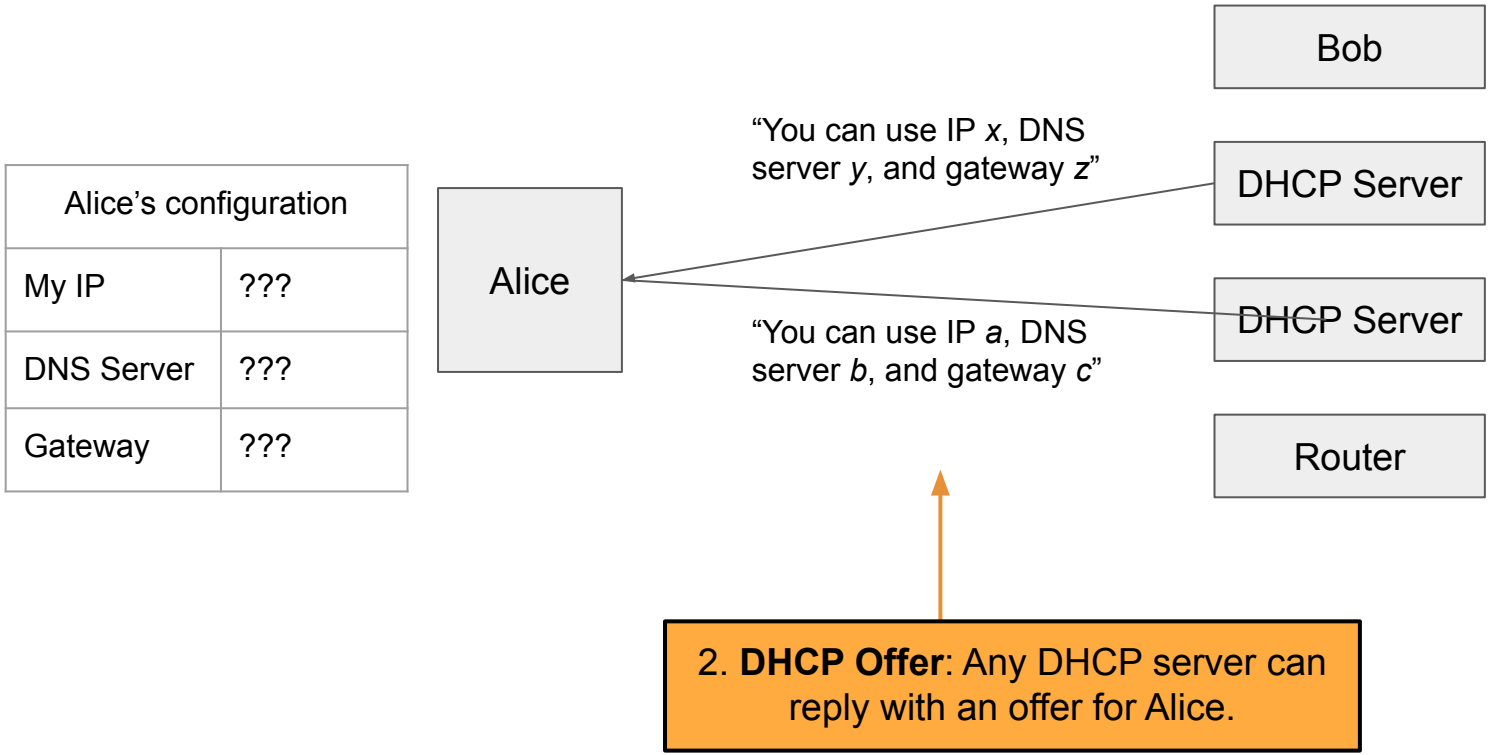
Router

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

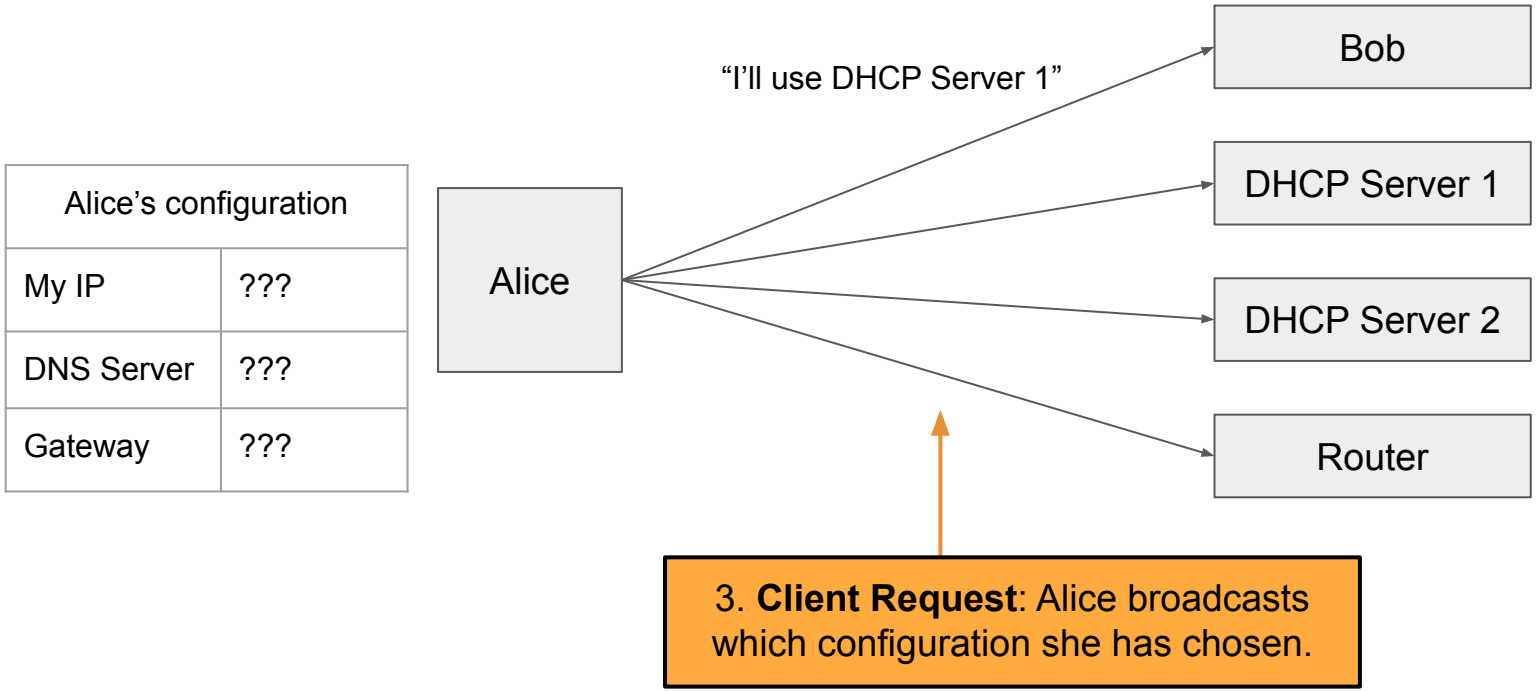
Dynamic Host Configuration Protocol (DHCP)



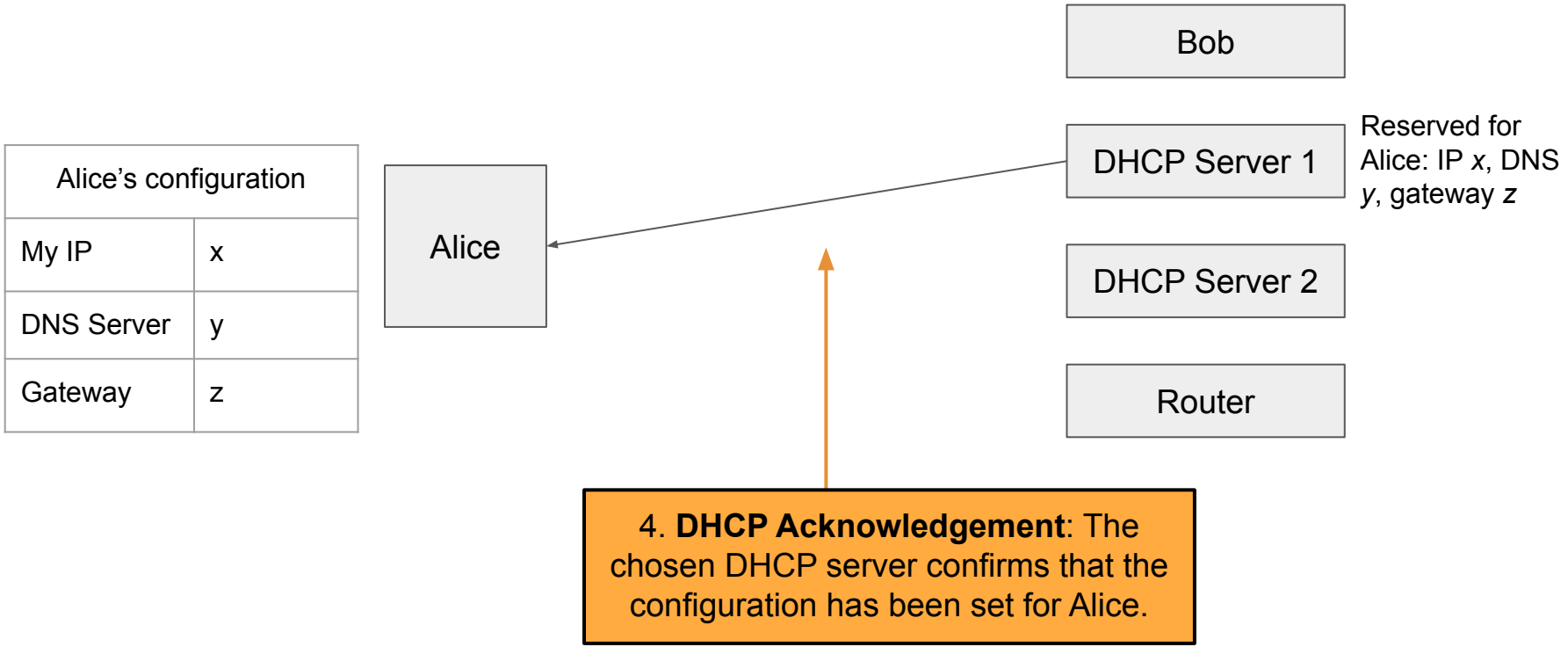
Dynamic Host Configuration Protocol (DHCP)



Dynamic Host Configuration Protocol (DHCP)



Dynamic Host Configuration Protocol (DHCP)



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

Wireless Local Networks

Wi-Fi

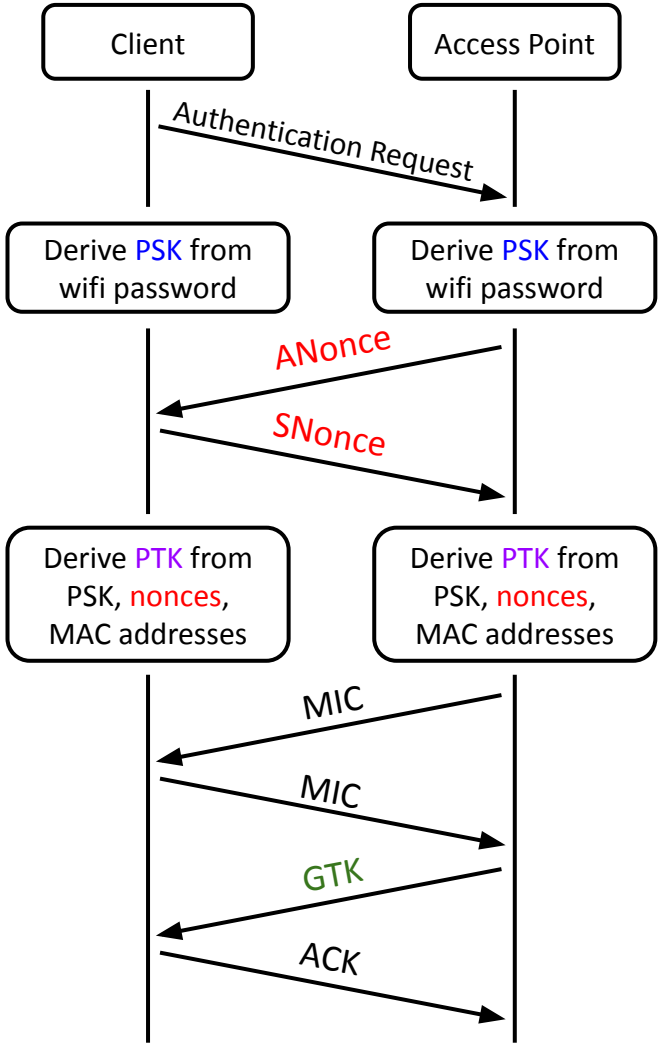
- **Wi-Fi**: A layer 2 protocol that wirelessly connects machines in a LAN
  - Alternative is Ethernet, which uses wires to connect machines in a LAN
- Parts of a Wi-Fi network
  - **Access point**: A machine that will help you connect to the network
  - **SSID** (service set identifier): The name of 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 network 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 (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

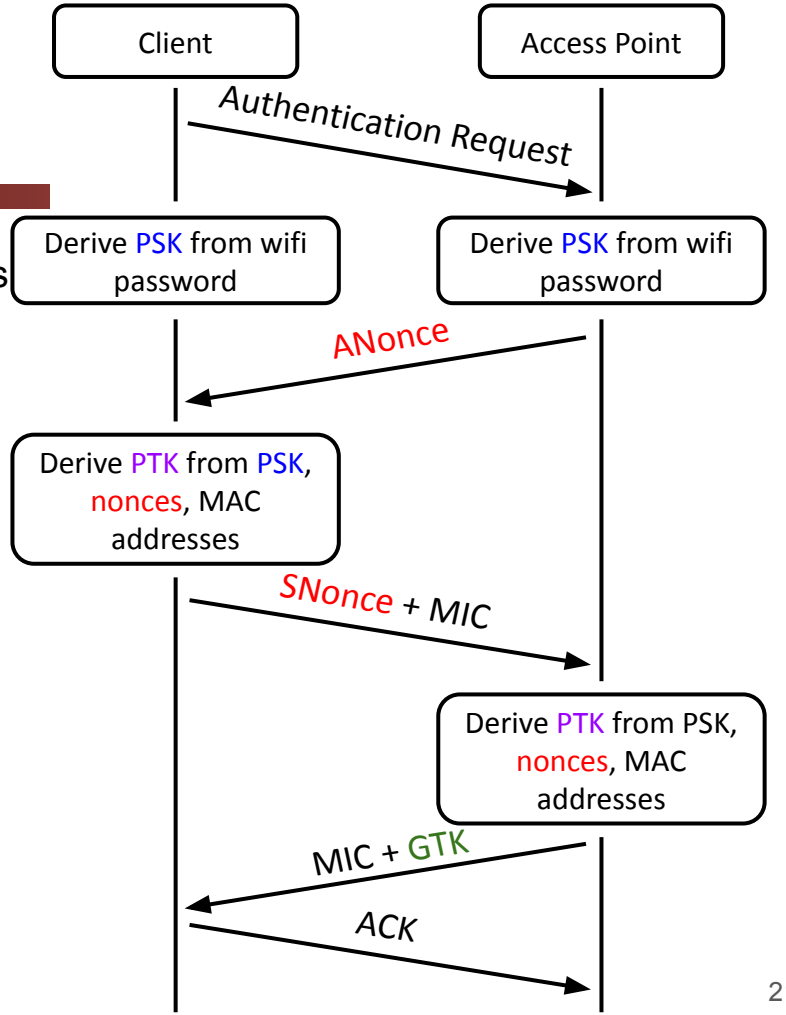


WPA Handshake

- 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
- The optimized version of the handshake decreases the number of messages sent back and forth

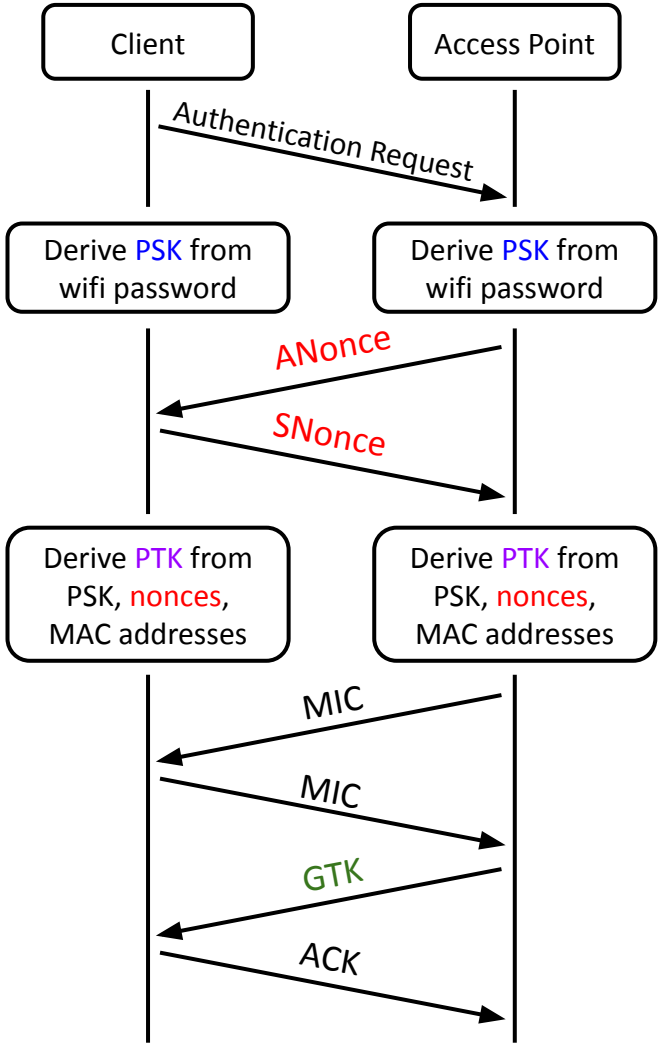
Optimized WPA 4-Way Handshake

1. The client sends an authentication request to the access point
2. Both use the password to derive the *PSK* (pre-shared key)
3. The AP sends *ANonce* to the client
4. The client generates *SNonce*, uses the *PSK*, nonces, and MAC addresses to derive the *PTK* (pairwise transport keys)
5. The client sends *SNonce* and its MIC to the AP
6. The AP uses the *PSK*, nonces, and MAC addresses to derive the *PTK* (pairwise transport keys)
7. The AP sends its MIC and *GTK* to the client
8. The client acknowledges receiving the GTK



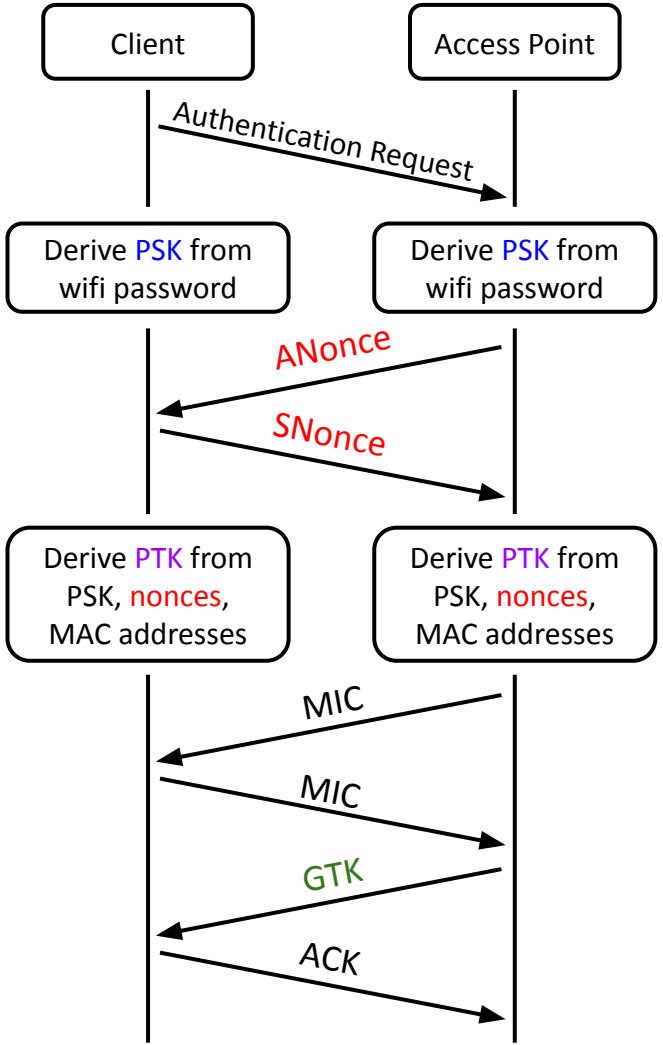
WPA-PSK Attacks

- **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 4-way handshake with the client and become a MITM!



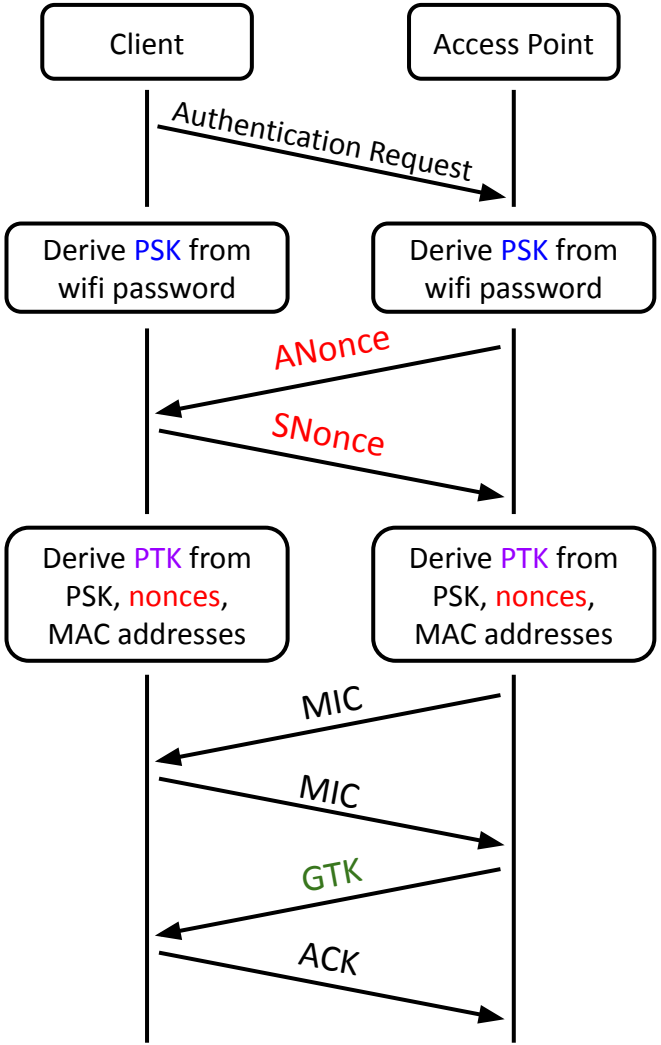
WPA-PSK Attacks

- **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

- **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 AirBears2 and 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 server, which the attacker can't do
  - **Brute-force attack**: The generated PSK replacement is long and random, too long to brute-force
  - **No 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!

Border Gateway Protocol (BGP)

Textbook Chapter 29

Review: Internet Protocol (IP)

- **Internet Protocol** (**IP**): The universal layer-3 protocol that all devices use to transmit data over the Internet
- **IP address**: An address that identifies a device on the Internet
  - IPv4 is 32 bits (e.g. `35.163.72.93`)
  - IPv6 is 128 bits (e.g. `2607:f140:8801:0000:0000:0000:0001:0023`)
    - Shorthand: omit sets of zeros: `2607:f140:8801::1:23`
  - Globally unique from any single perspective
    - For now, you can think of them as just being globally unique
  - IP addresses help nodes make decisions on where to forward the packet

Subnets

- Recall: Layer 3 routes packets across multiple nodes on different LANs
  - A packet might make many hops across different local networks before it can reach its destination
- IP routes by **subnets**, which are groups of addresses with a common prefix
  - A subnet is written as a prefix followed by the length of the prefix
    - Example: **128.32.0.0/16** is an IPv4 subnet with all addresses that begin with the prefix of **128.32.***
    - Since an IPv4 is a 32-bit address and there are 16 bits in the prefix, this subnet represents $2^{32 - 16} = 2^{16}$ addresses

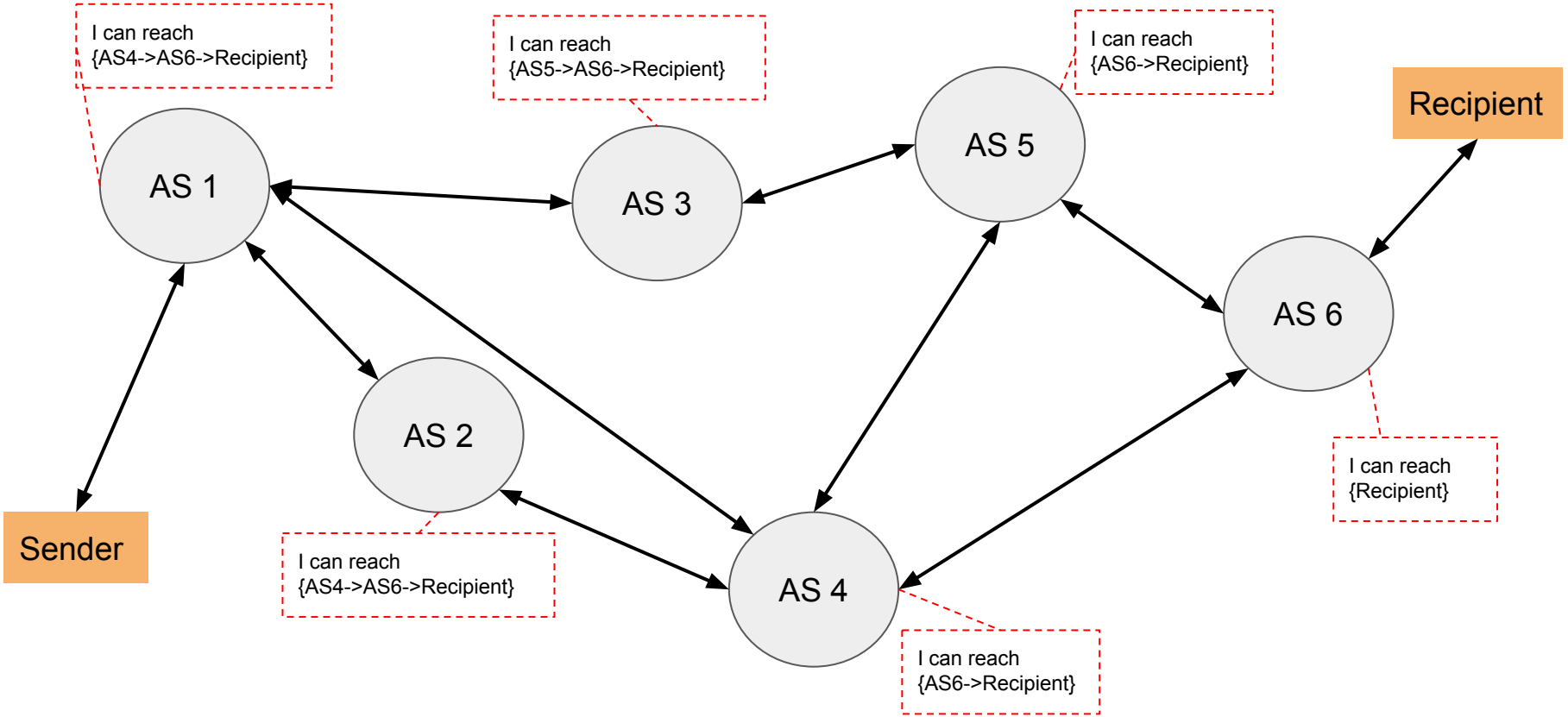
Routing Packets

- To send a packet to a computer within the local network:
  - Verify that the destination IP is in the same subnet
  - Use ARP (or contact a switch) to get the destination MAC address
  - Send the packet directly to the destination using the destination MAC address
- To send a packet to a computer that is not within the local network:
  - Send the packet to the gateway
  - Past the gateway, the packet goes to the Internet
  - It’s the gateway’s job to deliver the packet closer to the destination

Autonomous Systems

- Once your system sends the packet to the gateway, the packet has to be routed through the Internet
- The Internet is a network of networks, comprised of many **autonomous systems** (**AS**)
  - Each AS handles its own internal routing
  - Each AS is uniquely identified by its **autonomous system number** (**ASN**)
  - Each AS is comprised of one or more LANs
  - The AS can forward packet to other connected ASes
- The protocol for communicating between different Autonomous Systems is **Border Gateway Protocol** (**BGP**)
  - Each router announces what networks it can provide and the path onward from the router
  - The most precise route with the shortest path and no loops is the preferred route

BGP


I can reach
{AS4->AS6->Recipient}
I can reach
{AS5->AS6->Recipient}
I can reach
{AS6->Recipient}
Recipient
AS 1
AS 3
AS 5
AS 6
AS 2
AS 4
Sender
I can reach
{Recipient}
I can reach
{AS4->AS6->Recipient}
I can reach
{AS6->Recipient}

IP and BGP Attacks

- Each AS implicitly trusts the surrounding ASes and accepts advertised routes
- **IP spoofing**: Malicious clients can send IP packets with source IP values set to a spoofed value
  - Edge ASes should block packets with source IPs set to the wrong value, but some don't
  - Enables packets that look like they're coming from someone else!
  - We rely on defenses provided by higher layers to further prevent this ("defense in depth")
- **BGP hijacking**: A malicious autonomous system can lie and claims itself to be responsible for a network which it isn't
  - Example: AS3 broadcasts that it is responsible for 128.32.0.0/16
    - Now, the malicious AS can act as a MITM for traffic to 128.32.0.0!
  - No real defenses on this level, so we rely on defenses from higher levels

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

Summary

- Border Gateway Protocol (BGP): Routing packets
  - The Internet is made of smaller **autonomous systems** (**AS**)
  - Each AS broadcasts the shortest routes it knows of (dependent on the shortest routes of its neighbors and distance to neighbors)