



Lecture (09)

CS
IT

Delivering Packets from the Wireless to Wired Network

By:

Dr. Ahmed ElShafee

Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless
Networks

Agenda

- The Wireless Network Road Trip
- Configuring VLANs and Trunks

٢

Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless Networks

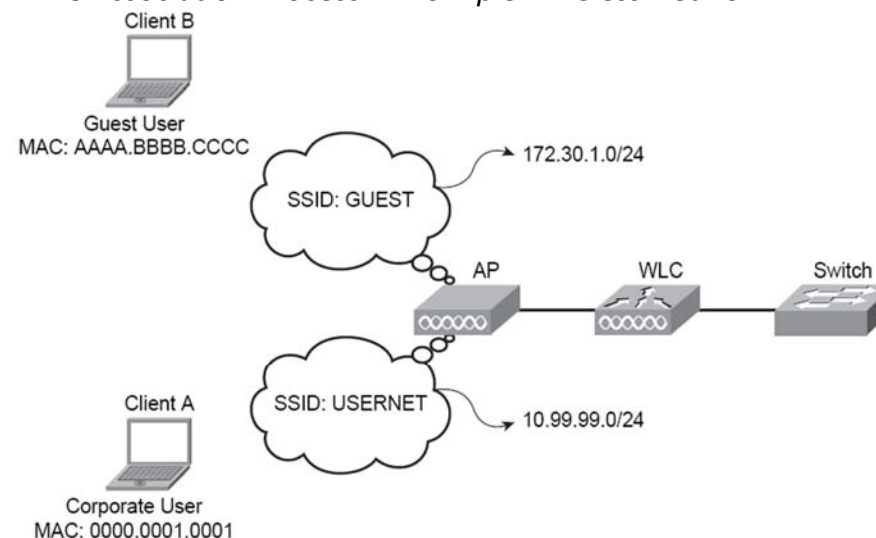
The Wireless Network Road Trip

- At this point, you already have an understanding of how frames are sent on a wireless network.
- In the Wireless Network, frames do not stay on the wireless network; rather, they travel from an AP to a wireless LAN controller (WLC).
- The objective is, how traffic is kept separate as it travels from the AP to the WLC and then to the wired network?
- To better understand this process, you must understand how a network typically looks and the process that each device uses to send and receive data.

٣

Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless Networks

- The Association Process ... *A Simple Wireless Network*



Topology & Configuration

- Figure shows multiple wireless clients are in range of an AP that is advertising multiple service set identifiers (SSID).
- One SSID puts users on a network that is offered to guest users called Guest.
- The other SSID is called UserNet and is designed for authenticated users of the corporate network.
- Naturally, more security is going to be applied to users of UserNet, such as authentication and encryption, as opposed to the network Guest.
- The Guest network places users on the 172.30.1.0/24 subnet. The UserNet places users on the 10.99.99.0/24 network.

Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless Networks

-
- Although these two networks are on different subnets and users associate with different SSIDs, recall that an AP can advertise multiple SSIDs but actually uses the same wireless radio.
 - In the wireless space, the SSID and IP subnet keep the networks logically separated.

Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless Networks

Association

- Clients have more than one way to find an AP and associate with it.
- A client can passively scan the network and listen on each frequency for beacons being sent by an AP,
- or it can use an active scan process and send a probe request in search of a specific AP.

Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless Networks

-
- So a client scans the channels hoping to hear a beacon from an AP or actively sends a probe request.
 - If a probe response is received or a beacon is heard, the client can attempt to associate with the SSID received in that probe response or beacon.
 - The next step is to authenticate and associate with the AP. When the client chooses an SSID, it sends an authentication request.
 - The AP should reply with an authentication response.
 - After this occurs and a "Success" message is received, an association request is sent, including the data rates and capabilities of the client, followed by an association response from the AP.

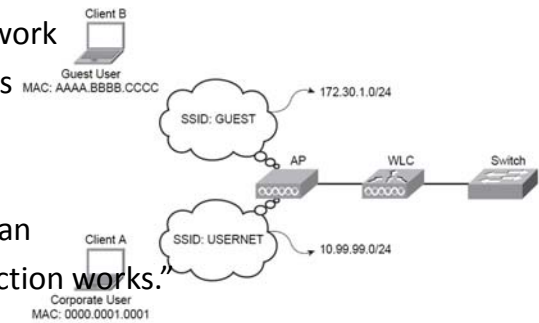
Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless Networks

- The association response from the AP includes the data rates that the AP is capable of, other capabilities, and an identification number for the association.
- Next, the client must determine the speed.
- It does this by determining the Received Signal Strength Indicator (RSSI) and signal-to-noise ratio (SNR), and it chooses the best speed to send at based on these determinations.
- All management frames are sent at the lowest rate, whereas the data headers can be sent faster than management frames, and the actual data frames at the fastest possible rate.

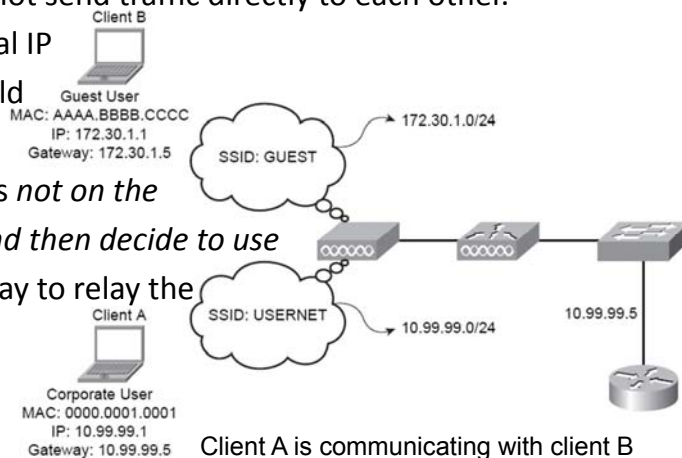
Sending to a Host on Another Subnet

- When a client is associated with an AP, the general idea is to send data to other devices.
- First try to send data between Client A in Figure, which is on the User-Net network, and Client B, which is on the Guest network.

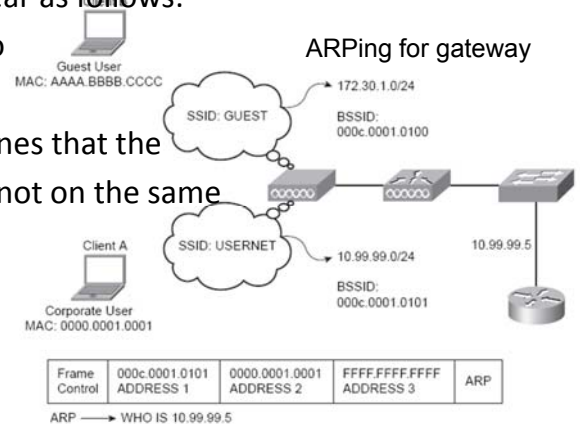
Note: "Although a typical network would not allow guest users to send traffic to internal WLAN users for security purposes, this will provide an Example of how the connection works."



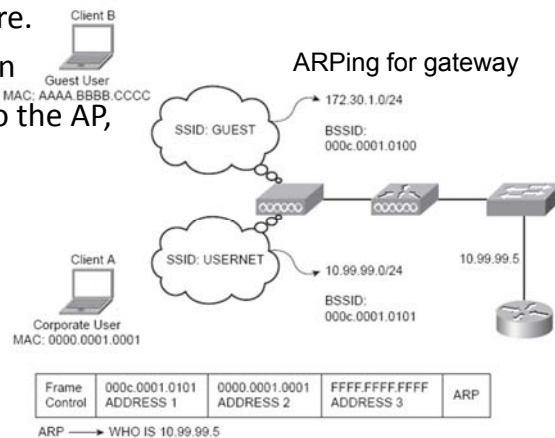
- The two clients are on two different subnets, so the rules of how IP works are still in play.
- The clients cannot send traffic directly to each other.
- Based on normal IP rules, they would first determine that the other is *not on the same subnet and then decide to use a default gateway to relay the information.*



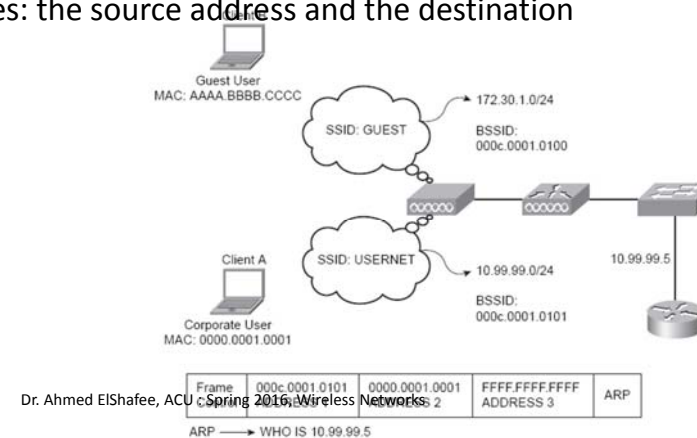
- If a client has never communicated With the default gateway, it uses Address Resolution Protocol (ARP) to resolve its MAC address.
- The process would appear as follows:
- Step 1. Client A wants to send traffic to Client B.
- Step 2. Client A determines that the IP address of Client B is not on the same subnet.



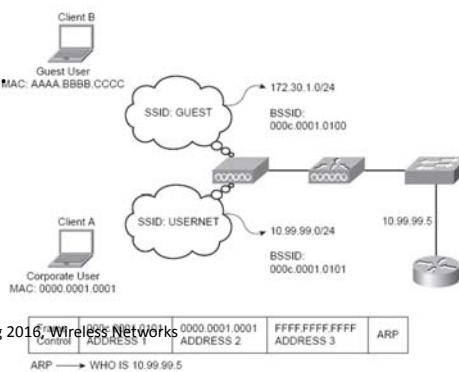
- Step 3. Client A decides to send the traffic to the default gateway of 10.99.99.5.
- Step 4. Client A looks in its ARP table for a mapping to the gateway, but it is not there.
- Step 5. Client A creates an ARP request and sends to the AP, as seen in Figure



- When the ARP request is sent to the AP, the process is a little bit differently than on a wired network.
- Remember that on a wired network, the header has only two MAC addresses: the source address and the destination address.



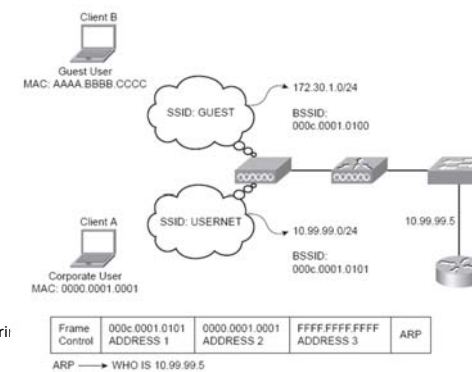
- An 802.11 frame can have four addresses: the source address (SA), destination address (DA), transmitter address (TA), and receiving address (RA).
- In this situation, the SA is the MAC of the client sending the ARP request, the DA is broadcast (for the ARP), and the RA is the AP.
- No TA is present in this example



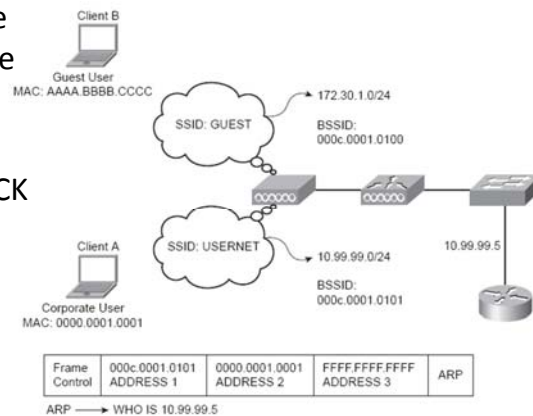
Frame Control	ADDRESS 1 000c.0001.0101	ADDRESS 2 0000.0001.0001	ADDRESS 3 FFFF.FFFF.FFFF	ARP REQUEST
---------------	-----------------------------	-----------------------------	-----------------------------	-------------

ARP Request

- The AP receives the ARP and sees its MAC address.
- It verifies the frame check sequence (FCS) in the frame and waits the short interframe space (SIFS) time.

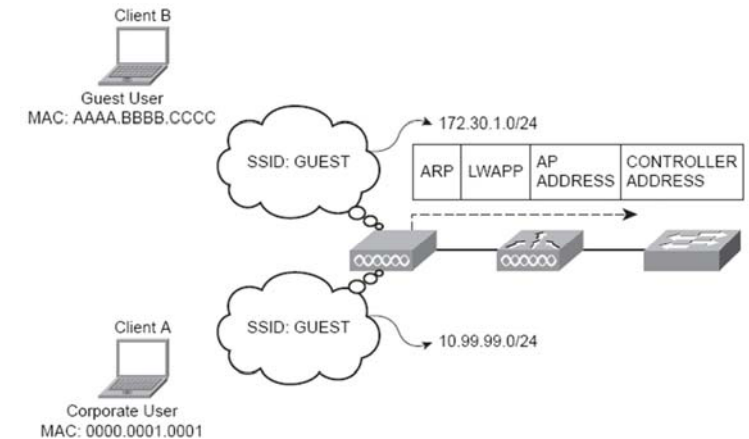


- When the SIFS time expires, it sends an ACK back to the wireless client that sent the ARP request.
- This ACK is not an ARP response; rather, it is an ACK for the wireless frame transmission



17

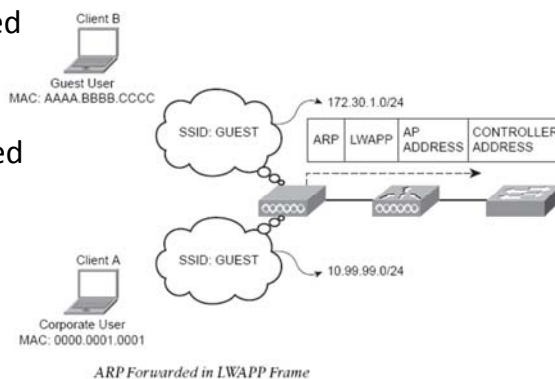
- The AP then forwards the frame to the WLC using the Lightweight Access Point Protocol (LWAPP), as illustrated in Figure.



ARP Forwarded in LWAPP Frame

18

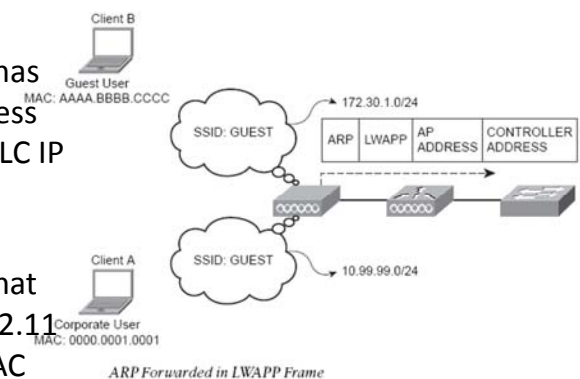
- The LWAPP frame that travels from the AP to the WLC is traveling on a wired network.
- This brings forth the question, “What happened to the 802.11 frame format?” LWAPP process.



ARP Forwarded in LWAPP Frame

19

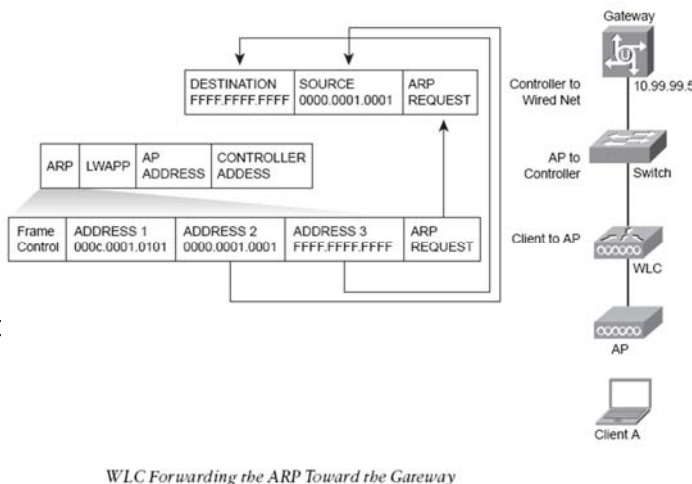
- simply encapsulates the frame inside a 6-byte header.
- The new 6-byte header has the AP IP and MAC address as the source and the WLC IP and MAC address as the destination.
- Encapsulated inside of that header is the original 802.11 frame with the three MAC addresses, including the broadcast MAC address for the ARP



ARP Forwarded in LWAPP Frame

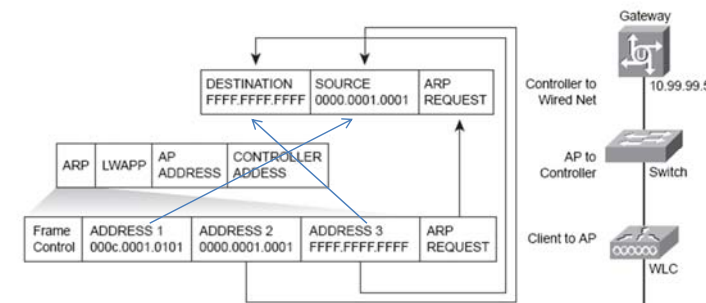
20

- When the WLC receives the LWAPP frame, it opens the frame revealing the ARP request and rewrites the ARP request in an 802.3 frame that can be sent across the wired network.



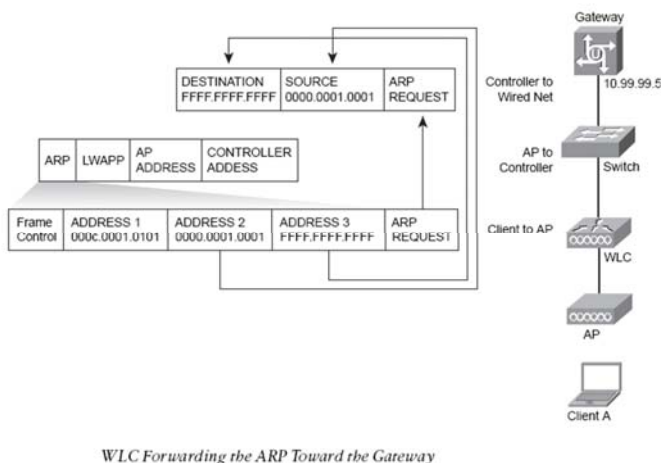
٢١

- The first address from the 802.11 frame is dropped, the second address is placed as the source address in the new 802.3 frame, and the third address, the broadcast address, is placed as the destination address.
- The WLC then forwards the ARP request, in 802.3 format, across the wired network, as seen in next Figure.



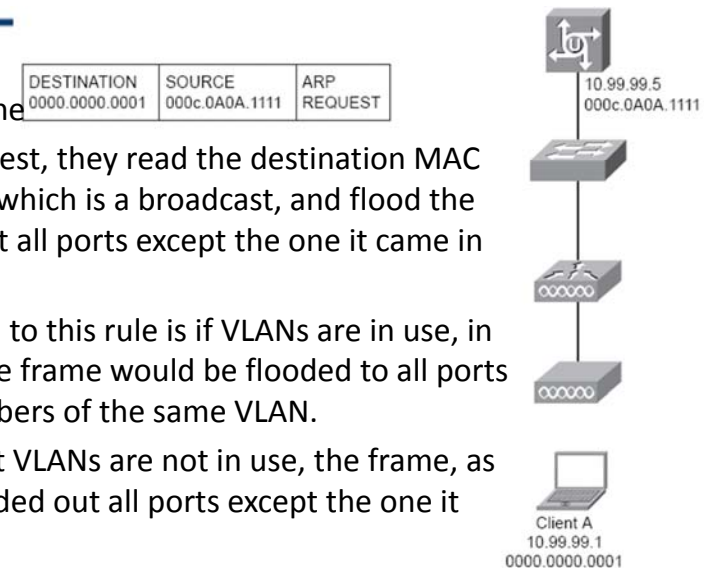
٢٢

- Here you can see how the frame appears between the wireless Client A and the AP, how the AP encapsulates the frame and sends it to the WLC, and how the WLC rewrites the frame and sends it to the wired network.



٢٣

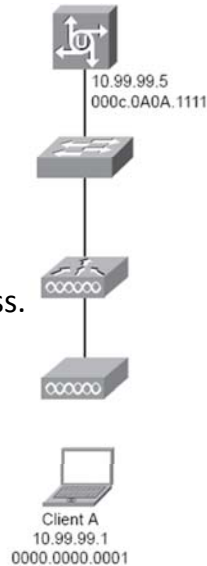
- As switches receive the ARP request, they read the destination MAC address, which is a broadcast, and flood the frame out all ports except the one it came in on.
- The exception to this rule is if VLANs are in use, in which case the frame would be flooded to all ports that are members of the same VLAN.
- Assuming that VLANs are not in use, the frame, as stated, is flooded out all ports except the one it came in on.



٢٤

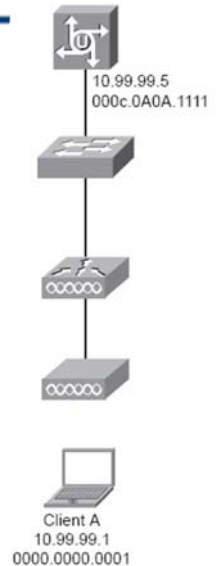
- At some point, the frame will be received by a Layer 3 device, hopefully the default gateway.
- In Figure, the router has received the ARP request and will respond to it with its MAC address.

DESTINATION	SOURCE	ARP
0000.0000.0001	000c.0A0A.1111	REQUEST



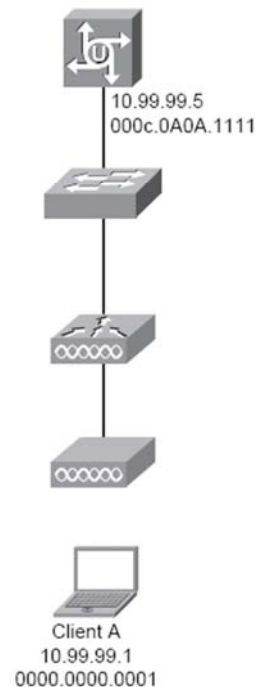
Gateway Responds to ARP

- That ARP response is sent back as a unicast message, so the switches in the path are going to forward it directly to the port that leads back to the wireless client, rather than flooding the frame out all ports.
- Eventually the frame is received by the WLC, and it must be rebuilt as an 802.11 frame.



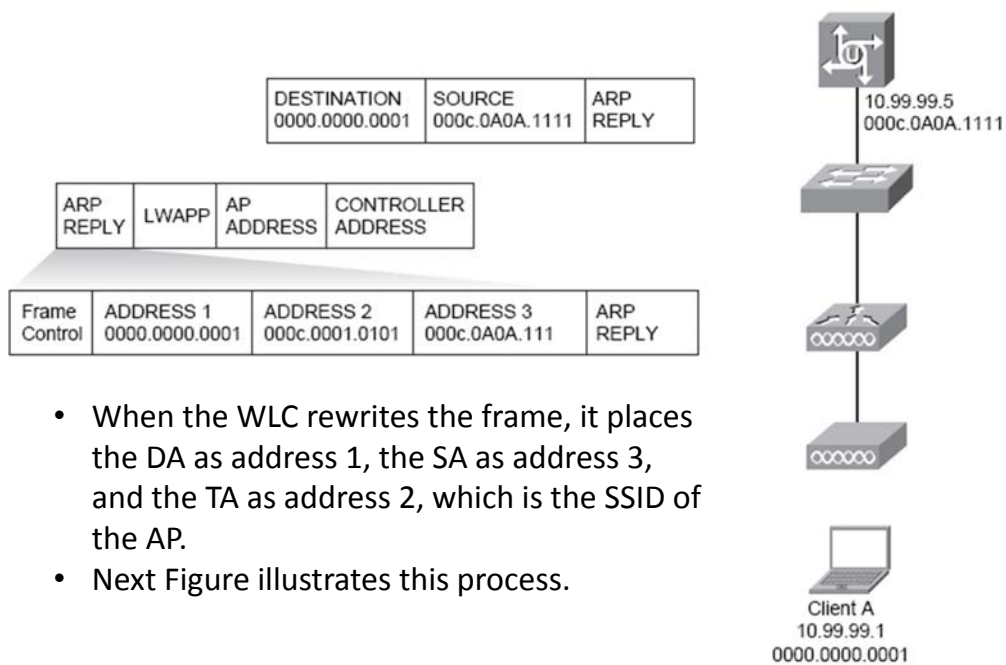
DESTINATION	SOURCE	ARP
0000.0000.0001	000c.0A0A.1111	REPLY

ARP	LWAPP	AP ADDRESS	CONTROLLER ADDRESS
-----	-------	------------	--------------------



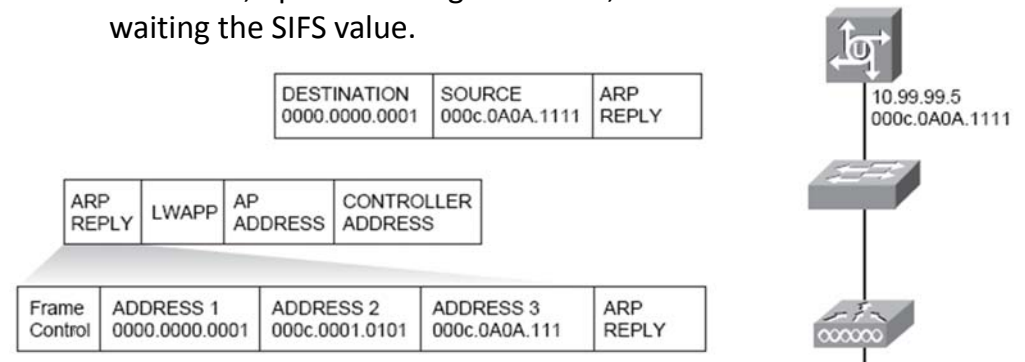
WLC Receives ARP Reply from GW and Converts It to LWAPP

- Next, the AP must remove the LWAPP header, exposing the 802.11 frame.
- The 802.11 frame is buffered, and the process of sending a frame on the wireless network begins.
- The AP starts a backoff timer and begins counting down.
- If a wireless frame is heard during the countdown, the reservation in the heard frame is added to the countdown and the AP continues.
- Eventually, the timer expires, and the frame can be sent as an 802.11 frame.

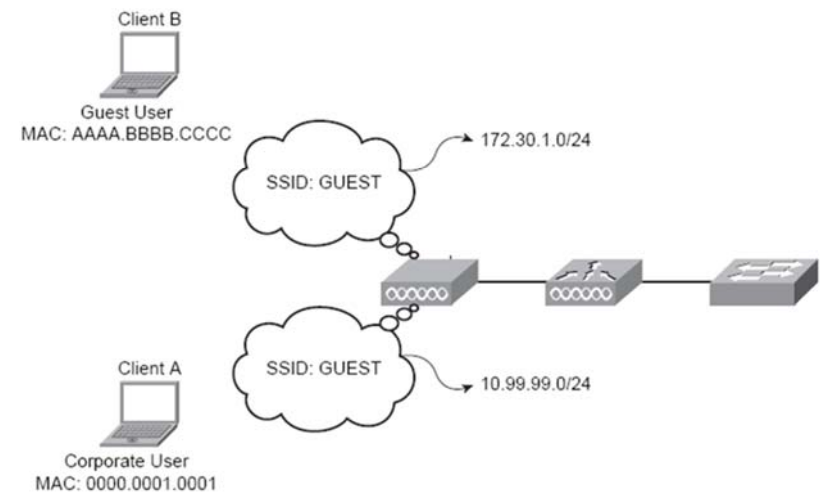



WLC Forwards LWAPP Frame to AP

- As illustrated in Figure, the newly formed 802.11 frame is placed inside an LWAPP header where the AP IP and MAC is the destination and the WLC IP and MAC is the source.
- The LWAPP frame is forwarded to the AP.
- The client, upon receiving the frame, sends an ACK after waiting the SIFS value.



- The ARP process of the client now has a mapping to the GW MAC address and can dispatch the awaiting frame.
- Remember that it still must follow the rules, a backoff timer, and a contention window and eventually transmit the frame following the ARP response.





Thanks,..
See you next week (ISA),...

Dr. Ahmed ElShafee, ACU : Spring 2016, Wireless Networks