The Wireless Network Road Trip

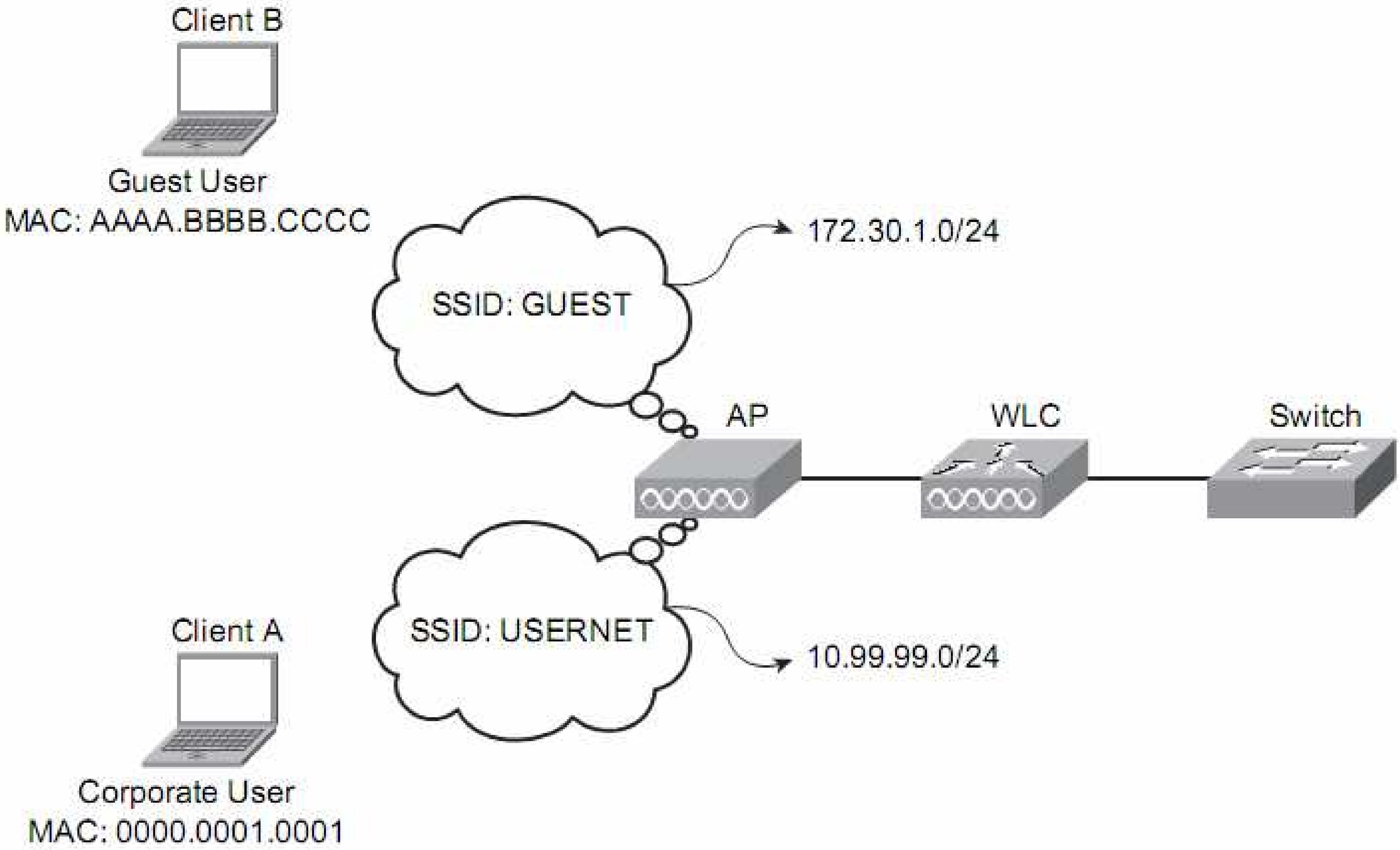


Figure 9-1 *A Simple Wireless Network*

The Association Process

To begin, you need a network. This lecture uses the common logical topology seen in Figure 9-1. As you can see, 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. 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.

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. Users of the UserNet would likely actively scan the network, whereas a guest would passively scan.

Getting back to the association process, 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. 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. Just as the client determines its rates to send, the AP, in turn, does the same. Now that the client is associated, it can attempt to send data to other devices on the network.

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. To illustrate this, first try to send data between Client A in Figure 9-2, which is on the UserNet network, and Client B, which is on the Guest network. 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.

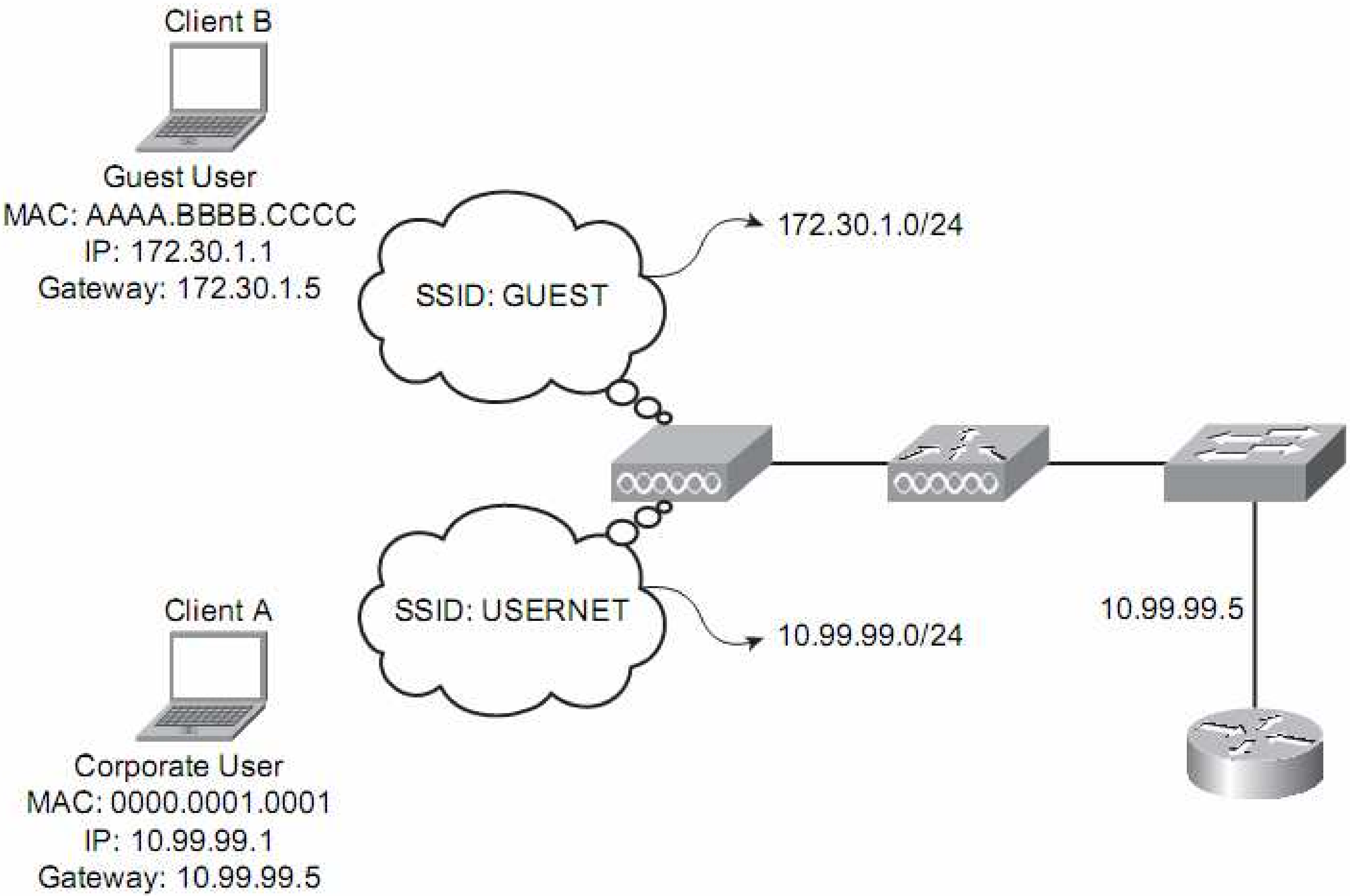


Figure 9-2 *Client A Communicating with Client B*

The two clients are clearly on two different subnets. The clients cannot send traffic directly to each other. 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:

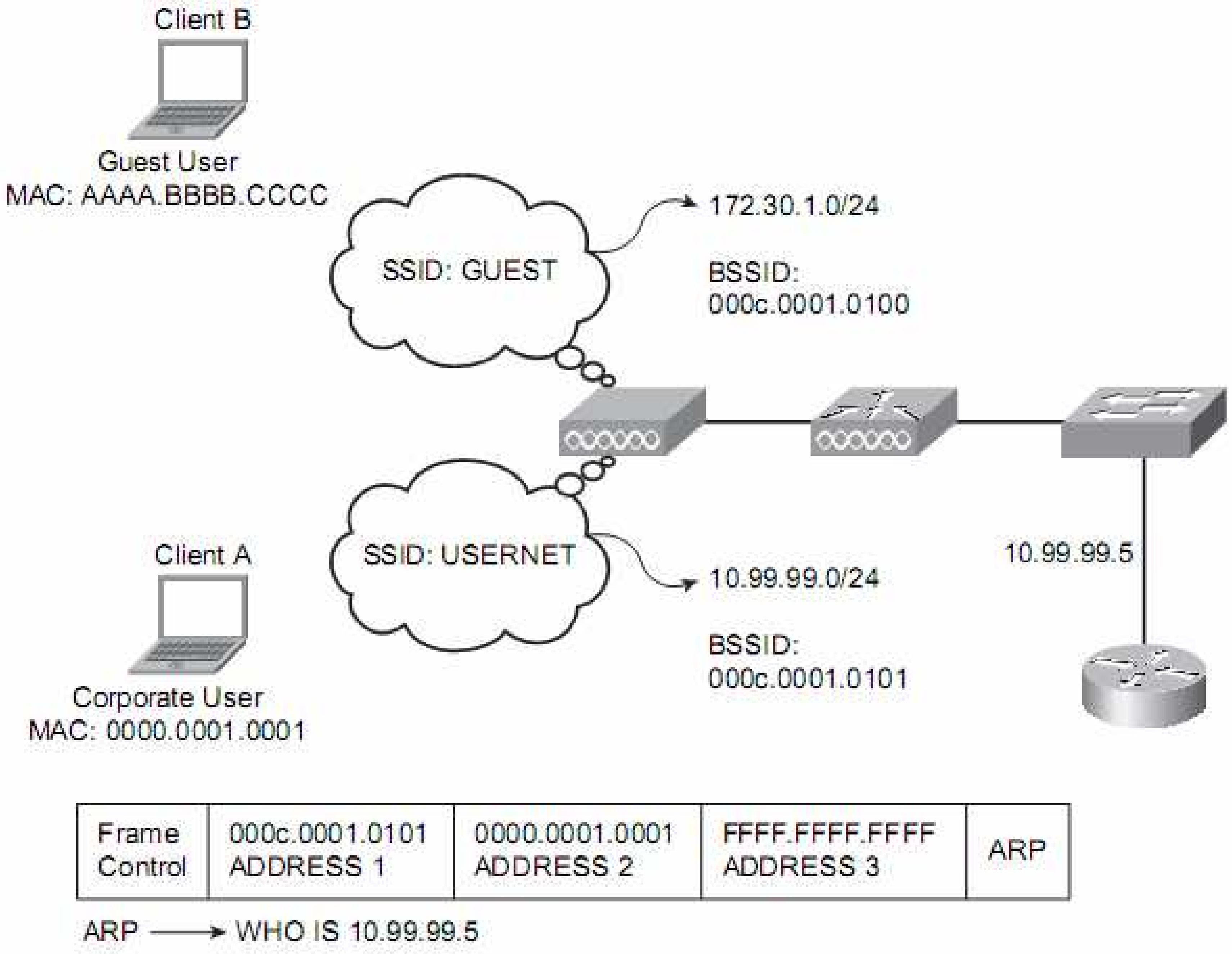
Step 1. Client A wants to send traffic to Client B.

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 9-3.

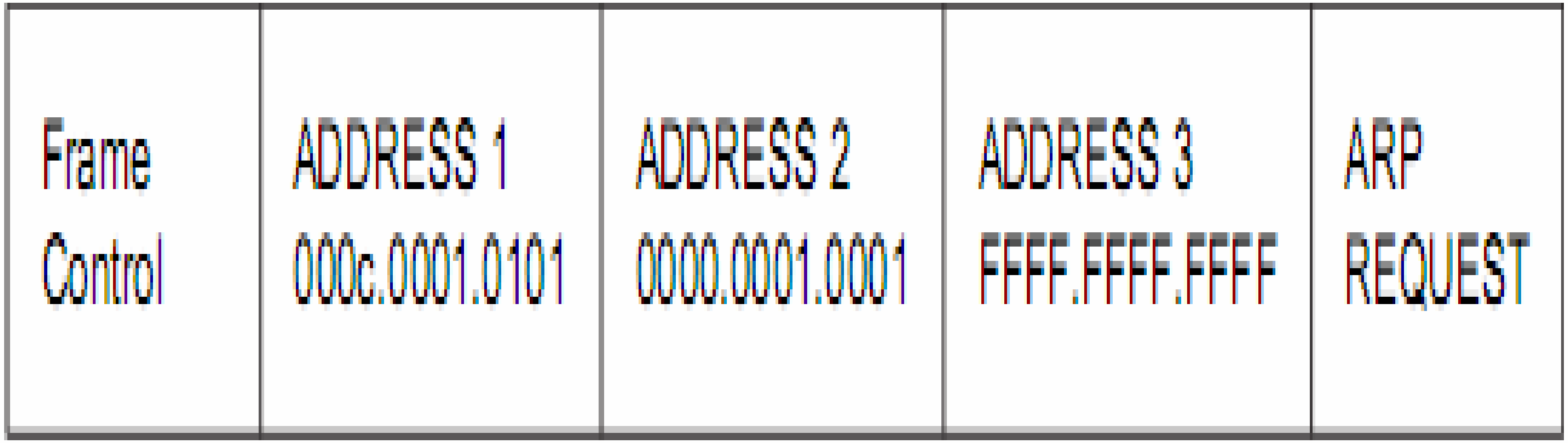


Frame Control	000c.0001.0101 ADDRESS 1	0000.0001.0001 ADDRESS 2	FFFF.FFFF.FFFF ADDRESS 3	ARP

ARP ⟶ WHO IS 10.99.99.5

Figure 9-3 *ARPing for the Gateway*

When the ARP request is sent to the AP, it is an interesting process and actually works 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. Figure 9-4 shows the ARP request.



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

Figure 9-4 *ARP Request*

The AP receives the ARP and sees its MAC address. The AP then forwards the frame to the WLC using the Lightweight Access Point Protocol (LWAPP), as illustrated in Figure 9-5

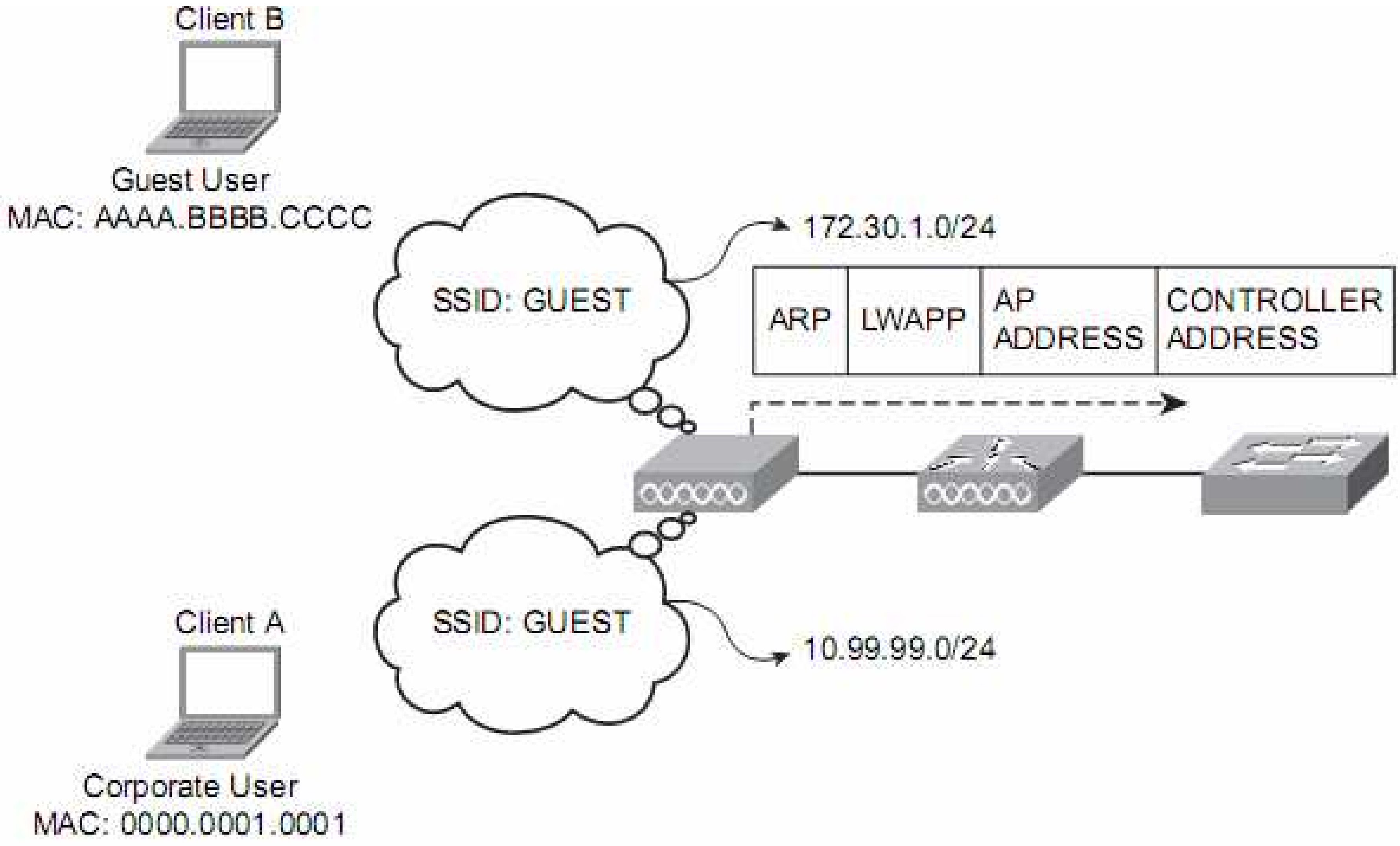


Figure 9-5 *ARP Forwarded in LWAPP Frame*

The LWAPP frame that travels from the AP to the WLC is traveling on a wired network. This brings the question, *“What happened to the 802.11 frame format?”* LWAPP 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 process. 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. 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 Figure 9-6. 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.

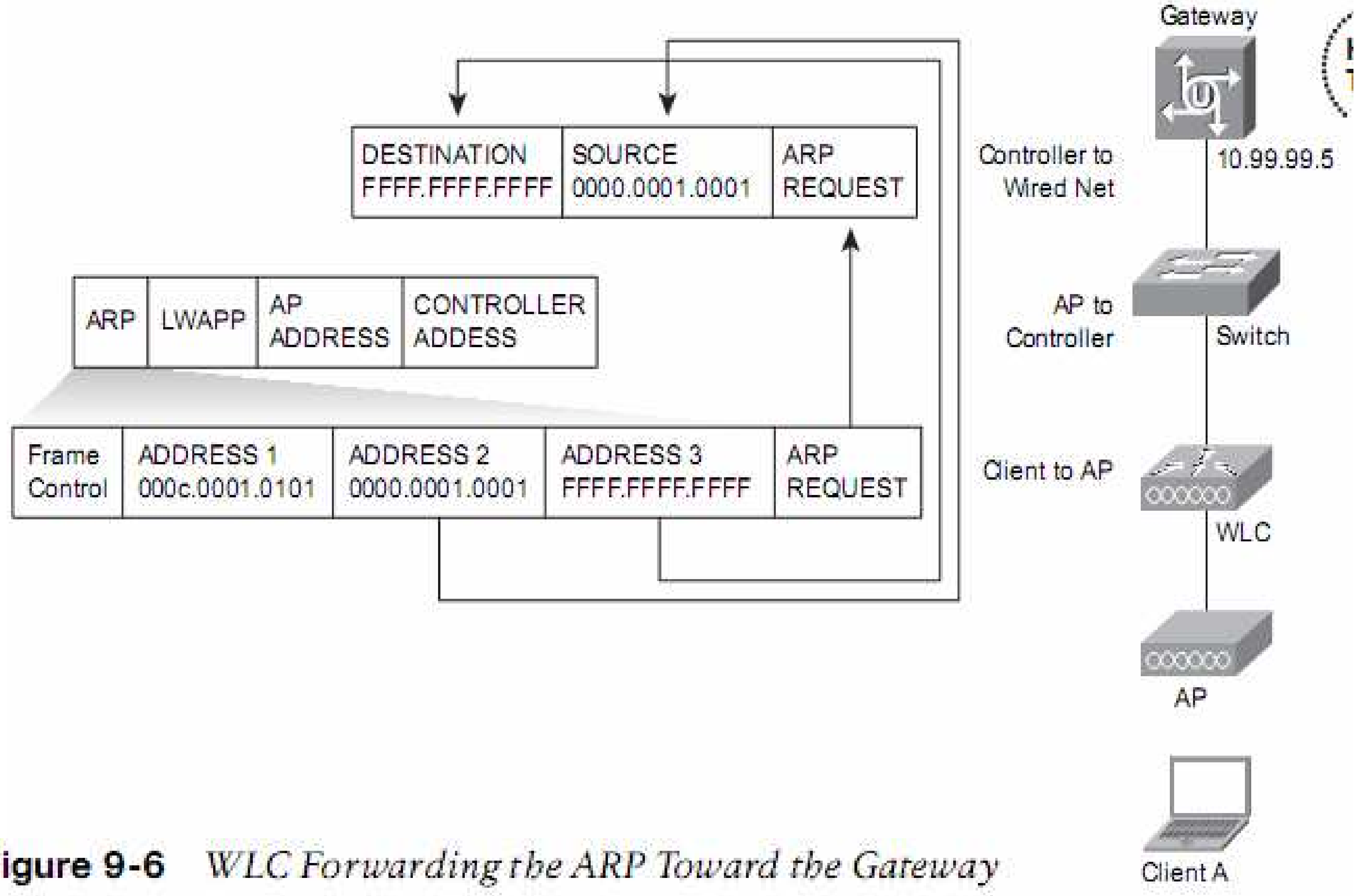
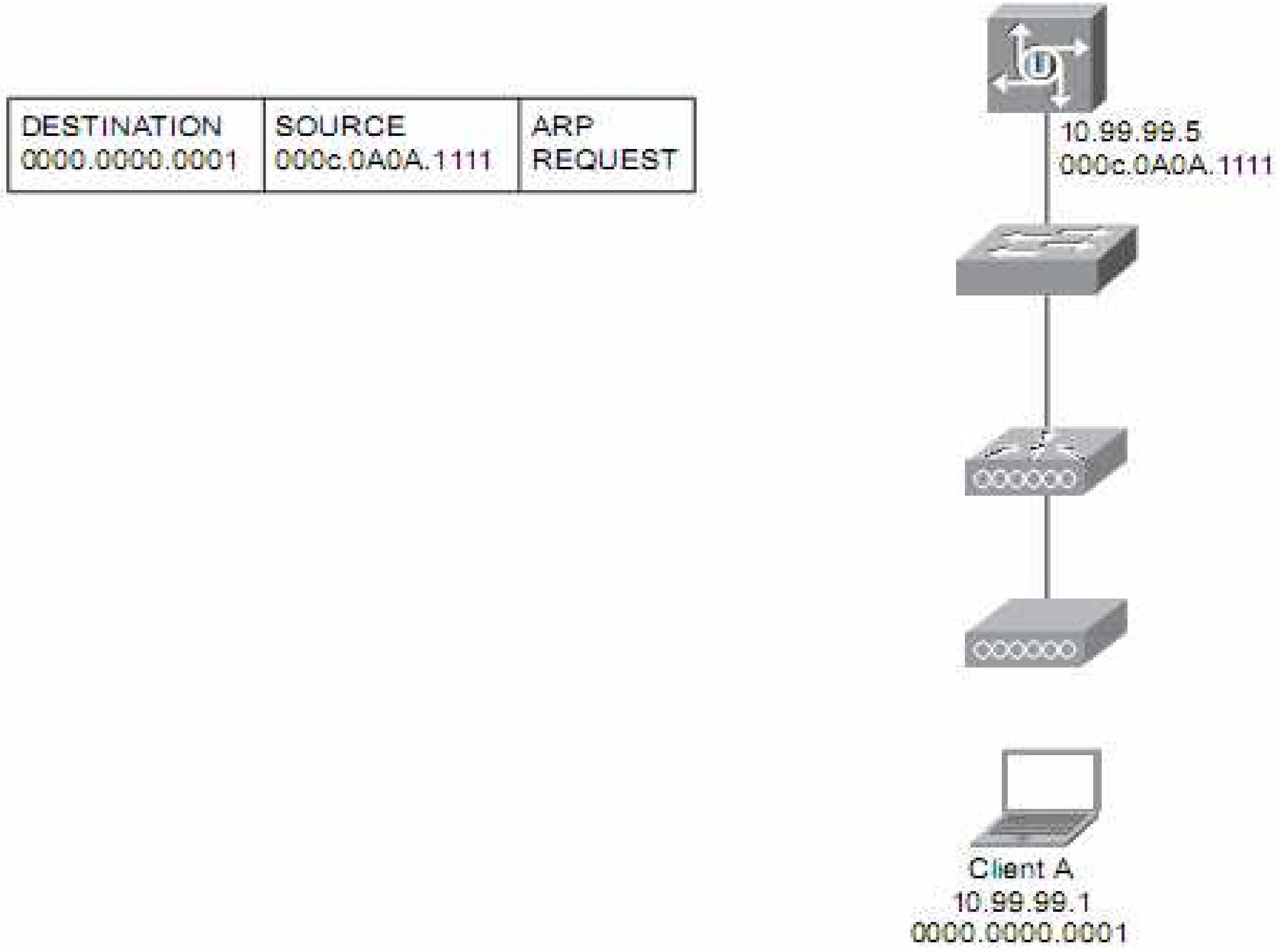


Figure 9-6 *WLC Forwarding the ARP Toward the Gateway*

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.

At some point, the frame will be received by a Layer 3 device, hopefully the default gateway. In Figure 9-7, the router has received the ARP request and will respond to it with its MAC address.



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

Figure 9-7 *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. When the WLC rewrites the frame, it places the DA as address 1, the SA as address 3, and the TA as address 2, which is the SSID of the AP. Figure 9-8 illustrates this process.

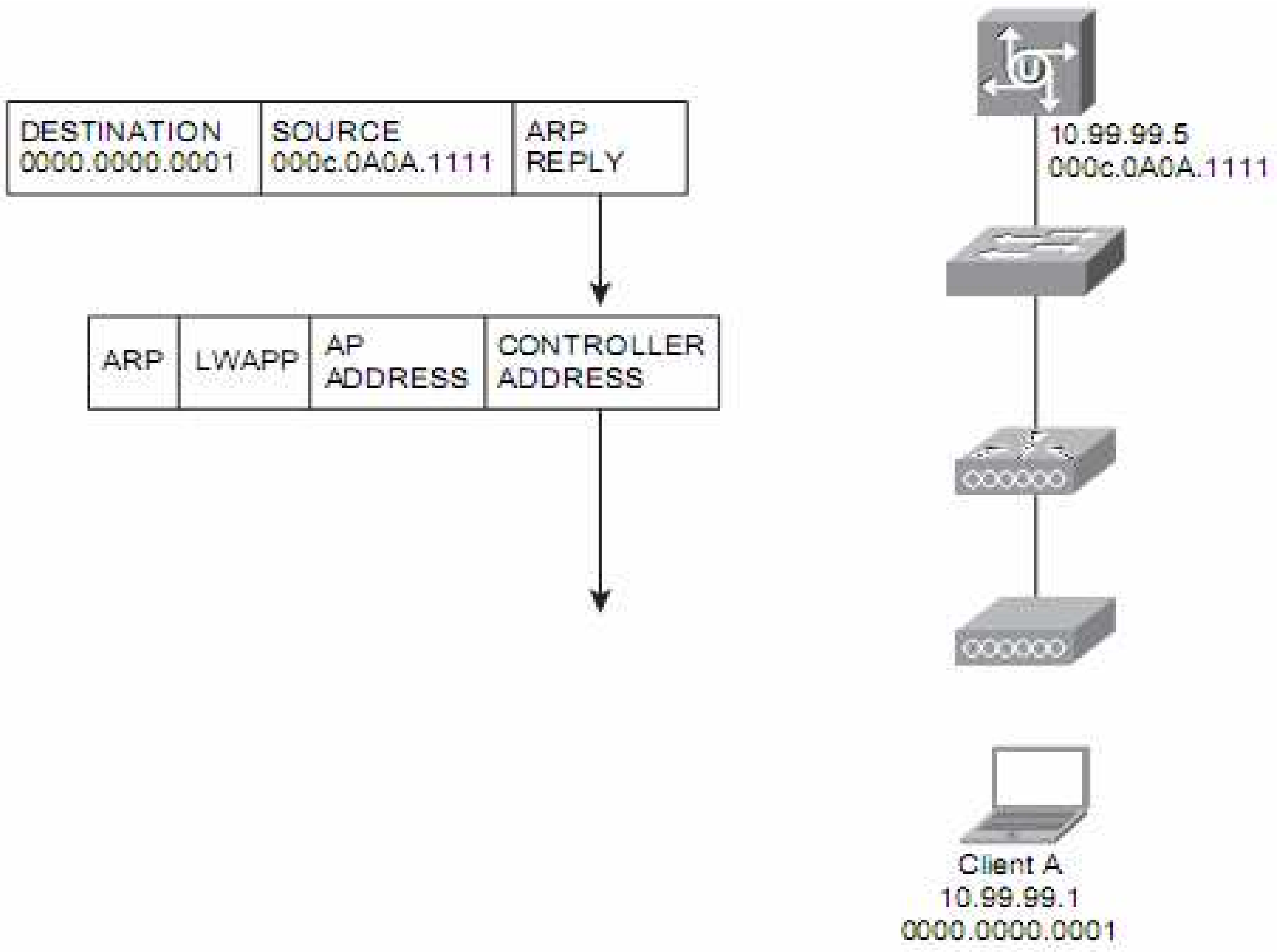


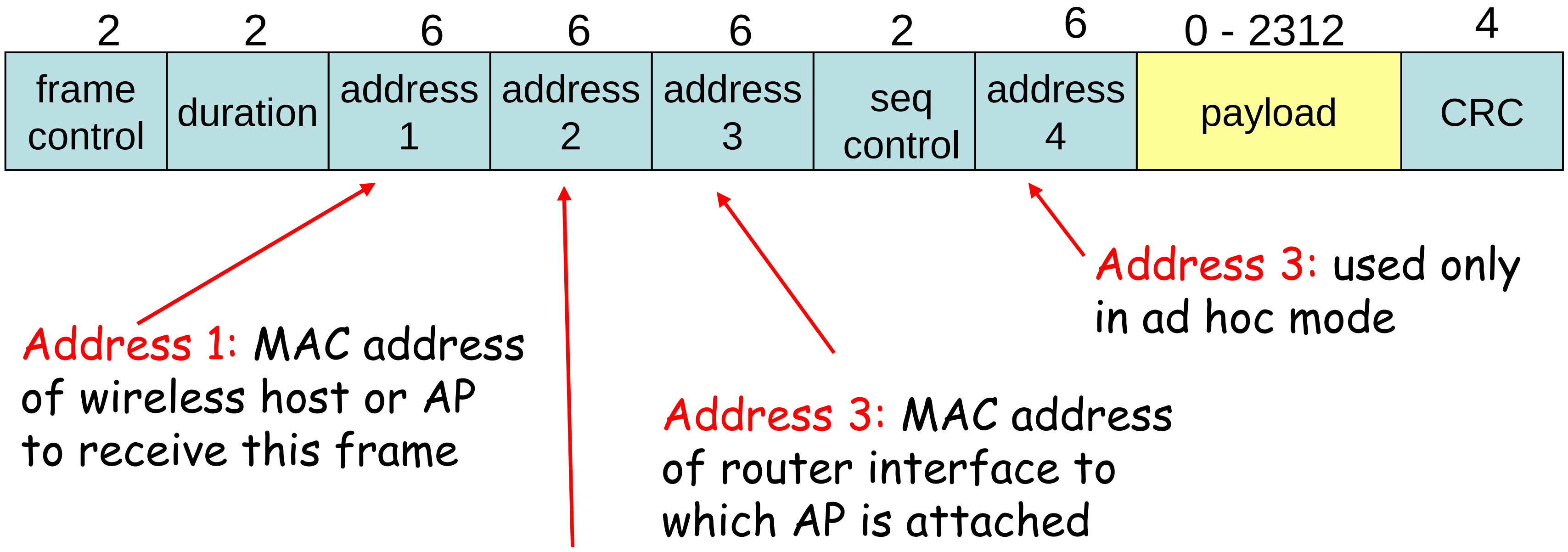
Figure 9-8 *WLC Receives ARP Reply from GW and Converts It to LWAPP*

As illustrated in Figure 9-9, 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

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 ARP process of the client now has a mapping to the GW MAC address and can dispatch the awaiting frame.

802.11 frame: addressing



2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

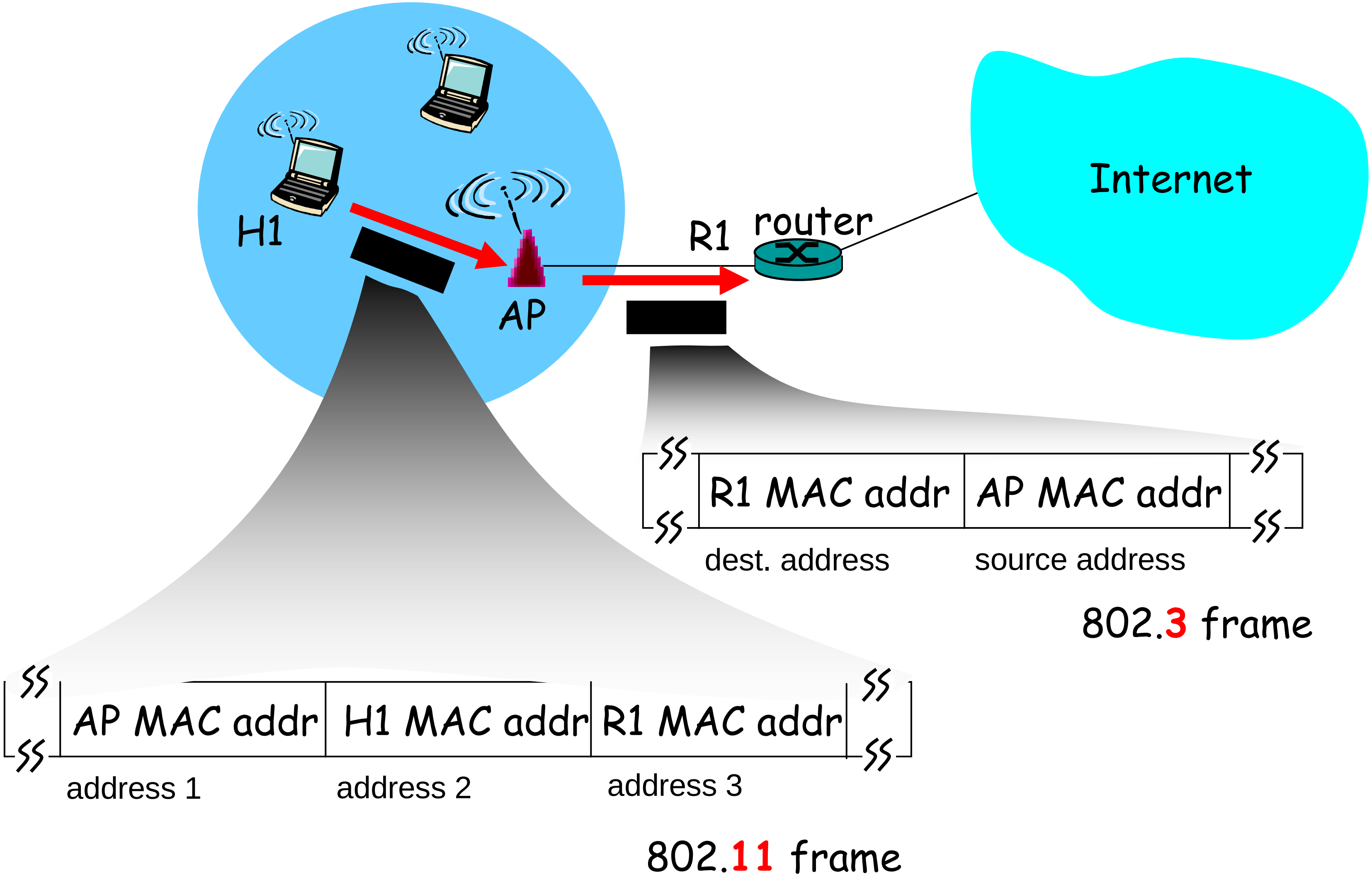
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 3: used only in ad hoc mode

802.11 frame: addressing



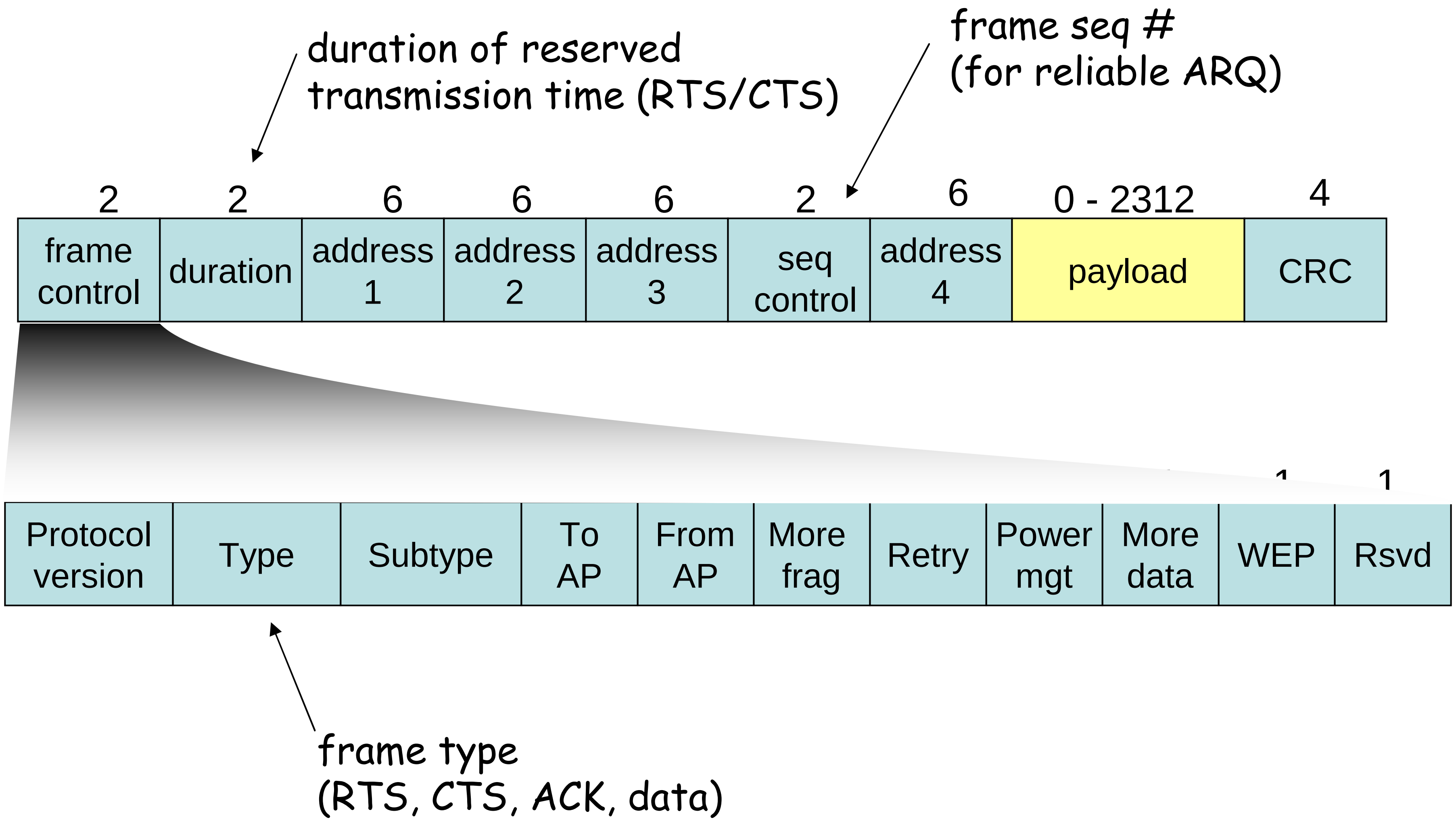
R1 MAC addr	AP MAC addr
dest. address	source address

802.3 frame

AP MAC addr	H1 MAC addr	R1 MAC addr
address 1	address 2	address 3

802.11 frame

802.11 frame: more



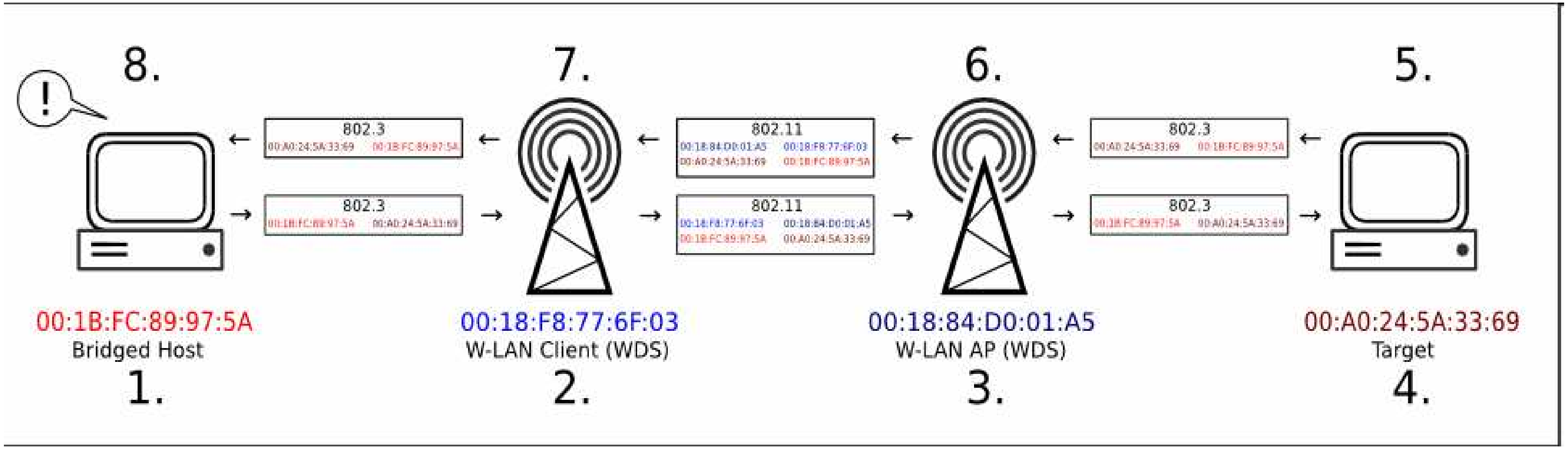
duration of reserved transmission time (RTS/CTS)

frame seq #
(for reliable ARQ)

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

									1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

frame type
(RTS, CTS, ACK, data)


8.
7.
6.
5.
802.3
00:A0:24:5A:33:69
00:1B:FC:89:97:5A
802.3
00:1B:FC:89:97:5A
00:A0:24:5A:33:69
802.11
00:18:84:D0:01:A5
00:18:F8:77:6F:03
00:A0:24:5A:33:69
00:1B:FC:89:97:5A
802.11
00:18:F8:77:6F:03
00:18:84:D0:01:A5
00:1B:FC:89:97:5A
00:A0:24:5A:33:69
802.3
00:A0:24:5A:33:69
00:1B:FC:89:97:5A
802.3
00:1B:FC:89:97:5A
00:A0:24:5A:33:69
00:1B:FC:89:97:5A
Bridged Host
1.
00:18:F8:77:6F:03
W-LAN Client (WDS)
2.
00:18:84:D0:01:A5
W-LAN AP (WDS)
3.
00:A0:24:5A:33:69
Target
4.