

Data Communications Assignment 2 Resit

Stefan M Ahmed

21359035

07/19

Element 1

This element is about network interfaces which are how the devices are connected to a network, whether they are wired or wireless. They are the connection between the host/router and the larger network i.e. the internet which may be wired e.g. ethernet or wireless. A host such as a computer has at least two interfaces which are wired e.g. ethernet port for connecting an ethernet cable and wireless e.g. antennas attached to a network interface card. A router has several interfaces which are both wired and wireless e.g. ethernet connection ports for ethernet cables and antennas for sending and receiving wireless data. Interfaces are connected by an ethernet switch or a wireless base station.

IP addresses are 32 bit addresses that identify a host and a router interface. IP addresses are to do with each interface rather than the host or router the interface is joined to. They are a length of numbers separated by dots and each number is eight bits.

In the large network such as the internet we have the network layer which is transport route from the sending host to the receiving host. In the network layer we have devices such as hosts(computers, laptops, smart phones), wireless base stations(which connect the hosts to the internet), access points (which connect the hosts to the internet too), switches and routers which are known in the network as nodes. Each node is connected by paths known as channels.

Network interfaces can be detected by using prompts on a computer when the devices which have the interface are connected to a network. There are certain lines of prompts to use to pick up interfaces and have details of them displayed on the computer screen. Details can also be showed in tables such as routing tables.

Data packets being sent and received between devices connected to a network using the transfer control protocol will have detail of the protocol in the packets. These details can be found in the packets when they are captured using a packet-sniffing tool or utilities on the computer that use command prompts.

Tables:

A routing table is useful to see where data packets are sent to and received from on a network. It is also useful to see which network connections or interfaces are being used to send and receive data packets. It uses routing algorithms to see which route the packets need to take from the source host to the destination host. Each and every router within the network stores the routing table. Each router studies the header fields in the datagrams going through it.

A switch forwarding table shows the hosts MAC address, interface the host is reached by and the Time To Live of hosts sending and receiving data over the network. Every switch such as an ethernet switch which connects the host to the internet has a switch table with all this information entered. The ethernet switch stores and moves ethernet frames along the network. The switch learns which host is reached through which interface, where the sender is i.e. the location of the sender through

the local area network segment in the data frame passing through the switch and...when it receives the frame...

The ARP(Address resolution protocol) table stores the MAC and IP addresses of the host and the Time To Live. Each node on the local area network has this table. Host A does not have Bs MAC address so sends an ARP query packet containing Bs IP address. Query packet, containing MAC address of B as FF-FF-FF-FF-FF-FF(since A does not know the address), is sent over the network and received by B. B responds to the query by sending its MAC address to A's MAC address in a unicast frame. A then saves i.e. caches the pair as information in the ARP table until the information is no longer new.

Other routing tables store values in binary format and the output link, which is the channel the data packets travel along from the source to the destination host. The values in binary format are stored in the header of the data packets which moves along the network. Each of these value in the table have the output link, as a number, for the packets to travel along.

A forwarding table stored by each router as data packets are being forwarded along the network stores the destination address and the output link as a number.

ARP does not need an administrator to enter information in the ARP table plus they work with subnets. A subnet is made of interfaces for devices which have the same subnet portion of IP address. Splitting the IP into a subnet is splitting the IP into a subnet portion and a host portion.

The Practical Session:

This section focuses on typing prompts as commands to find details of, set addresses and activate or deactivate available network interfaces. It also focuses on using commands to show routing tables of information about interfaces connected to our computer. This is to be done on the virtual machine called Ubuntu which I installed on our computer.

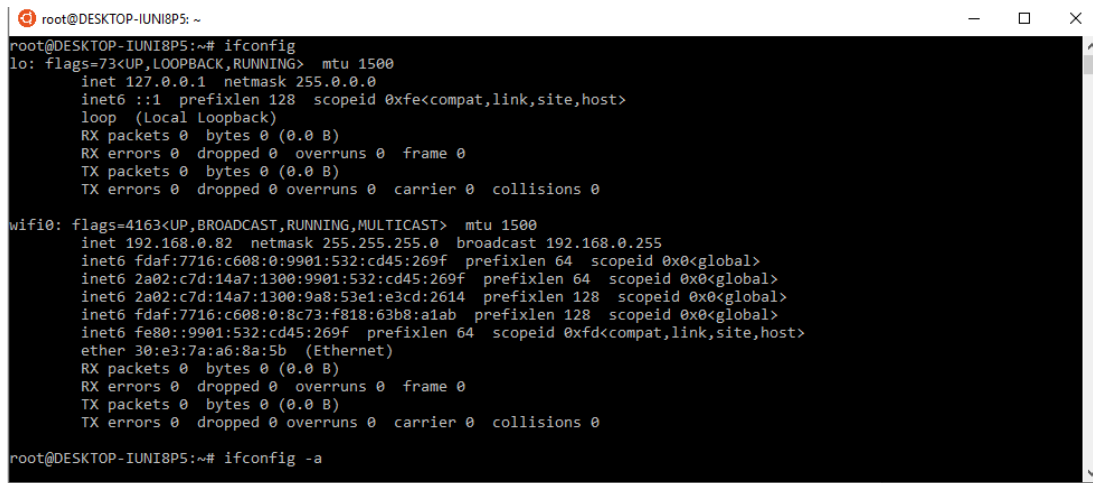
Ifconfig is short for interface configuration used in the utility for working on systems or networks in the Linux/Unix environment to look at, look for, change or find network connections or information to do with networks that are connected by typing lines of commands with options. Typing commands with arguments is like using them with options.

Ifconfig is the command used to give IP address, netmask or broadcast address to a network interface and send commands with arguments to get certain types of information. You can check details of the connection to the network that should be useful such as if the connection to the larger network e.g. the internet is working or there are connections problems such as the computer being suddenly disconnected from the internet. The command is also used for making and giving another name to an interface and activating and deactivating interfaces i.e. turning them on or off.

I will try the ifconfig commands to check and deal with network interfaces on our computer for this task on the virtual machine in the Linux environment.

1. Understand the use of the ifconfig command

A1. find out the MAC address and the allocated IP address for the active network interfaces.

A terminal window titled 'root@DESKTOP-IUNI8P5: ~' showing the output of the 'ifconfig' command. The output is divided into two sections: one for the 'lo' (loopback) interface and one for the 'wifi0' (wireless) interface. The 'lo' section shows an IP address of 127.0.0.1, a netmask of 255.0.0.0, and various statistics. The 'wifi0' section shows an IP address of 192.168.0.82, a netmask of 255.255.255.0, a broadcast address of 192.168.0.255, and several MAC addresses (fdaf:7716:c608:0:9901:532:cd45:269f, 2a02:c7d:14a7:1300:9a8:53e1:e3cd:2614, fdaf:7716:c608:0:8c73:f818:63b8:a1ab, fe80::9901:532:cd45:269f) along with an Ethernet MAC address of 30:e3:7a:a6:8a:5b. Both sections include statistics for RX and TX packets, bytes, errors, and collisions.

```
root@DESKTOP-IUNI8P5:~# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 1500
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0xfe<compat,link,site,host>
    loop (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

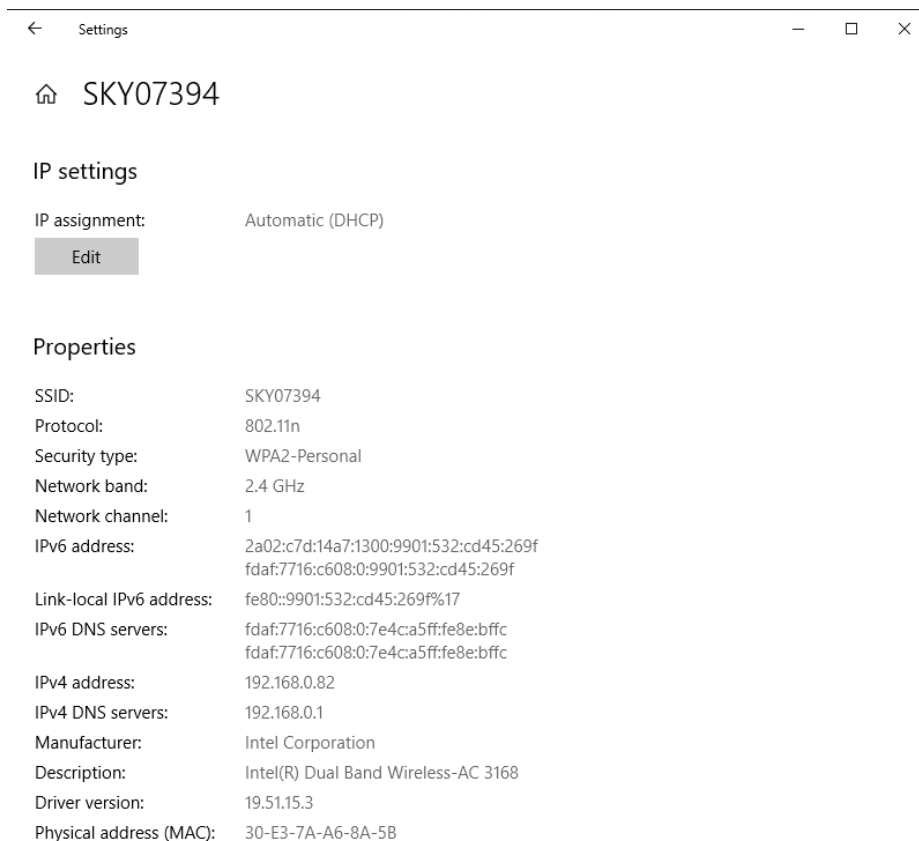
wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.82 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fdaf:7716:c608:0:9901:532:cd45:269f prefixlen 64 scopeid 0x0<global>
    inet6 2a02:c7d:14a7:1300:9a8:53e1:e3cd:2614 prefixlen 64 scopeid 0x0<global>
    inet6 2a02:c7d:14a7:1300:9a8:53e1:e3cd:2614 prefixlen 128 scopeid 0x0<global>
    inet6 fdaf:7716:c608:0:8c73:f818:63b8:a1ab prefixlen 128 scopeid 0x0<global>
    inet6 fe80::9901:532:cd45:269f prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 30:e3:7a:a6:8a:5b (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@DESKTOP-IUNI8P5:~# ifconfig -a
```

Here I run the ifconfig command line without any arguments to display details of connections between our host/router and the internet i.e. interfaces which are active. Details of the interfaces most importantly include addresses such as their IP and MAC addresses.

As shown in the shot above, the interfaces we have are a wireless interface “wifi0” and a loopback interface “lo”. The wireless connection “wifi0” has a MAC address for the ethernet. The MAC address for this interface is the ethernet address labelled ether and is 30:e3:7a:a6:8a:5b. Our computer uses a wireless connection and a MAC address is needed for this wireless connection and a wired (Ethernet) connection if our computer used one. Our IP (Internet Protocol) address is the inet address for “wifi0” which is 192.168.0.82.

The active network interface lo which is a loopback interface has a Mask 255.0.0.0. The allocated IP address for “lo” is the usual inet address 127.0.0.1



```
wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.82 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fdaf:7716:c608:0:9901:532:cd45:269f prefixlen 64 scopeid 0x0<global>
    inet6 2a02:c7d:14a7:1300:9901:532:cd45:269f prefixlen 64 scopeid 0x0<global>
    inet6 2a02:c7d:14a7:1300:9a8:53e1:e3cd:2614 prefixlen 128 scopeid 0x0<global>
    inet6 fdaf:7716:c608:0:8c73:f818:63b8:a1ab prefixlen 128 scopeid 0x0<global>
    inet6 fe80::9901:532:cd45:269f prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 30:e3:7a:a6:8a:5b (Ethernet)
```

In fact all the necessary details of our network connection are given as properties in the settings for our network connection on our computer including the terms used in this topic such as protocol, channel, Address, DNS, MAC and SSID. Most of the details given match the details of our interfaces displayed by ifconfig including our IP address and MAC address. Our IP which is the inet address is given as the IPv4 address. All the inet6 addresses are given as link-local and addresses of DNS servers. Our MAC address which is the Physical address matches the address of the Ethernet although it is in capitals.

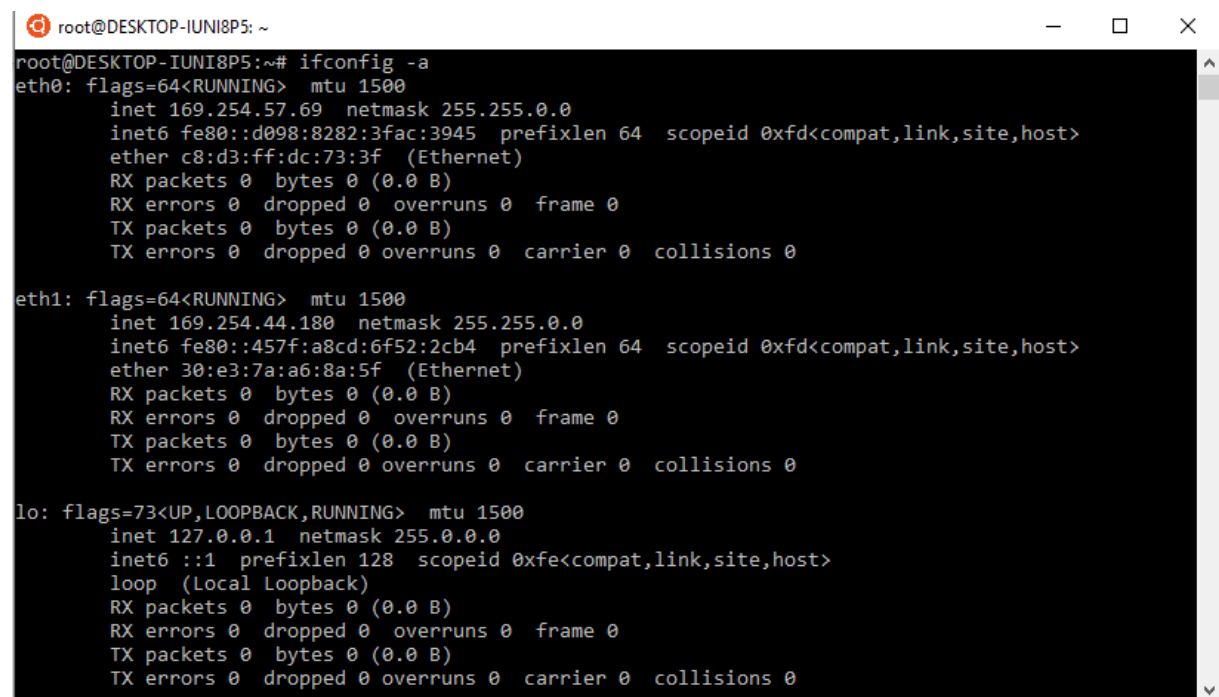
A2: Do you have a loopback interface being showed? If it is, explain

what are loopback interfaces and how they are used

The interface lo is a loopback interface which is being showed. A loopback interface is an interface built into the computer that is used to see if the computer can send and receive packets of data

using the protocols TCP and IP between itself. Loopbacks are also used to test how well the connection between a computer and a server running on it is such as when the client communicates with the server to request a web page. Loopbacks are given IP addresses in the 127.0.0.0/8 address range. The IP is 127.0.0.1 broadcast via the address 255.255.255.254 for your computer. There is one IP address that works for loopbacks being 127.0.0.1 since this is the inet for the loopback on our computer and other people's computers.

I now run the command `Ifconfig` followed by the argument `-a`



```
root@DESKTOP-IUNI8P5: ~  
root@DESKTOP-IUNI8P5:~# ifconfig -a  
eth0: flags=64<RUNNING> mtu 1500  
    inet 169.254.57.69 netmask 255.255.0.0  
    inet6 fe80::d098:8282:3fac:3945 prefixlen 64 scopeid 0xfd<compat,link,site,host>  
    ether c8:d3:ff:dc:73:3f (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=64<RUNNING> mtu 1500  
    inet 169.254.44.180 netmask 255.255.0.0  
    inet6 fe80::457f:a8cd:6f52:2cb4 prefixlen 64 scopeid 0xfd<compat,link,site,host>  
    ether 30:e3:7a:a6:8a:5f (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 1500  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0xfe<compat,link,site,host>  
    loop (Local Loopback)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
Select root@DESKTOP-IUNI8P5: ~
wifio: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.82 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fdaf:7716:c608:0:9901:532:cd45:269f prefixlen 64 scopeid 0x0<global>
    inet6 2a02:c7d:14a7:1300:9901:532:cd45:269f prefixlen 64 scopeid 0x0<global>
    inet6 2a02:c7d:14a7:1300:841e:e1ad:37a4:f1f9 prefixlen 128 scopeid 0x0<global>
    inet6 fdaf:7716:c608:0:b1b5:977e:535b:16ca prefixlen 128 scopeid 0x0<global>
    inet6 fe80::9901:532:cd45:269f prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 30:e3:7a:a6:8a:5b (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wifii: flags=64<RUNNING> mtu 1500
    inet 169.254.84.128 netmask 255.255.0.0
    inet6 fe80::f544:363d:71b3:5480 prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 30:e3:7a:a6:8a:5c (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wifii2: flags=64<RUNNING> mtu 1500
    inet 169.254.112.1 netmask 255.255.0.0
    inet6 fe80::b00f:221d:b421:7001 prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 32:e3:7a:a6:8a:5b (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

This command with the argument -a displays details of all the interfaces that are running or not.

I then run the command Ifconfig followed by the argument eth0

```
root@DESKTOP-IUNI8P5: ~
root@DESKTOP-IUNI8P5:~# ifconfig eth0
eth0: flags=64<RUNNING> mtu 1500
    inet 169.254.57.69 netmask 255.255.0.0
    inet6 fe80::d098:8282:3fac:3945 prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether c8:d3:ff:dc:73:3f (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@DESKTOP-IUNI8P5:~#
```

This command displays details of the specific interface which is called eth0.

A3:

UP : This keyword when used in the prompt line is used to activate a network interface which is not yet activated or ready for communication. It turns the interface on ready to send and receive data.

BROADCAST: This keyword is used for setting a broadcast address to an interface. The broadcast is used to send data to all the devices connected to a network. The address is used as an address of a network so that any device connected to the network sends and receives data in the form of

datagrams. If a host sends a datagram with address 255.255.255.255 as the destination, the message is received by all hosts connected to the same subnet.

MULTICAST: This semantic is used to send data to a group of devices connected to a network. It is used by a router to route data to other routers on a network to make themselves known to each other on the network. Packets of data are routed to many devices or even many packets are routed to many addresses.

MTU: This is the maximum transmission unit used for setting a limit to the size of packets of data before they are transmitted through an interface. A size of packets as big as 1000 can be set before they are transmitted.

Turning an interface on or off

The command `ifconfig eth0 up` turns a network interface on and the command `ifconfig eth0 down` turns an interface off if it is activated.

This is how they are entered and their function:

`ifconfig eth0 up` - Turn network interface on

`ifconfig eth0 down` - Turn network interface off

Setting an IP, Netmask and broadcast to a network interface

The commands `ifconfig eth0` followed by the IP assigns the IP to the interface `eth0`, `ifconfig eth0 netmask 255.255.255.254` sets the netmask to `eth0` and `ifconfig eth0 broadcast` followed by the address gives the broadcast address to `eth0`.

This is how they are entered and their function:

`ifconfig eth0 192.168.1.7` - assign the IP address 192.168.1.7 to `eth0`

`ifconfig eth0 netmask 255.255.255.254` - set the netmask to `eth0`

`ifconfig eth0 broadcast 192.168.1.255` - give broadcast address 192.168.1.255 to `eth0`

A4: Explain what is netmask and how it is used only if you did not do so as part of A2.

Netmask is a 32 bit mask used to split an IP address into a subnet. Netmasks are classed in 8,16 and 24 bits. The classes are Class A(for 8 bits being 255.0.0.0), Class B(for 16 bits being 255.255.0.0) and Class C(for 24 bits being 255.255.255.0). The 32 bit netmask 255.255.255.255 is a broadcast address which does not let hosts and networks connect to it. The last 255 in the address makes it a broadcast.

A Netmask with a greater length can have more networks which from Class A to Class C there are less hosts and therefore the number of networks and subnetworks increases. The commonly used Netmask is the 24 bit netmask 255.255.255.0 which can have more networks or subnetworks and enough hosts. The formula $2^{(\text{length of netmask} - \text{no. of segments used})} - 2$ can be used to work out how many networks a netmask can have.

Changing the MAC address of a network interface

If a MAC address of an interface is wanted to be changed it is done so by running `ifconfig` with `hw ether` and the address. This is `ifconfig hw ether AA : BB : DD : EE : FF : CC`

A5: To prevent a MAC address spoofing attack you first have to know how and why a spoofing attack happens. A spoofing attack happens by a bad person sending a packet of data using a false address. In this case a false MAC address. They do it to get through to the control server and pose as another device attached to the network. A means if preventing a spoofing attack is binding the port to the MAC address so the computer only recognises the MAC address and the port binded to it when the port receives incoming traffic. There is no incoming traffic if the port and MAC are not the same as the MAC and the port binded to the MAC.

2. The routing table and the use of the route command.

A utility that gives statistics about networks that are connected to the computer is the network statistics utility. It can be used on both Windows and Linux/Unix computers. The command is used with options to show different information.

netstat is used on the utility to show information of network connections coming in and out (following TCP and UDP), the routing table and details of interfaces being used. Information in the routing table or to do with the routing table is of network connections to the host computer that is using the network statistics utility to display the routing table.

If packets are to pass through a network a device has to know the way to the network it is going to.

A device agrees it is connected to a network if it has an IP address and a network mask set up and the route to the network, which is not put into the table by administrators but automatically like ARP tables. Information about data being passed along the connection i.e. interface is used to put routes into tables automatically.

A6:

I start with the command netstat -r

```
root@DESKTOP-IUNI8P5: ~  
root@DESKTOP-IUNI8P5:~# netstat -r  
Kernel IP routing table  
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface  
127.0.0.0         0.0.0.0          255.0.0.0       U        0 0        0 lo  
127.0.0.1         0.0.0.0          255.255.255.255 U        0 0        0 lo  
127.255.255.255  0.0.0.0          255.255.255.255 U        0 0        0 lo  
224.0.0.0         0.0.0.0          240.0.0.0       U        0 0        0 lo  
255.255.255.255  0.0.0.0          255.255.255.255 U        0 0        0 lo  
0.0.0.0          SkyRouter.Home    255.255.255.255 U        0 0        0 wifi0  
192.168.0.0       0.0.0.0          255.255.255.0   U        0 0        0 wifi0  
192.168.0.82      0.0.0.0          255.255.255.255 U        0 0        0 wifi0  
192.168.0.255     0.0.0.0          255.255.255.255 U        0 0        0 wifi0  
224.0.0.0         0.0.0.0          240.0.0.0       U        0 0        0 wifi0  
255.255.255.255  0.0.0.0          255.255.255.255 U        0 0        0 wifi0  
root@DESKTOP-IUNI8P5:~#
```

A6: Explain how the route table works by go through the meaning of each column of this table such as Destination, Gateway, Flags, Refs, Use, Netif and Expire

Like the ARP and switch forwarding table the route table works by data being sent and received through routers over the network and displaying information of where will be routed to including addresses and interfaces being used. The routing table above on our machine is the kernel routing table depending on the TCP/IP configuration of our machine, output by netstat -r. Therefore there are different columns being used. Information of the addresses, connections and times taken that are to do with the route are displayed in the columns.

The different columns being used in the table are Genmask, MSS, Window and IRTT instead of Refs, Use, Netif and Expire. The MSS, Window and IRTT columns are about the Transport Control Protocol (TCP) being used over the connection.

The routing table columns of this kernel are:

Destination – The address of the network or host the data is being sent to.

Gateway – In case no network is directly connected the default gateway is used to keep sending messages to a device that, for a reason has information about the network.

Genmask – This is the netmask given for a destination network. As you can see in the table, a host has destination 255.255.255.255 and a default route has 0.0.0.0 for example 240.0.0.0. Genmask is the name of the column to show how general the netmask i.e. route is.

Flags – Flags information about the network with letters which have different meanings such as C which means the entry is saved i.e. cached, H which means the data is going to a host, ! which means don't go down the route, G means a gateway address is being used and S means another router needs to be added to the route. A column of all U's meaning all the routes are active i.e. up as shown in our routing table. Every route is flagged by a 'U' which stands for 'up'.

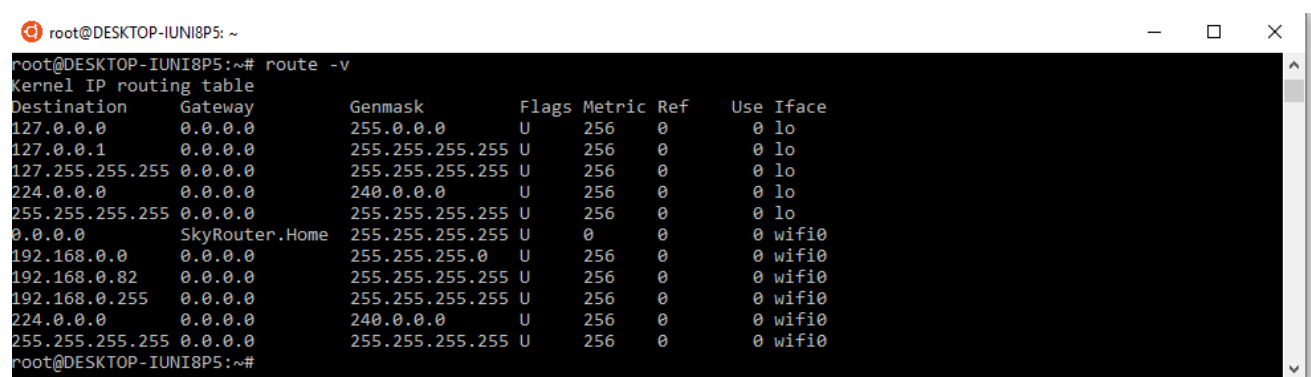
MSS – This stands for the Maximum Segment Size, which is set as a default, of the TCP connections being used over the route. The transfer control protocol is the control, format, order of and response to data being transferred between devices such as computers over a network and this is the maximum size of the protocol segment especially if it is in a link layer frame.

Window – This is the maximum window size, which is set as a default, of the TCP connections being used over the route. The window, having the TCP being used to control the transfer of data between devices on the network, has a maximum size especially if it is in a data frame.

IRTT – This stands for the Initial Round Trip Time which is used by the Kernel to decide which are the best TCP parameters being used over the connection in case it takes time to receive the actual TCP parameters.

Iface – This is the interface the packets will be sent to along the route.

I can also display the same routing table with columns that are different to this one by using the route command instead of netstat, with argument -v. The same routing table showing details of our network routes with columns Metric, Ref and Use instead of MSS, Window and IRTT.



```
root@DESKTOP-IUNI8P5: ~  
root@DESKTOP-IUNI8P5:~# route -v  
Kernel IP routing table  
Destination Gateway Genmask Flags Metric Ref Use Iface  
127.0.0.0 0.0.0.0 255.0.0.0 U 256 0 0 lo  
127.0.0.1 0.0.0.0 255.255.255.255 U 256 0 0 lo  
127.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 lo  
224.0.0.0 0.0.0.0 240.0.0.0 U 256 0 0 lo  
255.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 lo  
0.0.0.0 SkyRouter.Home 255.255.255.255 U 0 0 0 wifio  
192.168.0.0 0.0.0.0 255.255.255.0 U 256 0 0 wifio  
192.168.0.82 0.0.0.0 255.255.255.255 U 256 0 0 wifio  
192.168.0.255 0.0.0.0 255.255.255.255 U 256 0 0 wifio  
224.0.0.0 0.0.0.0 240.0.0.0 U 256 0 0 wifio  
255.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 wifio  
root@DESKTOP-IUNI8P5:~#
```

These columns are:

Metric – how far it is to the where the data packets are going which is usually the number of hops to where the packets are going.

Ref – this columns shows the number of users of a router. Protocols for connections stay on one route while there is the connection the protocol is for.

Use – This column shows the number of packets being sent along the given route.

Other columns not displayed on our computer are:

Netif – Like the Iface column shows the interface that is to do with the route.

Expire – This is the time taken for the route to expire i.e. how long it has been since the host stopped responding to the route.

Now I issue the following command:

route /?

```
root@DESKTOP-IUNI8P5:~# route /?
Usage: route [-nNvee] [-FC] [<AF>]      List kernel routing tables
       route [-v] [-FC] {add|del|flush} ... Modify routing table for AF.

       route {-h|--help} [<AF>]          Detailed usage syntax for specified AF.
       route {-V|--version}              Display version/author and exit.

       -v, --verbose                     be verbose
       -n, --numeric                     don't resolve names
       -e, --extend                      display other/more information
       -F, --fib                         display Forwarding Information Base (default)
       -C, --cache                       display routing cache instead of FIB

<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
```

This command shows the arguments that can be used with the route command like the one I used to show the same routing table but with different columns. The arguments can be used to change, add, remove or display specific information entered about the route in the routing table.

For Windows systems here is a list of the functions of commands:

route PRINT: This command outputs the route that is running i.e. active.

route ADD: Add a route (followed by the network gateway e.g. 0.0.0.0 and the mask gateway IP)

route CHANGE: Change a route that is currently being used

route DELETE: Remove a route (by typing the network gateway after the DELETE option)

For Linux systems:

-F: This prints info about routes where the data packets are being sent along i.e. forwarded since the -F argument is for showing forwarding info in the table called a forwarding information base as shown below.

```
root@DESKTOP-IUNI8P5:~# route -F
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
127.0.0.0 0.0.0.0 255.0.0.0 U 256 0 0 lo
127.0.0.1 0.0.0.0 255.255.255.255 U 256 0 0 lo
127.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 lo
224.0.0.0 0.0.0.0 240.0.0.0 U 256 0 0 lo
255.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 lo
0.0.0.0 SkyRouter.Home 255.255.255.255 U 0 0 0 wifi0
192.168.0.0 0.0.0.0 255.255.255.0 U 256 0 0 wifi0
192.168.0.82 0.0.0.0 255.255.255.255 U 256 0 0 wifi0
192.168.0.255 0.0.0.0 255.255.255.255 U 256 0 0 wifi0
224.0.0.0 0.0.0.0 240.0.0.0 U 256 0 0 wifi0
255.255.255.255 0.0.0.0 255.255.255.255 U 256 0 0 wifi0
```

route add: Same as Windows. Add a route.

route del: Same as Windows. Remove a route.

To change a route that is currently being used use the options route del and route add.

```
Select root@DESKTOP-IUNI8P5: ~
root@DESKTOP-IUNI8P5:~# route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.0      0.0.0.0         255.0.0.0       U        0     0        0 lo
127.0.0.1      0.0.0.0         255.255.255.255 U        0     0        0 lo
127.255.255.255 0.0.0.0         255.255.255.255 U        0     0        0 lo
224.0.0.0      0.0.0.0         240.0.0.0       U        0     0        0 lo
255.255.255.255 0.0.0.0         255.255.255.255 U        0     0        0 lo
0.0.0.0        192.168.0.1     255.255.255.255 U        0     0        0 wifi0
192.168.0.0    0.0.0.0         255.255.255.0   U        0     0        0 wifi0
192.168.0.82   0.0.0.0         255.255.255.255 U        0     0        0 wifi0
192.168.0.255  0.0.0.0         255.255.255.255 U        0     0        0 wifi0
224.0.0.0      0.0.0.0         240.0.0.0       U        0     0        0 wifi0
255.255.255.255 0.0.0.0         255.255.255.255 U        0     0        0 wifi0
```

According to the details the argument -n is for numeric which shows information expressed in numbers instead of words or names. The gateway Skyrouter.home is expressed in numbers which is the address 192.168.0.1.

The argument -v I used previously stands for verbose which means to use more words than are needed to be used to show information. The table outputs as many words that are needed to be used such as the name of the gateway which is SkyRouter.Home. The base station we are using in our home and our internet service provider is the popular brand Sky.

If we wanted to delete a route from the routing table we would start with running the command route PRINT to output the default gateway route and then run the command route DELETE * where * is the address of the network such as 0.0.0.0.

A7: When I run route PRINT I get the following output. This output is just details of the route command which is the same as the details I get when I run route /?. So far the PRINT option does not output the default gateway route.

```
Select root@DESKTOP-IUNI8P5: ~
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
root@DESKTOP-IUNI8P5:~# route PRINT
Usage: route [-nNvee] [-FC] [<AF>]
       route [-v] [-FC] {add|del|flush} ... Modify routing table for AF.

route [-h|--help] [<AF>]
route [-V|--version]
       Detailed usage syntax for specified AF.
       Display version/author and exit.

-v, --verbose           be verbose
-n, --numeric           don't resolve names
-e, --extend            display other/more information
-F, --fib               display Forwarding Information Base (default)
-C, --cache             display routing cache instead of FIB

<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
root@DESKTOP-IUNI8P5:~#
```

And then the following:

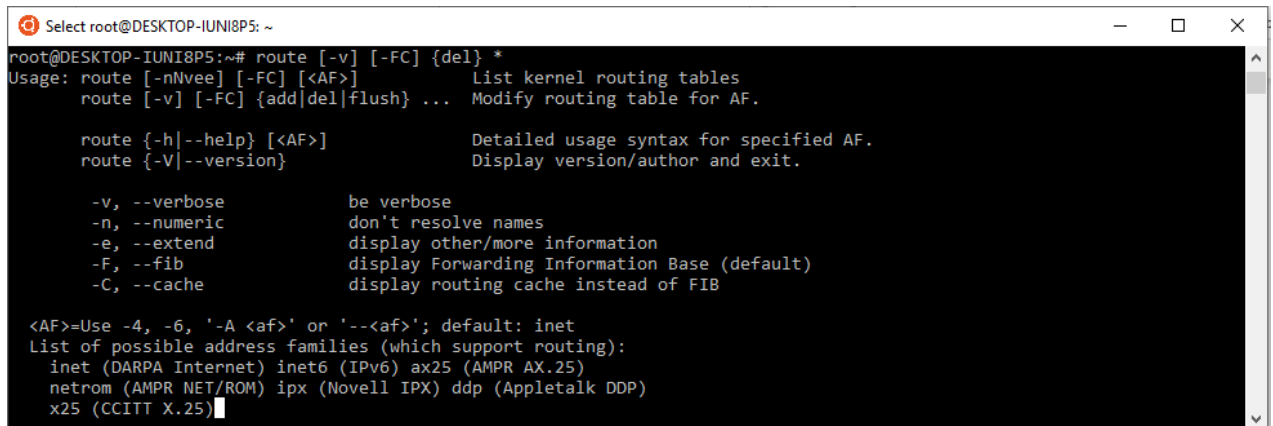
First the route DELETE * to remove the gateway route that was initially provided.

Next the route DELETE 0.0.0.0

The third time I run the route del * command

And fourth the route del 0.0.0.0 command.

With the Linux Kernel running on our computer we have its own arguments that can be used with the route command as route [-v] [-FC] {del} *. So I decide to run that.



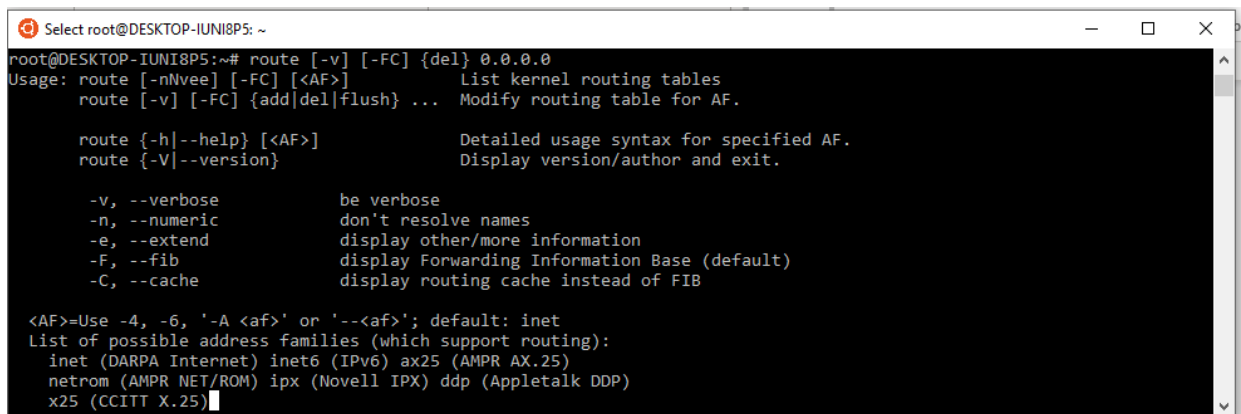
```
Select root@DESKTOP-IUNI8P5: ~
root@DESKTOP-IUNI8P5:~# route [-v] [-FC] {del} *
Usage: route [-nNvee] [-FC] [<AF>]          List kernel routing tables
       route [-v] [-FC] {add|del|flush} ...  Modify routing table for AF.

       route {-h|--help} [<AF>]              Detailed usage syntax for specified AF.
       route {-V|--version}                  Display version/author and exit.

       -v, --verbose                        be verbose
       -n, --numeric                        don't resolve names
       -e, --extend                        display other/more information
       -F, --fib                           display Forwarding Information Base (default)
       -C, --cache                         display routing cache instead of FIB

<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
  inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
  x25 (CCITT X.25)
```

I then change it to route [-v] [-FC] {del} 0.0.0.0



```
Select root@DESKTOP-IUNI8P5: ~
root@DESKTOP-IUNI8P5:~# route [-v] [-FC] {del} 0.0.0.0
Usage: route [-nNvee] [-FC] [<AF>]          List kernel routing tables
       route [-v] [-FC] {add|del|flush} ...  Modify routing table for AF.

       route {-h|--help} [<AF>]              Detailed usage syntax for specified AF.
       route {-V|--version}                  Display version/author and exit.

       -v, --verbose                        be verbose
       -n, --numeric                        don't resolve names
       -e, --extend                        display other/more information
       -F, --fib                           display Forwarding Information Base (default)
       -C, --cache                         display routing cache instead of FIB

<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
  inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
  x25 (CCITT X.25)
```

A8:

I study the routing tables after running each of those commands.

```
root@DESKTOP-IUNI8P5: ~  
root@DESKTOP-IUNI8P5:~# netstat -r  
Kernel IP routing table  
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface  
127.0.0.0         0.0.0.0          255.0.0.0       U        0 0        0 lo  
127.0.0.1         0.0.0.0          255.255.255.255 U        0 0        0 lo  
127.255.255.255   0.0.0.0          255.255.255.255 U        0 0        0 lo  
224.0.0.0         0.0.0.0          240.0.0.0       U        0 0        0 lo  
255.255.255.255   0.0.0.0          255.255.255.255 U        0 0        0 lo  
0.0.0.0           SkyRouter.Home    255.255.255.255 U        0 0        0 wifi0  
192.168.0.0       0.0.0.0          255.255.255.0   U        0 0        0 wifi0  
192.168.0.82      0.0.0.0          255.255.255.255 U        0 0        0 wifi0  
192.168.0.255     0.0.0.0          255.255.255.255 U        0 0        0 wifi0  
224.0.0.0         0.0.0.0          240.0.0.0       U        0 0        0 wifi0  
255.255.255.255   0.0.0.0          255.255.255.255 U        0 0        0 wifi0
```

```
root@DESKTOP-IUNI8P5: ~  
root@DESKTOP-IUNI8P5:~# route -n  
Kernel IP routing table  
Destination      Gateway          Genmask         Flags Metric Ref  Use Iface  
127.0.0.0         0.0.0.0          255.0.0.0       U        256 0    0 lo  
127.0.0.1         0.0.0.0          255.255.255.255 U        256 0    0 lo  
127.255.255.255   0.0.0.0          255.255.255.255 U        256 0    0 lo  
224.0.0.0         0.0.0.0          240.0.0.0       U        256 0    0 lo  
255.255.255.255   0.0.0.0          255.255.255.255 U        256 0    0 lo  
0.0.0.0           192.168.0.1     255.255.255.255 U        0 0    0 wifi0  
192.168.0.0       0.0.0.0          255.255.255.0   U        256 0    0 wifi0  
192.168.0.82      0.0.0.0          255.255.255.255 U        256 0    0 wifi0  
192.168.0.255     0.0.0.0          255.255.255.255 U        256 0    0 wifi0  
224.0.0.0         0.0.0.0          240.0.0.0       U        256 0    0 wifi0  
255.255.255.255   0.0.0.0          255.255.255.255 U        256 0    0 wifi0
```

Both tables still show the same information about the route. So far the route delete commands I have run have not removed any gateway routes.

```
Select root@DESKTOP-IUNI8P5: ~  
root@DESKTOP-IUNI8P5:~# route ADD 0.0.0.0 MASK 0.0.0.0 192.168.0.82  
Usage: route [-nNvee] [-FC] [<AF>]          List kernel routing tables  
       route [-v] [-FC] {add|del|flush} ...  Modify routing table for AF.  
  
       route {-h|--help} [<AF>]             Detailed usage syntax for specified AF.  
       route {-V|--version}                 Display version/author and exit.  
  
       -v, --verbose                        be verbose  
       -n, --numeric                        don't resolve names  
       -e, --extend                        display other/more information  
       -F, --fib                           display Forwarding Information Base (default)  
       -C, --cache                         display routing cache instead of FIB  
  
<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet  
List of possible address families (which support routing):  
  inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)  
  netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)  
  x25 (CCITT X.25)
```

I could try as many options given here but that could take too much time and I could end up putting too many screenshots with explanations on this assignment. I also cannot run the Add command to put the default gateway back without deleting it.

If the default gateway had been removed some addresses in the destination, gateway and genmask column would probably not be shown in the table. The flag column would probably show some exclamation marks, rather than all U's, that some of the routes have no data going down them. This

is useful to see if computers connected to the local area network can be accessed and if the gateway route has to be put back.

A9:

I have not managed to delete and add the default gateway route so I will not be studying the routing table to check the route has been restored.

Element 2

Intro

This element of the assignment is about wireless network connections. Devices connected as a network or to a network wirelessly, i.e. without wires. We have the wired network connections where devices are connected using wires and cables such as an Ethernet cable (that looks and works just like a telephone cable) as a network or to a network. This section focuses on wireless network connections working too with wired connections where devices such as computers, mobile phones and servers connect to larger networks through transmitters, devices known as access points and stations known as base stations.

There is the local area network (LAN) being wireless known as 802.11 wireless LAN. This is used for wireless network connectivity and works by sending data to and from devices and access points for wireless connections. Data being sent is in the form of packets and data frames. There are also protocols used to send data between devices. A device has to communicate with a station known as an access point and a router to connect to a larger network such as the internet.

Channels are the communication path. The path of communication that connects each node together.

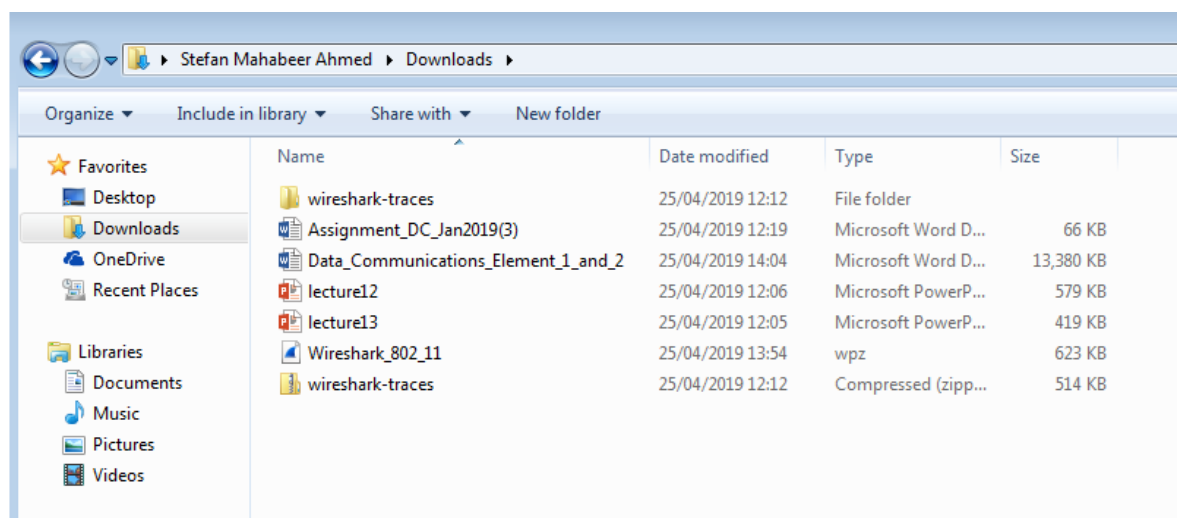
Devices such as computers, mobile phones and servers connect to larger networks such as the internet through access points, stations or base stations and routers. This involves them picking up

data from the access points(AP's) or stations and data being sent back and forth between the two. Data being sent back and forth is in the form of frames and protocols being used for the sending.

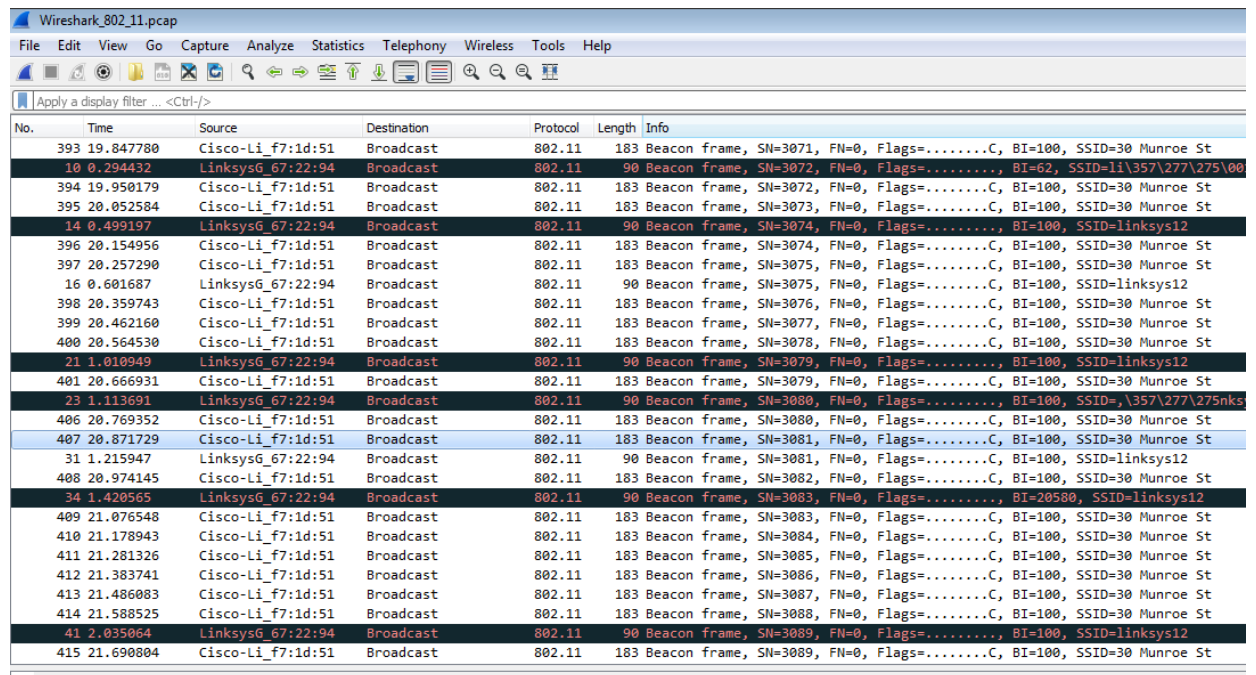
This section focuses on using the packet sniffing tool Wireshark on the computer to capture data packets during a live wireless network connection and study the captured packets by opening them. The packets captured contain data frames such as beacon frames with details of protocols, addresses, transmission and other necessary information.

The captured frames captured in this topic have the Transfer Control Protocol TCP segments. The TCP is the protocol that controls the transfer of messages being sent and received over a network including their format, order of and response.

1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?



First the downloaded trace file is captured, using Wireshark packet sniffing tool and Aircap, which is in stored in the downloads folder and opened from there.



No.	Time	Source	Destination	Protocol	Length	Info
393	19.847780	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3071, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=11\357\277\275\00
394	19.950179	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
395	20.052584	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3073, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=Linksys12
396	20.154956	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
397	20.257290	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=Linksys12
398	20.359743	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3076, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
399	20.462160	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3077, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
400	20.564530	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3078, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID=Linksys12
401	20.666931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
23	1.113691	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=, \357\277\275nks
406	20.769352	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
407	20.871729	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=Linksys12
408	20.974145	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3082, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
34	1.420565	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=.....C, BI=20580, SSID=Linksys12
409	21.076548	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3083, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
410	21.178943	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3084, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
411	21.281326	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3085, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
412	21.383741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3086, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
413	21.486083	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3087, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
414	21.588525	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3088, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
41	2.035064	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=Linksys12
415	21.690804	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Here is the trace file of all the packets that were captured from the wireless network connection. The data packets are mostly shown as frames between the devices sending the data. In fact data being sent to and from devices and access points is in the form off frames, known as beacon frames, as shown in this trace.

Connecting to the internet

A device such as a computer, laptop or a smartphone connects wirelessly to a larger network such as the internet through a base station or an access point. This is called association. The device or host connects to the internet through the base station or AP by checking channels, receiving beacon frames which have the Aps name (SSID) and MAC address. Then it carries out the authentication to using the MAC address and password of the AP to confirm association and connection to the larger network.

No.	Time	Source	Destination	Protocol	Length	Info
393	19.847780	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3071, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=lin\357\277\275\00
394	19.950179	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
395	20.052584	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3073, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=linksys12
396	20.154956	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
397	20.257290	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	0.601687	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
398	20.359743	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3076, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
399	20.462160	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3077, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
400	20.564530	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3078, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
21	1.010949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID=linksys12
401	20.666931	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
23	1.113691	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=lin\357\277\275nks
406	20.769352	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
407	20.871729	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
408	20.974145	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3082, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
34	1.420565	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3083, FN=0, Flags=.....C, BI=20580, SSID=linksys12
409	21.076548	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3083, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
410	21.178943	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3084, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
411	21.281326	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3085, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
412	21.383741	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3086, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
413	21.486083	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3087, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
414	21.588525	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3088, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
41	2.035064	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=linksys12
415	21.690804	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3089, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

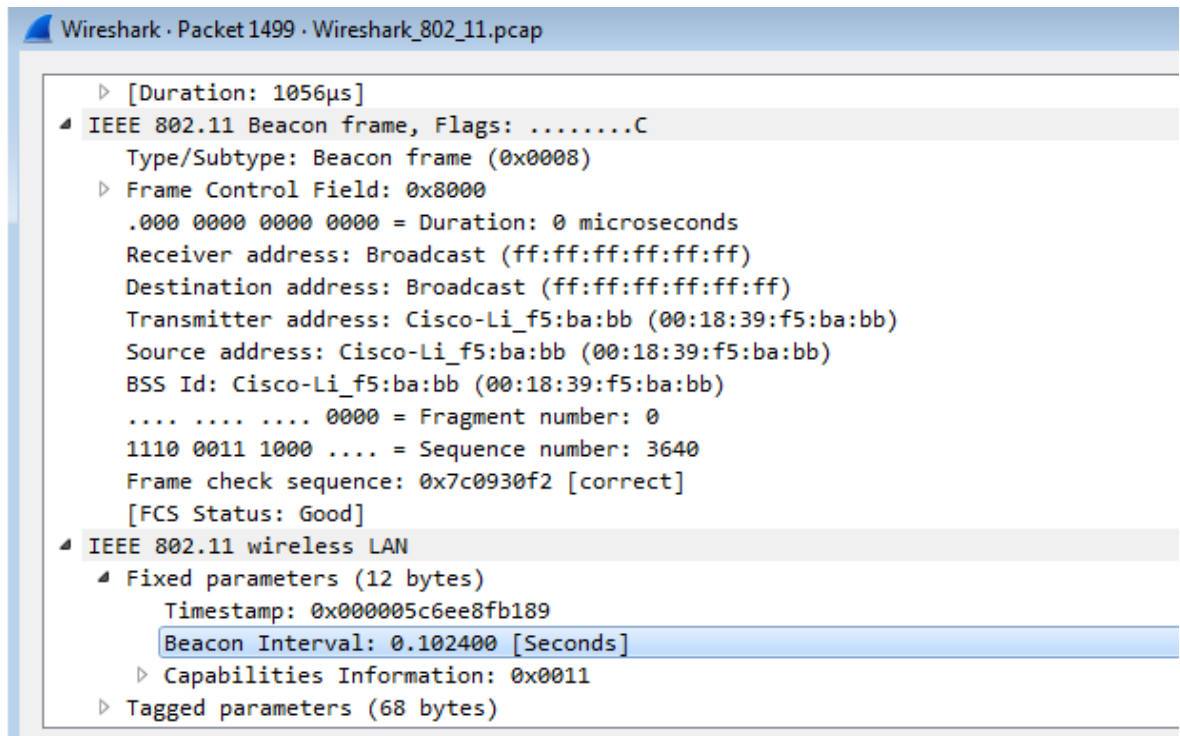
The SSID's of the two access points sending out most of the beacon frames to show they exist are 30 Munroe Street and *Linksys_SES_24086*.

SSID stands for Service Set Identifier – an identifier given to an access point or wireless station to identify it when it shows that it exists and connected to devices such as a computer or mobile phone to connect these devices to a network such as the internet. It is the name of the AP that shows on the list of APs in range that are ready to be connected to. Hence SSID in BSSID since an access point is part of a Basic Service Set. SSIDs and channel numbers are given to access points by network administrators when they are first set up and ready to be used.

2. What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

No.	Time	Source	Destination	Protocol	Length	Info
1800	52.306984	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3615, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1801	52.409458	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3616, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1802	52.511865	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3617, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1803	52.614237	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3618, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1804	52.716594	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3619, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1809	52.818980	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3620, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1895	56.102695	00:ac:20:67:22:94	5a:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3620, FN=4, Flags=.....C, BI=100, SSID=lin+m\357\277\275s[pack
1810	52.921323	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3621, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1811	53.023843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3622, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1812	53.126221	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3623, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1813	53.228606	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3624, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1814	53.330965	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3625, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1815	53.433332	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3626, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1816	53.535729	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3627, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1817	53.638203	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3628, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1818	53.740602	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3629, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1841	53.842947	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3630, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1842	53.945330	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3631, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1843	54.047713	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3632, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1844	54.150104	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3633, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1845	54.252616	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3634, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1846	54.354955	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3635, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1847	54.457361	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3636, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1848	54.559727	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3637, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1849	54.662085	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3638, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1850	54.764476	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3639, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1859	54.866954	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1499	42.532596	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1868	54.971071	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3641, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1873	55.072697	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3642, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1874	55.174099	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3643, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1513	42.039707	Cisco-Li_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3643, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1875	55.276451	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3644, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1876	55.378829	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3645, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1877	55.481339	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3646, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1878	55.583740	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3647, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

So here the data packet has been transmitted in the form of frames a.k.a 802.11 Wireless LAN frames which are beacon frames between the access points and the details of the packet are shown in the screenshot below.



The time interval of the transmission of the beacon frames - the linkisys_ses_24086 access point from the 30 munroe st access point is 0.1024 seconds. Shown above is this interval itself in the beacon frame in the 802.11 wireless LAN section listed as a fixed parameter.

3.What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

```

IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    ▷ Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... 0000 = Fragment number: 0
    1011 0011 0000 .... = Sequence number: 2864
    Frame check sequence: 0x7f8cf5af [correct]
    [FCS Status: Good]
  IEEE 802.11 wireless LAN
    Fixed parameters (12 bytes)
      Timestamp: 0x0000002896488182
      Beacon Interval: 0.102400 [Seconds]
      ▷ Capabilities Information: 0x0601
    Tagged parameters (119 bytes)
      Tagged parameter set: 30 Munroe St
0010 5e 00 00 47 af f5 8c 7f 80 00 00 00 ff ff ff ff ^..G....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 00 b3 ..Q....
0030 82 81 48 96 28 00 00 00 64 00 01 06 00 0c 33 30 ..H.(...d...30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St...
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI...
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e .....BC^
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 .b2/.*.2...$.H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 `l.....@....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01 .....P...
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....BC^b
00b0 32 2f 00 af f5 8c 7f 2/.....

```

The source MAC address on the beacon frame from 30 Munroe St is 00 16 b6 f7 1d 51 in hexadecimal notation (base 16 – each number is four bits e.g. 7 is 0111 in four bits). The address is listed in the beacon frame in brackets and at the bottom of the window where the content of the captured packet data is shown in hexadecimal and ascii format.

MAC (Multiple Access Control) Address

Here a MAC address is used in the fields in the frame. This is a 48 bit address different to IP addresses, which identifies devices used for connections in a network that use a protocol known as the medium access control protocol. Its job is to move a frame from an interface to another interface that is actually connected in a local area network. Hence it is the medium access control address of the device being used for connection....

...stored in the ROM chip of the network interface card and can sometimes be set using software

4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

```

IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  Flags: 0x00
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  .... .... 0000 = Fragment number: 0
  1011 0011 0000 .... = Sequence number: 2864
  Frame check sequence: 0x7f8cf5af [correct]
  [FCS Status: Good]
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
    Timestamp: 0x0000002896488182
    Beacon Interval: 0.102400 [Seconds]
  Capabilities Information: 0x00601
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e3 9c .....X.....
0010 5e 00 00 47 af f5 8c 7f 80 00 00 00 ff ff ff ff ^..G.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 00 b3 ..Q.....Q..
0030 82 81 48 96 28 00 00 00 64 00 01 06 00 0c 33 30 ..H.(...d....30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St.....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI...
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e .....BC^
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 ..b2/.*.2...$.H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 `l.....@.....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01 .....P...
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....BC^..b
00b0 32 2f 00 af f5 8c 7f 2/.....

```

The destination MAC address on the beacon frame from 30 Munroe St in hexadecimal notation is ff ff ff ff ff shown in the beacon frame as a broadcast and at the bottom of the window where the content of the captured packet data is shown in hexadecimal and ascii notation. It is only a pair of letter f's in this notation. Like ARP, MAC addresses are ff:ff:ff:ff:ff:ff when the sending host does not have the actual address while sending. This is an Ethernet broadcast i.e.it was broadcast along an ethernet interface which uses wires.

5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

```

IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  Flags: 0x00
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  .... .... 0000 = Fragment number: 0
  1011 0011 0000 .... = Sequence number: 2864
  Frame check sequence: 0x7f8cf5af [correct]
  [FCS Status: Good]
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
    Timestamp: 0x0000002896488182
    Beacon Interval: 0.102400 [Seconds]
  Capabilities Information: 0x0601

```

0000	00 00 18 00 ee 58 00 00	10 02 85 09 a0 00 e3 9cX.....
0010	5e 00 00 47 af f5 8c 7f	80 00 00 00 ff ff ff ff	^..G.....
0020	ff ff 00 16 b6 f7 1d 51	00 16 b6 f7 1d 51 00 b3Q.....
0030	82 81 48 96 28 00 00 00	64 00 01 06 00 0c 33 30	..H.(...d....30
0040	20 4d 75 6e 72 6f 65 20	53 74 01 04 82 84 8b 96	Munroe St.....
0050	03 01 06 05 04 00 01 00	00 07 06 55 53 49 01 0bUSI..
0060	1a 0c 12 0f 00 03 a4 00	00 27 a4 00 00 42 43 5e'...BC^
0070	00 62 32 2f 00 2a 01 00	32 08 8c 12 98 24 b0 48	..b2/*..2...\$..H
0080	60 6c dd 15 00 0a f5 0a	02 40 c0 00 03 01 03 05	`l.....@.....
0090	0e 04 ff 00 03 00 11 01	01 dd 18 00 50 f2 02 01P...
00a0	01 0f 00 03 a4 00 00 27	a4 00 00 42 43 5e 00 62'...BC^..b
00b0	32 2f 00 af f5 8c 7f		2/.....

The MAC BSS id on the beacon frame from 30 Munroe St is 00 16 b6 f7 1d 51 in hexadecimal notation, as shown where the content of captured packet data is shown in hexadecimal and ascii notation. This Id is the same as the source address.

The BSS id or Basic Service Set id is used to identify the basic service set. The basic service set is a set that consists of devices such as computers with an access point or a base station to connect the computers to a network such as the internet.

6. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?


```

Wireshark · Packet 20 · Wireshark_802_11.pcap

Frame check sequence: 0x7f8cf5af [correct]
[FCS Status: Good]
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
    Timestamp: 0x0000002896488182
    Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x0601
  Tagged parameters (119 bytes)
    Tag: SSID parameter set: 30 Munroe St
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 6
    Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag: Country Information: Country Code US, Environment Indoor
    Tag: EDCA Parameter Set
    Tag: ERP Information
    Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: Vendor Specific: Airgo Networks, Inc.
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e3 9c .....X..
0010 5e 00 00 47 af f5 8c 7f 80 00 00 00 ff ff ff ff ^..G.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 00 b3 .....Q.....
0030 82 81 48 96 28 00 00 00 64 00 01 06 00 0c 33 30 ..H.(...d....30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI..
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e .....BC^
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 ..b2/.*. 2....$.H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 ..1.....@.....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01 .....P...
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....BC^b
00b0 32 2f 00 af f5 8c 7f 2/.....

```

The four supported data rates are parameters that are tagged in this captured beacon frame. The rates are 1, 2, 5.5 and 11 Mbits/sec (Mbps).

```

Wireshark · Packet 20 · Wireshark_802_11.pcap

1011 0011 0000 .... = Sequence number: 2864
Frame check sequence: 0x7f8cf5af [correct]
[FCS Status: Good]
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
    Timestamp: 0x0000002896488182
    Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x0601
  Tagged parameters (119 bytes)
    Tag: SSID parameter set: 30 Munroe St
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 6
    Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag: Country Information: Country Code US, Environment Indoor
    Tag: EDCA Parameter Set
    Tag: ERP Information
    Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: Vendor Specific: Airgo Networks, Inc.
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e3 9c .....X..
0010 5e 00 00 47 af f5 8c 7f 80 00 00 00 ff ff ff ff ^..G.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 00 b3 .....Q.....
0030 82 81 48 96 28 00 00 00 64 00 01 06 00 0c 33 30 ..H.(...d....30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI..
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e .....BC^
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 ..b2/.*. 2....$.H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 ..1.....@.....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01 .....P...
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....BC^b
00b0 32 2f 00 af f5 8c 7f 2/.....

```

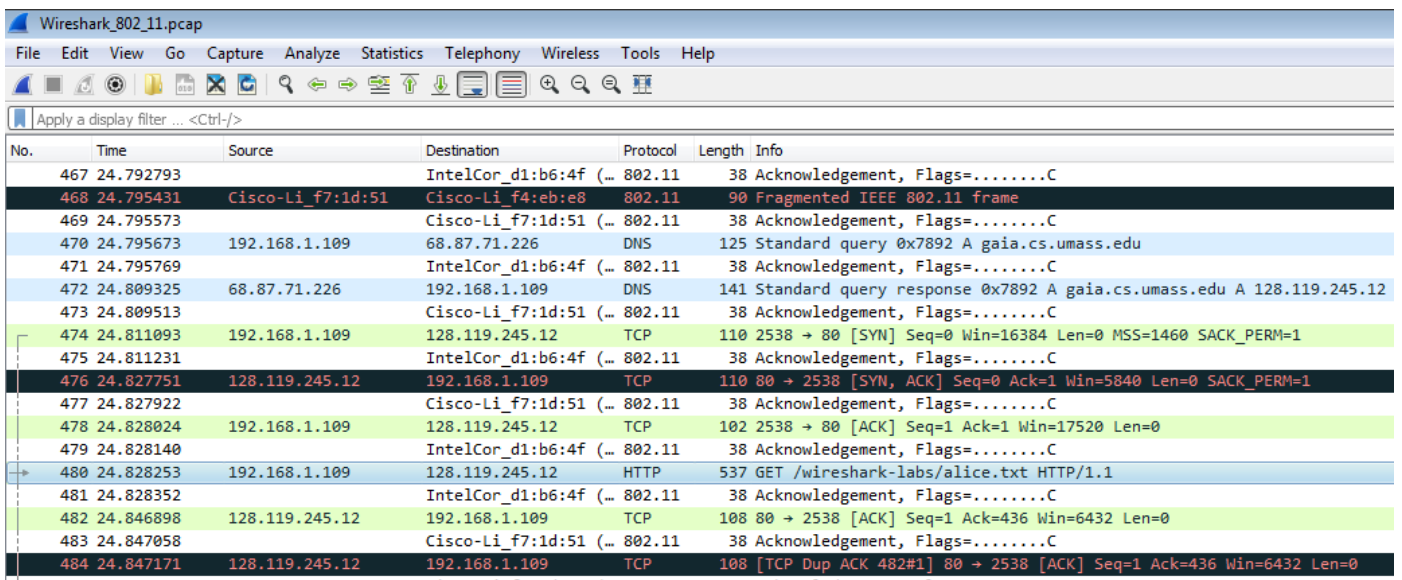
Eight extra support data rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mbits/sec (Mbps).

Transmission and data rates of wireless LANs

Data rates depend on the wireless link being supported by this access point and the host. There are many different 802.11 wireless LANs available that the host and AP may use such as 802.11a,g, 802.11ac, 802.11b, 802.11n and 802.15 with their own transmission rates in

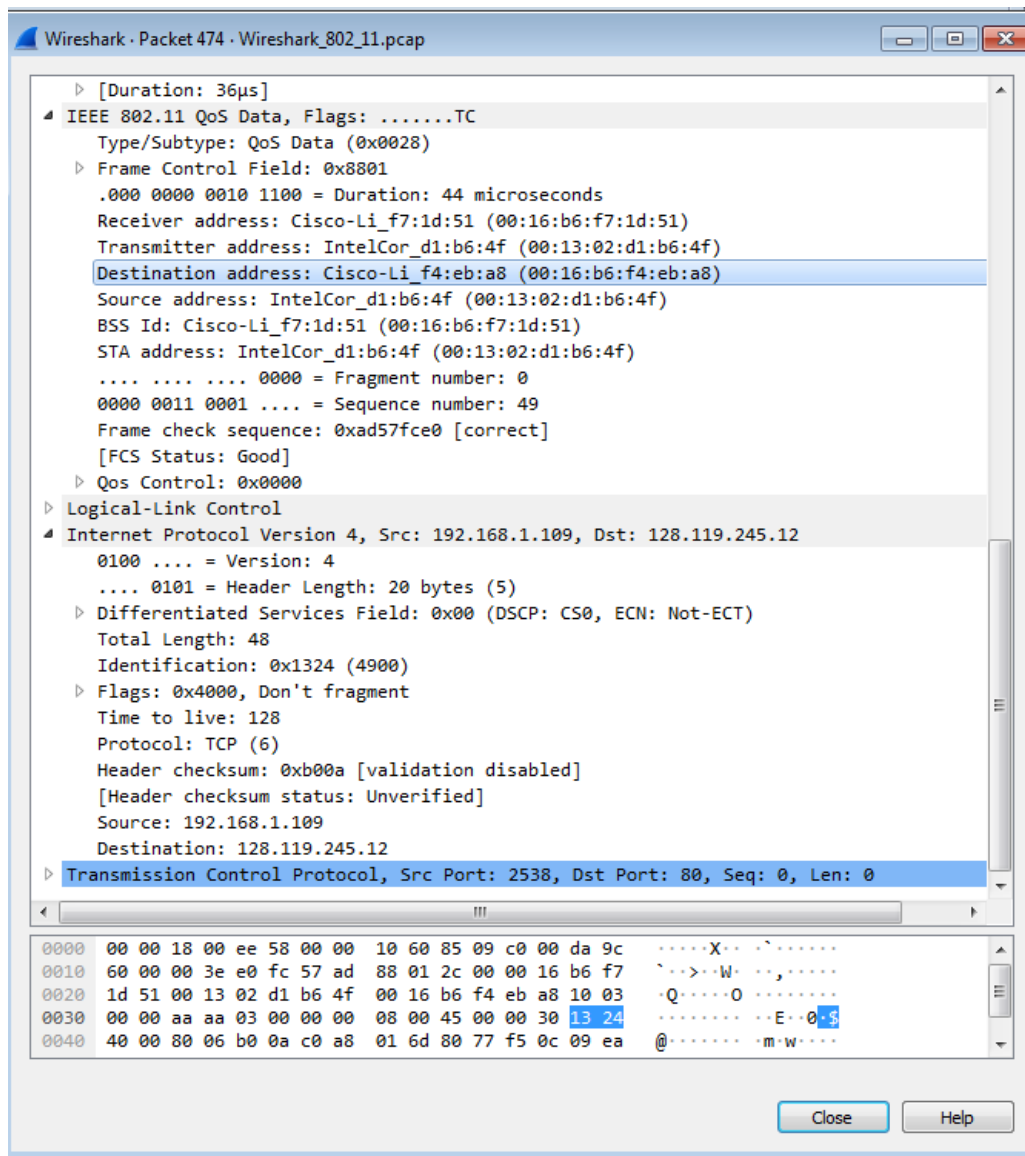
Mbps(Megabits per second) and transmission distance (in Metres). Some links such as the 802.11a,g, 802.11 b and the 802.15 use lower transmission rates from one to as much as fifty four Mbps. 802.11 wireless LANs are able to reduce their transmission rate to transmit data over longer distances. 802.11 wireless standards have different transmission distances depending on their rate of transmission. The rates advertised in the frame are as low as 1 and as high as 54Mbps which are not too high, so the transmission distance of the 802.11 wireless LAN used here can be increased.

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

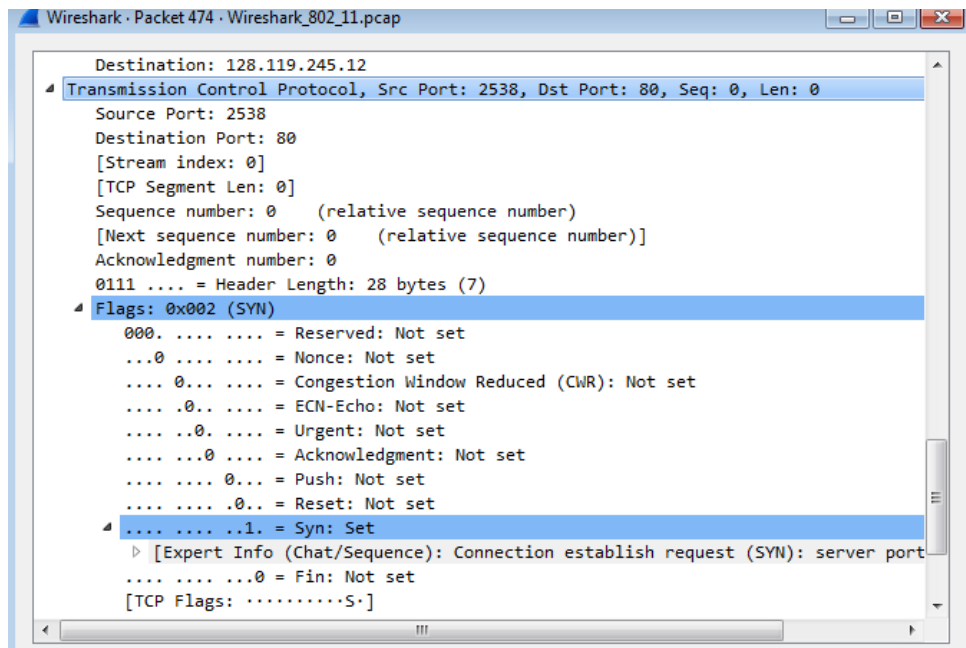


No.	Time	Source	Destination	Protocol	Length	Info
467	24.792793		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
468	24.795431	Cisco-Li_f7:1d:51	Cisco-Li_f4:eb:e8	802.11	90	Fragmented IEEE 802.11 frame
469	24.795573		Cisco-Li_f7:1d:51 (...)	802.11	38	Acknowledgement, Flags=.....C
470	24.795673	192.168.1.109	68.87.71.226	DNS	125	Standard query 0x7892 A gaia.cs.umass.edu
471	24.795769		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
472	24.809325	68.87.71.226	192.168.1.109	DNS	141	Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
473	24.809513		Cisco-Li_f7:1d:51 (...)	802.11	38	Acknowledgement, Flags=.....C
474	24.811093	192.168.1.109	128.119.245.12	TCP	110	2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475	24.811231		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110	80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	24.827922		Cisco-Li_f7:1d:51 (...)	802.11	38	Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1
481	24.828352		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
482	24.846898	128.119.245.12	192.168.1.109	TCP	108	80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483	24.847058		Cisco-Li_f7:1d:51 (...)	802.11	38	Acknowledgement, Flags=.....C
484	24.847171	128.119.245.12	192.168.1.109	TCP	108	[TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0

The frame that followed transport control protocol TCP rules when being transmitted, which has the SYN segment, starts from packet no.474 as shown in the screenshot above.



Three MAC address fields are destination, source and transmitter in the 802.11 frame shown above. The source MAC address (00:13:02:d1:b6:4f or 00 13 02 d1 b6 4f as base 16 hexadecimal) corresponds to the host sending the TCP segment. The transmitter address (00:13:02:d1:b6:4f) corresponds to the AP. The destination MAC address (00:16:b6:f4:eb:a8) corresponds to the first-hop router(which receives the frame containing its MAC address as the destination address from the host). The 32 bit IP address of the host, sending this TCP segment, is 192.168.1.109 and the 32 bit destination IP is 128.119.245.12. This destination IP corresponds to the server that holds the live copy of the gaiia.cs.umass.edu web page.



Frame Addressing

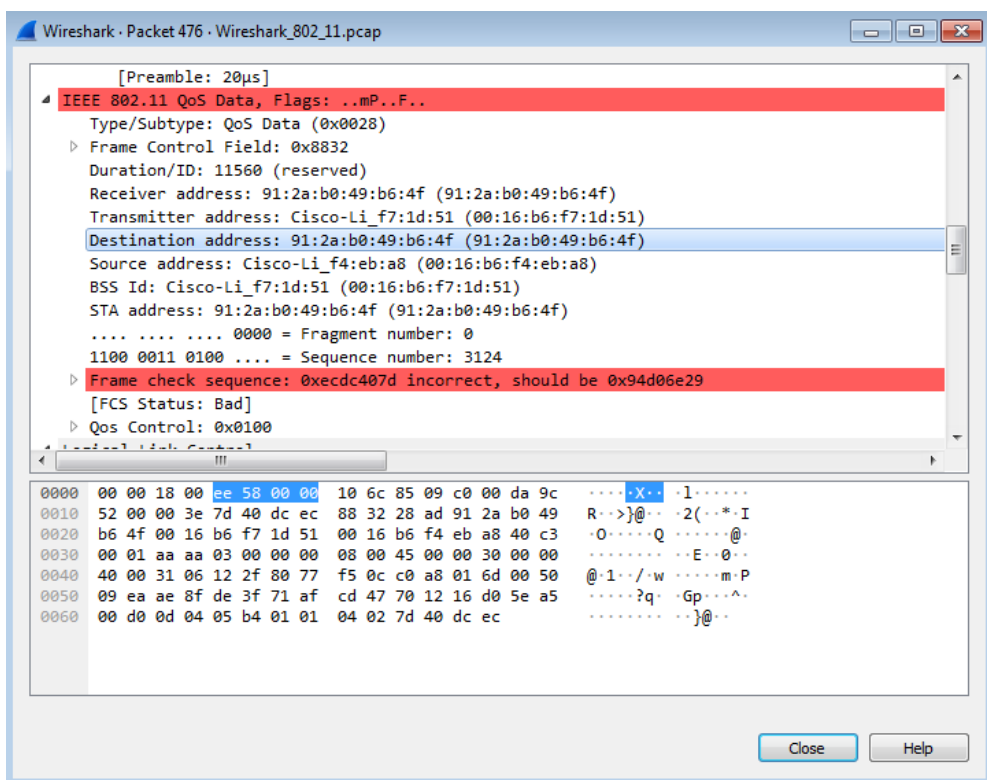
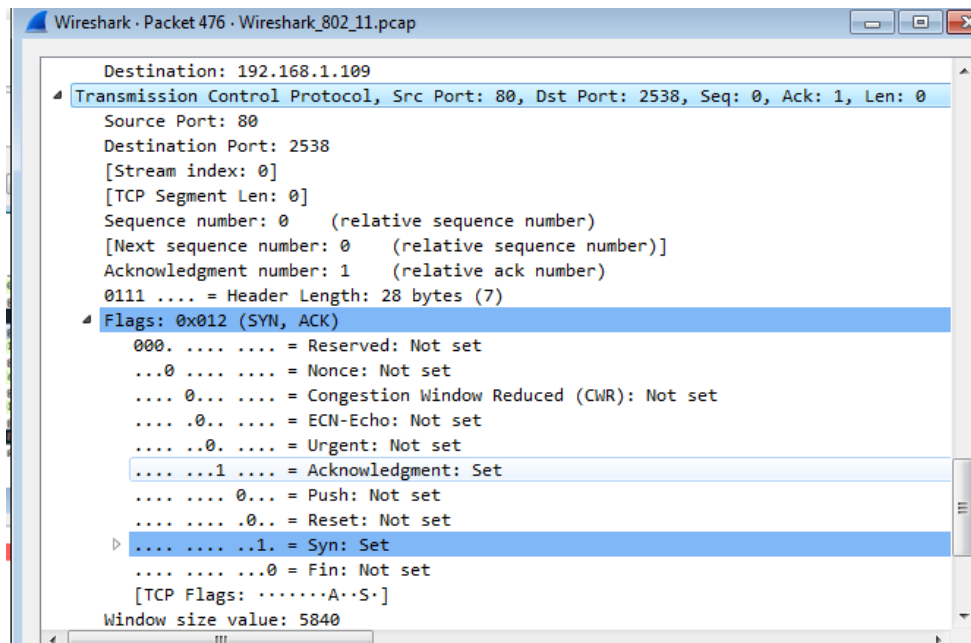
802.11 frames have fields to store addresses. The fields are address one, address two, address three and address four. The address one field stores the MAC address of the AP or host which transmits the frame, address two stores the MAC address of the host or AP to receive the frame and address three stores the destination MAC address of the router R3... Address four stores information about devices using an ad-hoc connection.

H1 creates a wireless 802.11 frame storing address one as MAC address of AP, two as its own MAC and three as the routers destination MAC, encapsulates datagram in the frame and sends it to the AP. When the AP receives the frame it turns the frame into an 802.3 ethernet frame to transmit through the ethernet cable to the first-hop router its next connection which is the router. This frame has the hosts MAC as the source address and the routers MAC as the destination address. When the AP gets the frame it turns the frame into an 802.11 frame and sends it along the wireless link

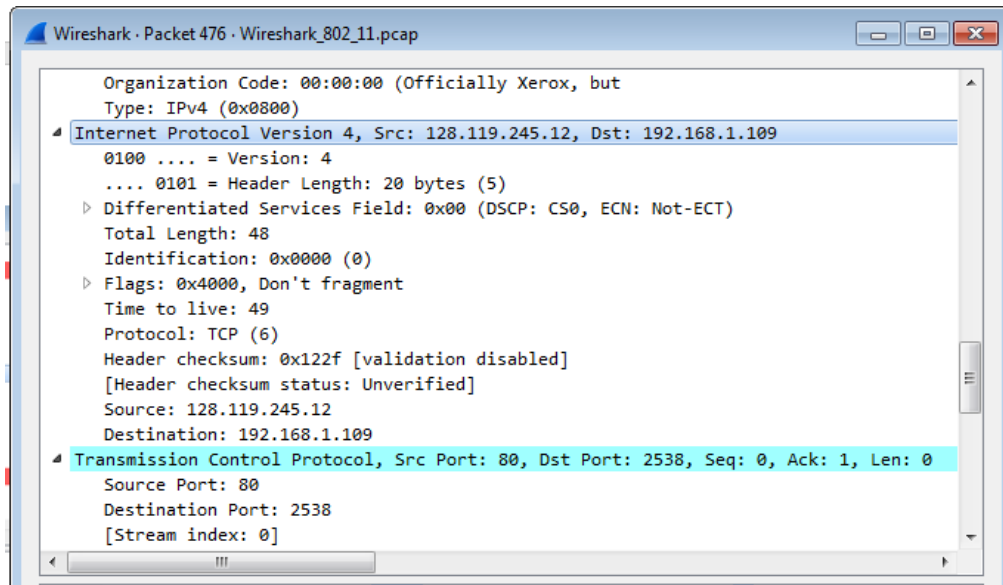
8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

474	24.811093	192.168.1.109	128.119.245.12	TCP	110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475	24.811231		IntelCor_d1:b6:4f (.. 802.11	38	Acknowledgement, Flags=.....C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	24.827922		Cisco-Li_f7:1d:51 (.. 802.11	38	Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (.. 802.11	38	Acknowledgement, Flags=.....C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537 GET /wireshark-labs/alice.txt HTTP/1.1
481	24.828352		IntelCor_d1:b6:4f (.. 802.11	38	Acknowledgement, Flags=.....C
482	24.846898	128.119.245.12	192.168.1.109	TCP	108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483	24.847058		Cisco-Li_f7:1d:51 (.. 802.11	38	Acknowledgement, Flags=.....C
484	24.847171	128.119.245.12	192.168.1.109	TCP	108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
485	24.847267		Cisco-Li_f7:1d:51 (.. 802.11	38	Acknowledgement, Flags=.....C

In the shot above, the frame containing the SYNACK segment for this TCP session is captured at t=24.827751 seconds.



The three MAC address fields are the source, transmitter and the destination. The source MAC address 00:16:b6:f4:eb:a8 is the address of the sender which corresponds to the first-hop router(whose MAC is the destination in the frame sent by the host). The MAC address of the destination is 91:2a:b0:49:b6:4f which corresponds to the host that sent the TCP SYN. (The destination address is different to the MAC address of the host in packet 474 if the host has two interfaces). The MAC address of the BSS id is 00:16:b6:f7:1d:51 which corresponds to the AP the server is connected to.



The IP address of the sender is of the server, holding the live copy of the gaia.cs.umass.edu web page, which is 128.119.245.12 and the destination IP is of the host the SYNACK is being sent to. The sender MAC address corresponds to the router not the IP address of the sender.

The packet in this TCP session is a SYNACK which is an Acknowledgements of the SYN packet that was sent. When a station gets the correct frame from another station it sends an acknowledgement (ACK for short) back to the station. In case the acknowledgement gets lost the station will send several copies of the frames. The sequence number (in the Transmission Control Protocol field of the frame above) allows the receiving station to tell a new frame has been transmitted and the frames which have been transmitted before that and the sequence no. field is used for this. The 802.11 protocol lets a sending station save a channel for an amount of time. This time, which includes the time the station takes to send its data frame plus the time taken to send an acknowledgement, is included in the frames duration field.

9. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

No.	Time	Source	Destination	Protocol	Length	Info
1727	49.429849	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1603, FN=0, Flags=.....TC
1728	49.430007	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (..)	802.11	38	Acknowledgement, Flags=.....C
1729	49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (..)	802.11	38	Acknowledgement, Flags=.....C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (..)	802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (..)	802.11	38	Acknowledgement, Flags=.....C

At t = 49.583615 a DHCP release frame is sent by the host, which is the IP-layer action, to the DHCP server to get released from the network it is connected to through the 30 Munroe St AP. At t = 49.609617 a deauthentication frame is sent by the host to disconnect from and end the association with the 30 Munroe St AP which is the 802.11-layer action. There are association request frames in the trace but not a disassociation frame.

DHCP – Dynamic Host Configuration Protocol

DHCP is the protocol that allows a device e.g. computer, laptop, smart phone to get an IP address from the DHCP server when it is connected to the internet. The DHCP server gives the IP address to the device only when it is and for as long as it is connected to the internet. The host no longer has an IP address which means it has left the network after it has sent the DHCP release.

10. Examine the trace file and look for AUTHENTICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49?

Wireshark_802.11.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1727	49.429849	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1603, FN=0, Flags=.....TC
1728	49.430007		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1729	49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770		IntelCor_d1:b6:4f (..	802.11	38	Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1743	49.641910		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1745	49.644710	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3589, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1747	49.646711		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1748	49.647827		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1752	49.662857		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1753	49.663950		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C

Starting at t = 49.638857 six AUTHENTICATION messages are sent from the wireless host to linksys_ses_24086 AP (MAC address Cisco-Li_f5:ba:bb).

Authentication

A host associates with an AP before connection to a larger network. This is by looking at channels, receiving beacon frames which have the AP's name (SSID) and MAC address and then accessing the AP's MAC address and password to connect to the network. Using the MAC address and password to join the larger network is known as authentication.

11. Does the host want the authentication to require a key or be open?

Wireshark_802_11.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1752	49.662857		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1753	49.663950		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1754	49.665704		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1755	49.669072		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1756	49.671321		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1757	49.673449		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1758	49.675828		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1759	49.676576		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1760	49.678737		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1761	49.685228		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1762	49.693106		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1763	49.746105	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1764	49.747831	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3590, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1765	49.749453	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1766	49.753595	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1767	49.849613	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3591, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1768	49.951978	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3592, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1769	50.054362	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3593, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1770	50.156729	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3594, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1771	50.259115	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3595, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1772	50.361455	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3596, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1773	50.463859	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3597, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1774	50.566342	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3598, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1775	50.668724	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3599, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1776	50.750964		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1777	50.752074		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1778	50.753072		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1779	50.754695	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1780	50.759321		Cisco-Li_f5:ba:bb (..	802.11	38	Acknowledgement, Flags=.....C
1781	50.771073	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3600, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1782	50.873457	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3601, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Looking at the trace there are several key messages after the association which does not mean the host wants the authentication to require a key.

12. I have looked through the trace from between $t = 49.638857$ and $t = 53$ and I do not see a reply authentication from the linksys_24086 AP. There is not a reply if the linksys_24086 AP want the host to authenticate with it with a key.

13. Now let's consider what happens as the host gives up trying to associate with the linksys_ses_24086 AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENTICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

Wireshark_802.11 (1).pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: wlan.fc.subtype == 11 and wlan.fc.type == 0

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=....R...C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=....R...C

I typed the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 in the filter field only the AUTHENTICATION frames for the host, at t = 63.168087 an authentication frame is sent from the host to the Access Point and at t = 63.169071 an authentication reply frame is sent from that Access Point.

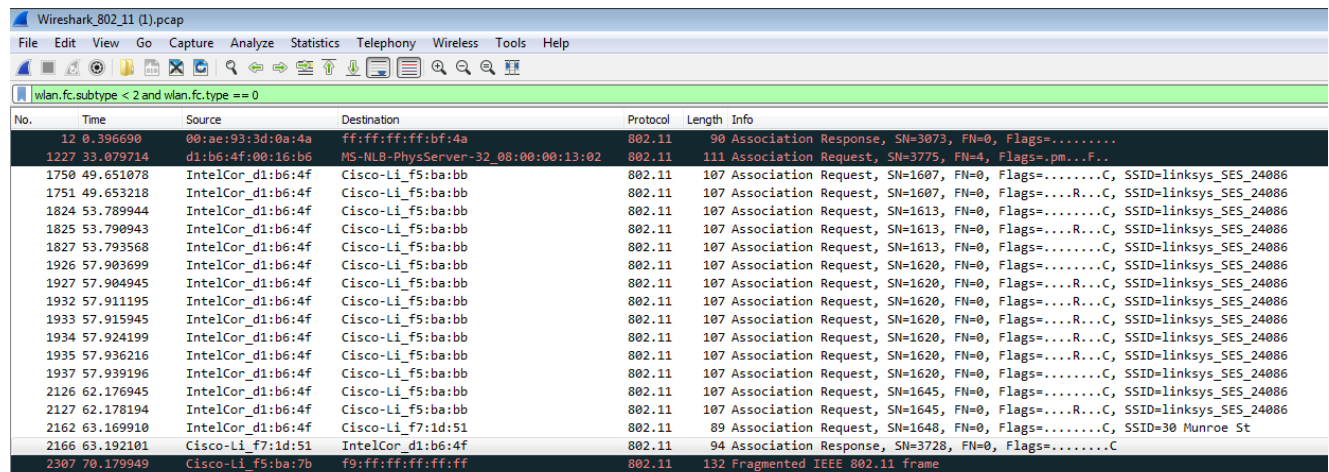
Wireshark_802.11 (1).pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: wlan.fc.subtype == 11 and wlan.fc.type == 0

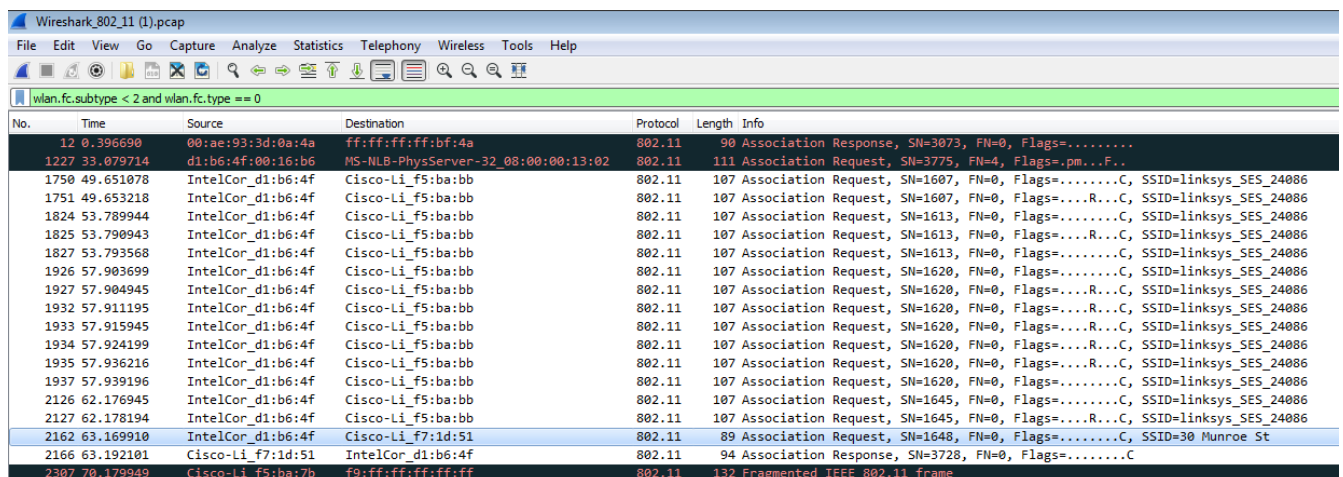
No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=....R...C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=....R...C

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression “wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.



No.	Time	Source	Destination	Protocol	Length	Info
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C, SSID=linksys_SES_24086
1227	33.079714	d1:b6:4f:00:16:b6	MS-NLB-PhysServer-32_08:00:00:13:02	802.11	111	Association Request, SN=3775, FN=4, Flags=.pm...F..
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1824	53.789944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1825	53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1827	53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1926	57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1927	57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1932	57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1933	57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
2126	62.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
2127	62.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

I use the expression “wlan.fc.subtype == 11 and wlan.fc.type == 0 to filter the display to only the association request and response frames between the host and the Aps in this trace.



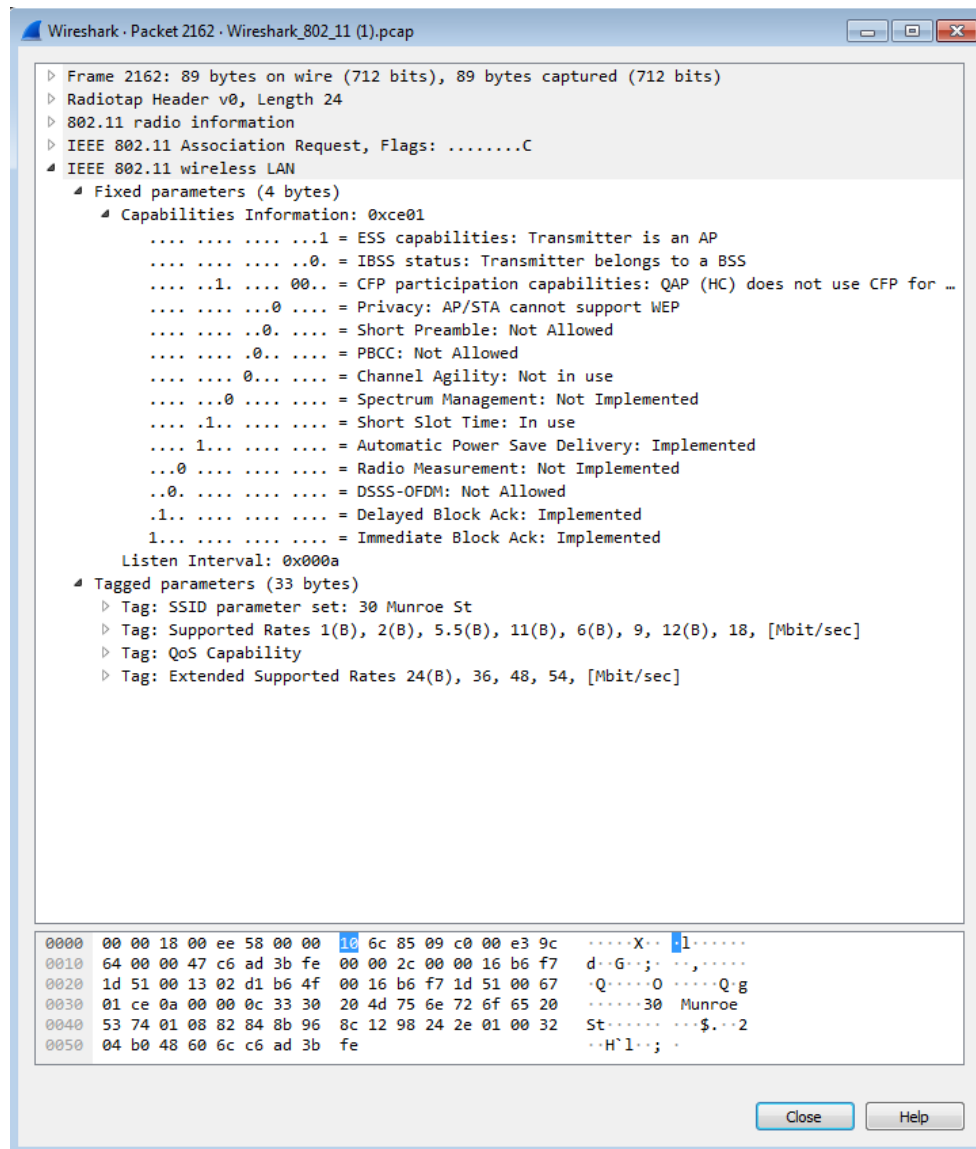
No.	Time	Source	Destination	Protocol	Length	Info
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C, SSID=linksys_SES_24086
1227	33.079714	d1:b6:4f:00:16:b6	MS-NLB-PhysServer-32_08:00:00:13:02	802.11	111	Association Request, SN=3775, FN=4, Flags=.pm...F..
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1824	53.789944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1825	53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1827	53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1926	57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1927	57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1932	57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1933	57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
2126	62.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
2127	62.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....R...C, SSID=linksys_SES_24086
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

Wireshark_802.11 (1).pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
wlan.fc.subtype < 2 and wlan.fc.type == 0						
No.	Time	Source	Destination	Protocol	Length	Info
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....
1227	33.079714	d1:b6:4f:00:16:b6	MS-NLB-PhysServer-32_08:00:00:13:02	802.11	111	Association Request, SN=3775, FN=4, Flags=..pm...F..
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1824	53.789944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1825	53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1827	53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1926	57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1927	57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1932	57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1933	57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
2126	62.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
2127	62.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=....R...C, SSID=linksys_SES_24086
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

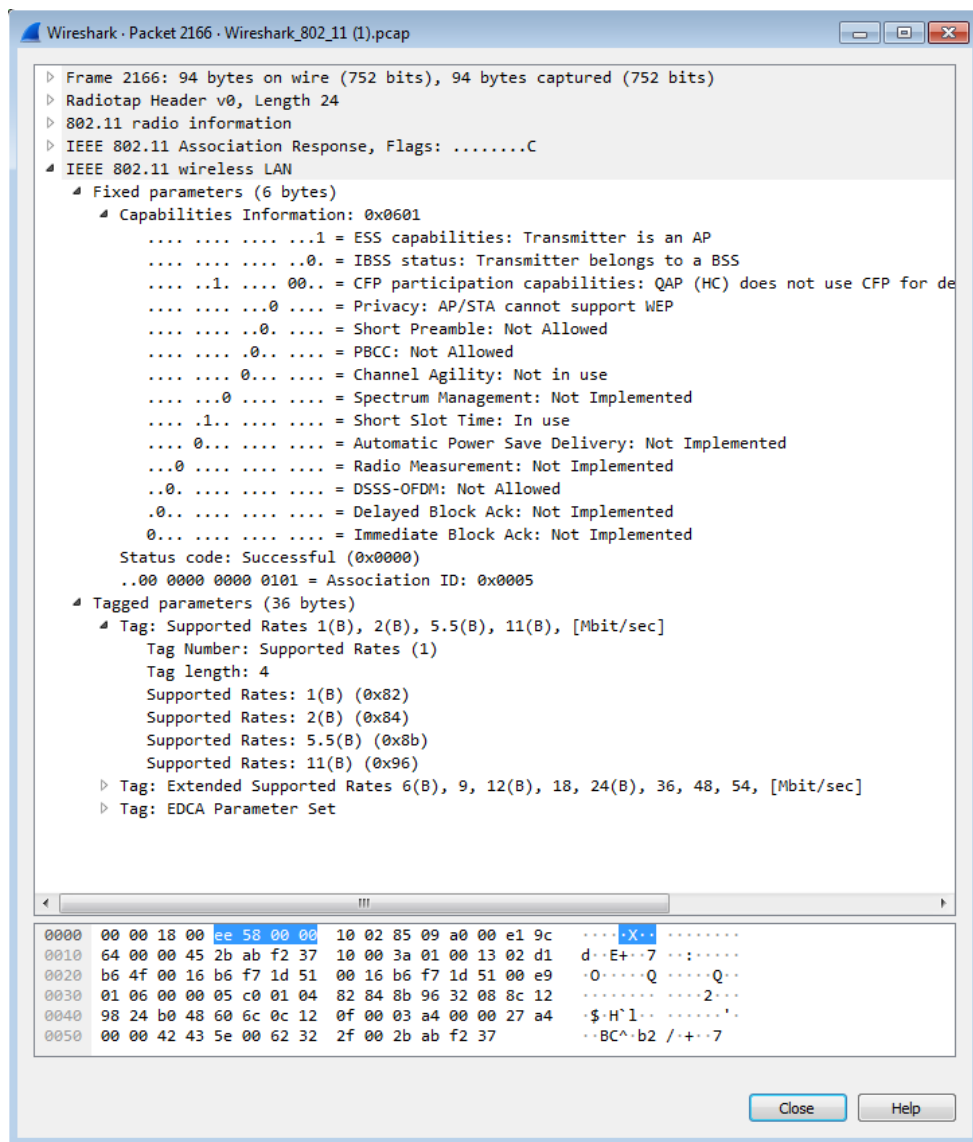
At t = 63.169910 an association request frame is sent from the host (00:13:02:d1:b6:4f) to the 30 Munroe St access point(BSS 00:16:b6:f7:1d:51). At t = 63.192101 an association response frame is then sent back to the host from the access point.

...

15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.



Looking into the field of parameters that are tagged the transmission rates the host is willing to use are in Megabits/second(Mbps) which are 1,2,5.5,11,6,9,12 and 18 Mbps and the additional supported rates are 24,36,48 and 54 Mbps.

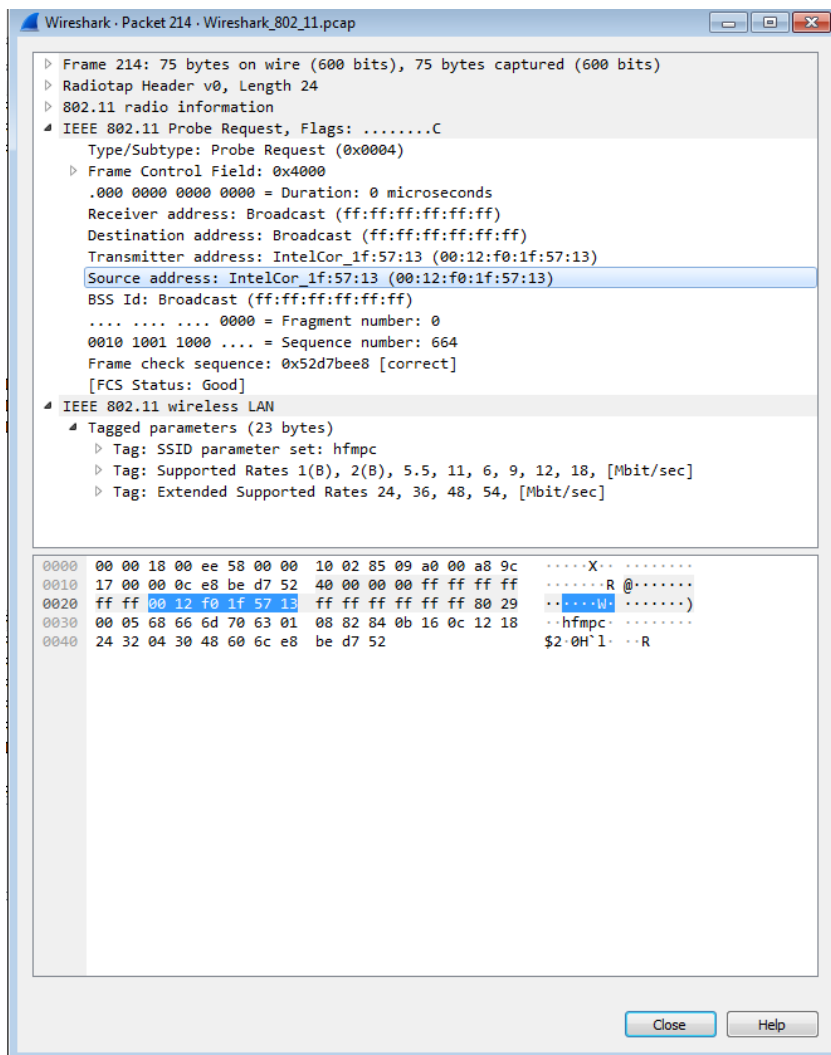


The transmission rates the access point is willing to use are 1,2,5.5,11 which are the supported rates in Megabits/second (Mbps) and the additional supported rates 6,9,18,24,36,48 and 54 Mbps. These rates are the same as the rates the host is trying to use.

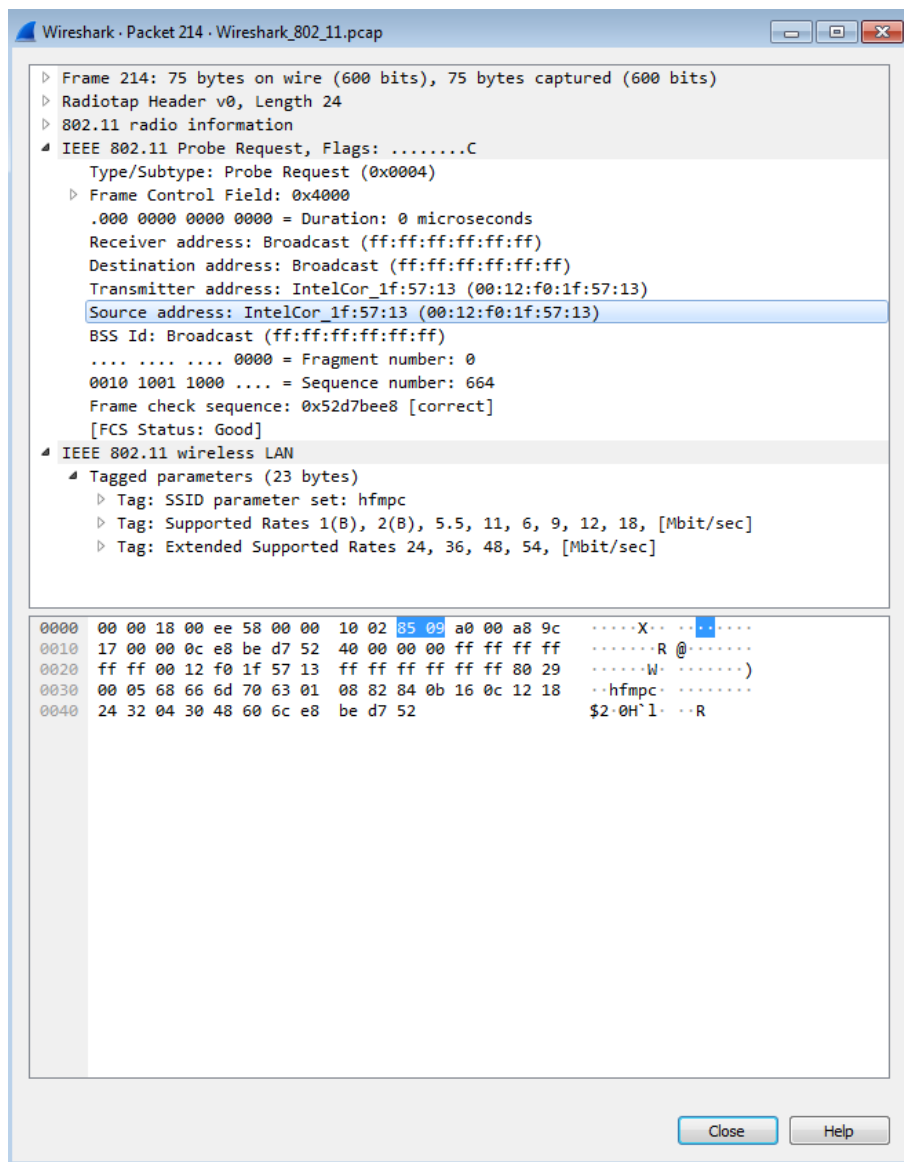
As already mentioned in question 6, wireless links with higher transmission rates and shorter transmission distances may change their distances of transmission by changing their rates. The Aps transmission rates in the frame are low enough for it to increase its transmission distance.

3. Other types of frame

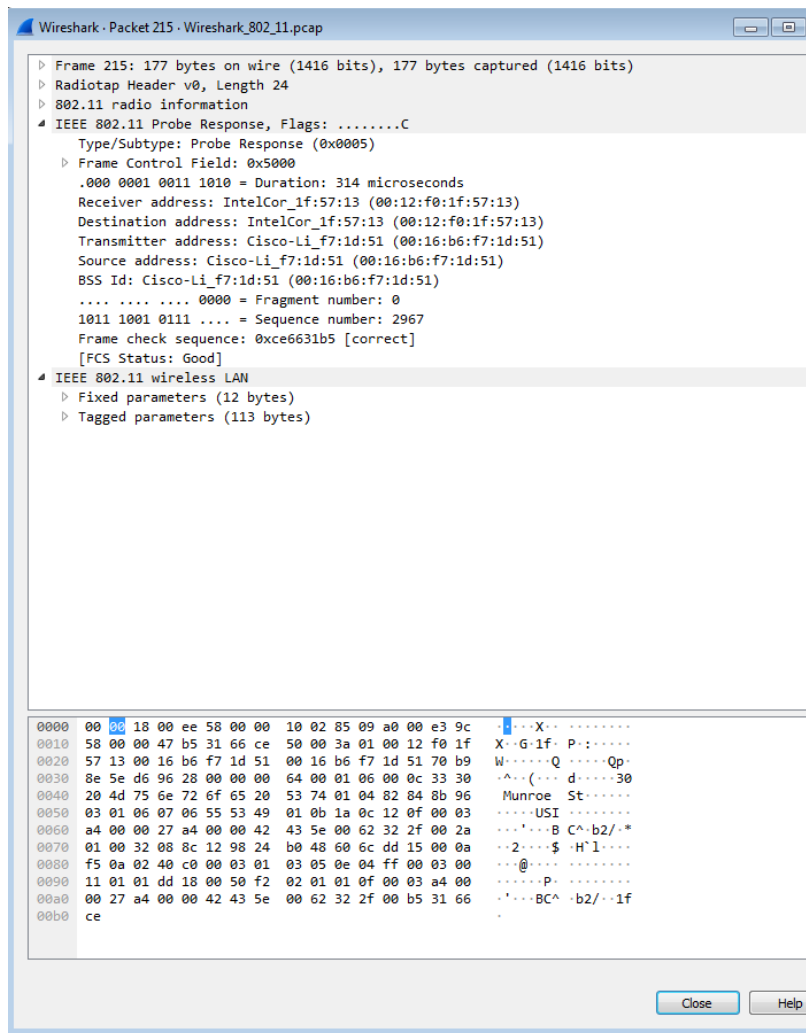
16. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).



Wireshark_802.11.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
187	8.457937	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
188	8.459435	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
189	8.461061	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
190	8.462561	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
191	8.464186	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
192	8.465688	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
193	8.481809	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
194	8.584261	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
195	8.686658	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
196	8.789061	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
197	8.891471	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
198	8.993880	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
199	9.096256	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
200	9.198659	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
201	9.301011	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
202	9.403429	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
203	9.403571		IntelCor_d1:b6:4f (...)	802.11	38	Acknowle
204	9.404443	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null
205	9.404543		IntelCor_d1:b6:4f (...)	802.11	38	Acknowle
206	9.505800	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
207	9.608247	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
208	9.710568	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
209	9.813054	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
210	9.915460	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
211	10.017848	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
212	10.120174	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
213	10.222587	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon f
214	10.300585	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Re
215	10.303565	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
216	10.305063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
217	10.306563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
218	10.308063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re
219	10.309572	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Re



At $t = 10.300585$ a probe request frame, as shown above, is broadcast from the host to the AP. The sender MAC address in this frame is 00:12:f0:1f:57:13, receiver MAC address is ff:ff:ff:ff:ff:ff and the BSS id MAC address is ff:ff:ff:ff:ff:ff. As mentioned in question 4 the receiver and BSS Id MAC addresses are ff:ff:ff:ff:ff:ff and broadcasts since this is a probe request frame being broadcast by the host to the AP and so therefore the frame has the MAC address of the host. The host does not have the receiver and BSS ID MAC addresses of the AP yet when broadcasting this probe request.



At $t = 10.30565$ a probe response frame, as shown above, is sent from the AP to the host. It has receiver MAC address 00:12:f0:1f:57:13 (which is the host), source and BSS Id MAC address 00:16:b6:f7:1d:51. Since this is a response by the AP to the probe request, the MAC addresses of the AP are in this response frame that were ff:ff:ff:ff:ff:ff in the request frame.

Other types of frame - Probe Frames

There are two kinds of association with APs which are Active scanning and Passive scanning. The purpose of these frames is to show the host associate with the AP, to connect to the internet, using the active scanning association. This is where probe request frames are broadcast from the host to the access points which are within the range and then the APs send probe response frames to the host before the association request and response frames are sent and received between the hosts chosen AP.

The passive scanning association is just the beacon frames being sent from the AP and received by the host followed by association request and response frames being sent and received between the two.

Conclusion

We have connections to the network which work with wires and without wires(wireless). The wired network connections (such as RJ45 Ethernet) are still popular and in use and working with wireless connections which are data being transmitted through the air, instead of wires, between antennas on receiving and transmitting stations. Nodes such as hosts and routers are connected to the larger network such as the internet using wireless 802.11 transmission and wires.

The packet sniffing tool is handy when trying to capture data frames used during a wireless network connection as well as a wired connection.

...the packet sniffer is useful to show how well a wireless connection is...

There are different types of 802.11 wireless LANs that are used. Some of these have data rates between 54 and 1300 Mbps and transmit data between a distance of ten to thirty metres which is the indoor range for example the 802.11ac, 802.11n and 802.11 a,g wireless LANs. The internet settings on our computer list the protocol followed by our network connection as 802.11n. 802.11n is the wireless LAN we are using. It's transmission distance is the indoor range but with a higher data rate and it is used in our home.

MAC addresses are ff:ff:ff:ff:ff:ff when the sender does not have or know the actual address while sending.

During active scanning, association request and response frames are sent and received by the host and AP after sending and receiving probe frames because the AP does not know which APs the host is going to choose to associate with. The host will want to join the subnet the AP is in when associated with the AP.