Wireless Network.
EP2950
12/01/2015

Wireless Network analysers

Report :
Pierre FLEITZ
Blanca Martinez
Masahiro Wakasa

Preparation questions :

a) We can have 4 addresses in the MAC frame, one address for the source, one for de destination, one for the transmitter and one for the receiver.
b) We can find the flag ToDS and From DS both equal to 0 in an Ad-hoc network.
c) By sending a probe request message (Active scanning) or by listening for Beacon messages (Passive scanning).

1. Beacon frames :

1. The SSIDs of the two access points that are issuing most of the beacon frames in this trace are '30 Munroe St' and 'inksys_SES_24086'.
2. The intervals of time between the transmissions of the beacon frames lynksis_ses_24086 acces point are 0.1024 seconds, and same from the 30 Munroe St. Access point.
3. The source MAC Address on the beacon frame from 30 Munroe St. is 00 :16 :b6 :f7 :1d :51.
4. The destination MAC address on the beacon frame from 30 Munroe St. is broadcast so ff :ff :ff :ff :ff :ff.
5. The MAC BSS id on the beacon frame from 30 Munroe St. is 00 :16 :b6 :f7 :1d :51.
6. These rates are :
   Supported rates : Rates 1(B) , 2(B), 5.5(B), 11 Mbps.
   Extended support rates : Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54 Mbps.

2. Data Transfer :

7. The three MAC addresses are :
   - the receiver address : 00 :16 :b6 :f7 :1d :51
   - the source/transmitter address : 00 :13 :02 :d1 :b6 :4f
   - the destination address : 00 :16 :b6 :f4 :eb :a8
   The MAC address corresponding to the wireless host is the source MAC Address (00 :13 :02 :d1 :b6 :4f), to the Access point is the receiver MAC

Addres (corresponding to the BSS Id) (00 :16 :b6 :f7 :1d :51) , to the first hop is the destination address (00 :16 :b6 :f4 :eb :a8).
The IP Address of the wireless host sending this TCP segment is 192.168.1.109.
The destination IP Address is 128.119.245.12.
This IP address correspond to some other network-attached device a server, the server gaia.cs.umass.edu.

8. The three MAC addresses are :
   - the destination/receiver address : 91 :2a ::b0 :49 :b6 :4f but it's an error the correct MAC address should be 00 :13 :02 :d1 :b6 :4f.
   - the transmitter address : 00 :16 :b6 :f7 :1d :51
   - the source address : 00 :16 :b6 :f4 :eb :a8
   The MAC address corresponding to the host is the destination MAC Address (91 :2a ::b0 :49 :b6 but should be 00 :13 :02 :d1 :b6 :4f), to the Access point is transmitter MAC Addres (00 :16 :b6 :f7 :1d :51), to the first hop is the source address (00 :16 :b6 :f4 :eb :a8).
   The IP Address of the host sending this TCP segment is 128.119.245.12.
   The destination IP Address is 192.119.245.12.
   No it's not, we can see here that the MAC address correspondong to the IP address 192.119.245.12 is 91 :2a ::b0 :49 :b6 :4f but it should be 00 :13 :02 :d1 :b6 :4f and we can see that there is an error in the checksum so we can conclude that an error occured.

3. Association/Disassociation :

9. We can see that at t = 49.583615 there is a DHCP release sent by the host to the DHCP server. And later at t = 49.609617 there is a Deauthentication frame. We were expecting to see a Disassociation frame and not a Deauthentication frame !
10. In order to find them we used the filter: wlan.fc.type_subtype eq 11. We counted 15 AUTHENTICATION messages sent from the wireless host to the linksys_ses__24086 AP.
11. We can see in the frame taht we have Authentication Algorithm as Open System, therefore we know that the host is requesting the association to be open.
12. No we can't see any reply from the linksys_ses_24086 AP.
13. At t = 63.168087 there is an AUTHENTICATION frame sent from the host to the 30 Munroe St. AP, and at t = 63.169707 there is a reply AUTHENTICATION sent from the AP to the host.
14. In order to find the ASSOCIATE REQUEST we used the filter :
    wlan.fc.type.subtype eq 0.
    At t = 63.169910 there is an ASSOCIATE REQUEST from host to the 30 Munroe St. AP.
    In order to find the ASSOCIATE REPLY we used the filter :
    wlan.fc.type.subtype eq 1.
    At t = 63.192101 there is the corresponding ASSOCIATE REPLY sent.

15. We can see in the ASSOCIATE REQUEST the host advertise that the supported rates are 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54 Mbps. And in the ASSOCIATE RESPONSES the AP advertise the same supported rates !

4. Other Frame types :

16. In order to find the PROBE REQUEST frames we used the filter : wlan.fc.type_subtype eq 4.
The sender (source) MAC Address in these frames is : 00 :12 :f0 :1f :57 :13
The receiver MAC Address in these frames is : ff :ff :ff :ff :ff :ff
The BSS ID MAC Address in these frame is : ff :ff :ff :ff :ff :ff
We use PROBE REQUEST during an active scanning in order to find an Access Point.

In order to find the PROBE REQUEST frames we used the filter : wlan.fc.type_subtype eq 5.
The sender (source) MAC Address in these frames is : 00 :16 :b6 :f7 :1d:51
The receiver MAC Address in these frames is : 00 :12 :f0 :1f :57 :13
The BSS ID MAC Address in these frame is : 00 :16 :b6 :f7 :1d :51
The PROBE RESPONSE is a frame sent by the Access Point to the host that sent the request.