

Wireshark Lab 7 – 802.11

IT 520 –A – Enterprise Infrastructure & Networks

David Gogolkiewicz

Recycle Bin Nokia Suite graduation videos '12 SMS Open Authorization Form Signe... untitled Test Newsletter... icon_loading... Writings HomePage

Acrobat Reader DC Skype Amazon Music ... World of Tanks Corel Paint Shop Pro... Correct Lights.jpg FontMana... 2015_02_12 2015_03_05 Fraps Blacklight Retribution... ryker Wireshark Test newsletter... Rocket Mania DriverToolkit Microsoft Edge Norton Installati... Adobe Applicati... Canon MG5300 ... Deer #3.pptx Sales Navigator... HP USB Disk Storage Fo... C281_Game... science project p... desktop.ini Science Fair Packet 20... Laplink PCmov... Dropbox Smartparts Pictures crossbow-... hu2011_set... Lenovo Soluti... Expenses desktop.ini

Command Prompt

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . : fios-router.home
Link-local IPv6 Address . . . . . : fe80::7dd2:65fe:cb63:5d58%4
IPv4 Address. . . . . : 192.168.1.195
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Ethernet adapter Npcap Loopback Adapter:

```
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::496e:f51d:a938:4bac%23
Autoconfiguration IPv4 Address. . : 169.254.75.172
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

Wireless LAN adapter Local Area Connection* 5:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Wireless LAN adapter Local Area Connection* 6:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Wireless LAN adapter Wi-Fi:

My Private IP address:
192.168.1.195

Question 1

Lab 7 Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Expression ... +

No.	Time	Source	Destination	Protocol	Length	Info
445	23.738803	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3110, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
446	23.738949	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1528, FN=0, Flags=.....TC
447	23.739049	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
448	23.739819	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1529, FN=0, Flags=...P...TC
449	23.739917	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
450	23.841201	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3111, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
451	23.943616	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3112, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
452	24.046004	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3113, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
453	24.148410	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3114, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
454	24.250778	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3115, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
455	24.353107	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3116, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
456	24.455592	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3117, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
457	24.557908	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3118, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
458	24.660319	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3119, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
459	24.763182	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3120, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
460	24.763316	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
461	24.763474	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3121, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

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)
.... = Fragment number: 0
1100 0010 1011 = Sequence number: 3115
Frame check sequence: 0x65a230b1 [unverified]
[FCS Status: Unverified]

IEEE 802.11 wireless LAN

- Fixed parameters (12 bytes)
 - Timestamp: 174343270786
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x0601
- Tagged parameters (119 bytes)
 - Tag: SSID parameter set: 30 Munroe St
 - Tag Number: SSID parameter set (0)
 - Tag length: 12
 - SSID: 30 Munroe St
 - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 - Tag Number: Supported Rates (1)
 - Tag length: 4
 - Supported Rates: 1(B), (0x02)

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e1 9cX.....
0010 58 00 00 45 b1 30 a2 65 80 00 00 ff ff ff ffE..e.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 b0 c2Q.....
0030 82 31 ab 97 28 00 00 00 64 00 01 06 00 0c 33 301...d...30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96Munroe 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 5eBC^.....
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48b2/*..2...\$-H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05l.....@.....
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 62BC^..b
00b0 32 2f 00 b1 30 a2 652/*..e

Indicates the identity of an ESS or IBSS (wlan.ssid), 12 bytes

Packets: 2364 · Displayed: 2364 (100.0%) Profile: Default

Type here to search

Address Links 12:07 PM 4/7/2019

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

-30 Munroe ST.
-Linksys_SES_24086

Question 1

Lab 7 Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Expression ... +

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
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	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713	Cisco-Li_f5:ba:bb	IntelCor_d1:b6:4f	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	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C

Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... = Fragment number: 0
0110 0100 0110 = Sequence number: 1606
Frame check sequence: 0xa07a577e [unverified]
[FCS Status: Unverified]

IEEE 802.11 wireless LAN

Tagged parameters (47 bytes)

- Tag: SSID parameter set: linksys_SES_24086
 - Tag Number: SSID parameter set (0)
 - Tag length: 17
 - SSID: linksys_SES_24086
- Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
 - Tag Number: Supported Rates (1)
 - Tag length: 8
 - Supported Rates: 1 (0x02)
 - Supported Rates: 2 (0x04)
 - Supported Rates: 5.5 (0x0b)
 - Supported Rates: 11 (0x16)
 - Supported Rates: 6 (0x0c)
 - Supported Rates: 9 (0x12)
 - Supported Rates: 12 (0x18)
 - Supported Rates: 18 (0x24)

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e6 9cX.....
0010 58 00 00 4a 7e 57 7a a0 40 00 00 00 ff ff ff ff X..J~Wz..@.....
0020 ff ff 00 13 02 d1 b6 4f ff ff ff ff ff ff ff ff 00 64O.....^d
0030 00 11 6c 69 6e 6b 73 79 73 5f 53 45 53 5f 32 34 ..linksys SES 24
0040 30 38 36 01 08 02 04 0b 16 0c 12 18 24 0a 01 07 086.....\$...
0050 32 04 30 48 60 6c dd 07 00 03 47 01 02 01 01 7e 2~H~l...~G.....
0060 57 7a a0 Wz~

Indicates the identity of an ESS or IBSS (wlan.ssid), 17 bytes

Packets: 2364 • Displayed: 2364 (100.0%) Profile: Default

Type here to search

Address Links 12:46 PM 4/7/2019

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

-30 Munroe ST.
-linksys_SES_24086

Lab 7 Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Question 2

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, 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
22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, 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=linksys12
24	1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
25	1.211992	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
26	1.212089	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
28	1.212282	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
29	1.212941	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1485, FN=0, Flags=...P...TC
30	1.213040	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
32	1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
33	1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2869, 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
35	1.519000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2870, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

0... .. = Protected flag: Data is not protected
0... .. = Order flag: Not strictly ordered
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: LinksysG_67:22:94 (00:06:25:67:22:94)
Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
.... .. = Fragment number: 0
1100 0000 1001 = Sequence number: 3081
Frame check sequence: 0xb6ef97a7 [unverified]
[FCS Status: Unverified]

IEEE 802.11 wireless LAN

- Fixed parameters (12 bytes)
 - Timestamp: 9534922650285
 - Beacon Interval: 0.102400 [Seconds]
 - Capabilities Information: 0x0011
- Tagged parameters (26 bytes)
 - Tag: SSID parameter set: linksys12
 - Tag Number: SSID parameter set (0)
 - Tag length: 9
 - SSID: linksys12
 - Tag: Supported Rates 1(R) 2(R) 5 11 [Mbit/sec]

0000 00 00 18 00 ee 58 00 00 10 04 85 09 a0 00 a3 9cX.....
0010 64 00 00 07 a7 97 ef b6 80 00 00 00 ff ff ff ffd.....
0020 ff ff 00 06 25 67 22 94 00 06 25 67 22 94 90 c0%g.....%g.....
0030 ad 72 ad 05 ac 08 00 00 64 00 11 00 00 09 6c 69d.....ll
0040 6e 6b 73 79 73 31 32 01 04 82 84 0b 16 03 01 06nksys12.....
0050 05 04 01 03 00 00 a7 97 ef b6

Beacon Interval (wlan.fixed.beacon), 2 bytes

Packets: 2364 · Displayed: 2364 (100.0%) Profile: Default

Type here to search

Address Links 12:16 PM 4/7/2019

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).

-0.102400 Seconds for 802.11 Wireless LAN Management Frame. Beacon frames for linksys-SES-2406 do not show up.

Lab 7 Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Question 3

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, 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
22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, 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=linksys12
24	1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
25	1.211992	IntelCor_d1:b6:4f	Broadcast	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
26	1.212089	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
28	1.212282	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
29	1.212941	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1485, FN=0, Flags=...P...TC
30	1.213040	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
32	1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
33	1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2869, 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
35	1.519000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2870, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Flags: 0x00

-00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
-0.. = More Fragments: This is the last fragment
-0... = Retry: Frame is not being retransmitted
- ...0.... = PWR MGT: STA will stay up
- ..0.... = More Data: No data buffered
- .0.... = Protected flag: Data is not protected
- 0... = Order flag: Not strictly ordered

..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 0100 = Sequence number: 2868

Frame check sequence: 0x080b1310 [unverified]

[FCS Status: Unverified]

IEEE 802.11 wireless LAN

Fixed parameters (12 bytes)

Timestamp: 17432033186

Beacon Interval: 0.102400 [Seconds]

Capabilities Information: 0x0601

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e4 9c d...X... ..

0010 64 00 00 48 10 13 0b 88 80 00 00 00 ff ff ff ff d...H... ..

0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 40 b3 ..00:16:b6:f7:1d:51:00:16:b6:f7:1d:51:40:b3: ..

0030 82 31 4d 96 28 00 00 00 64 00 01 06 00 0c 33 30 -1M-(-...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 01P.....

00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62BC^b

00b0 32 2f 00 10 13 0b 88 2/.....

Source Hardware Address (wlan.sa), 6 bytes

Packets: 2364 · Displayed: 2364 (100.0%)

Profile: Default

Type here to search

Address Links

12:20 PM 4/7/2019

What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St?
- (00:16:b6:f7:1d:51)

Question 4

Lab 7 Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression ... +

No.	Time	Source	Destination	Protocol	Length	Info
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, 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
22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, 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=linksys12
24	1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
25	1.211992	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
26	1.212089	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
28	1.212282	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
29	1.212941	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1485, FN=0, Flags=...P...TC
30	1.213040	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
32	1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
33	1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2869, 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
35	1.519000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2870, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Flags: 0x00
....0000 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
....0... = More Fragments: This is the last fragment
....0... = Retry: Frame is not being retransmitted
...0.... = PWR MGT: STA will stay up
..0.... = More Data: No data buffered
..0... = Protected flag: Data is not protected
0... = Order flag: Not strictly ordered
..0000 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 0100 = Sequence number: 2868
Frame check sequence: 0x080b1310 [unverified]
[FCS Status: Unverified]

IEEE 802.11 wireless LAN
Fixed parameters (12 bytes)
Timestamp: 17432033186
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0601

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e4 9c d...X...
0010 64 00 00 48 10 13 0b 88 80 00 00 00 ff ff ff ff d...H...
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 40 b3 ff...Q...
0030 82 31 4d 96 28 00 00 00 64 00 01 06 00 0c 33 30 1M...d...
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 10 13 0b 88 2/.....

Destination Hardware Address (wlan.da), 6 bytes

Packets: 2364 · Displayed: 2364 (100.0%) Profile: Default

Type here to search

Address Links 12:23 PM 4/7/2019

What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??
-(ff:ff:ff:ff:ff:ff)

Question 5

Lab 7 Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression ... +

No.	Time	Source	Destination	Protocol	Length	Info
19	0.904619	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
20	1.007015	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, 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
22	1.109406	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, 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=linksys12
24	1.211843	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
25	1.211992	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
26	1.212089	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
28	1.212282	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
29	1.212941	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1485, FN=0, Flags=...P...TC
30	1.213040	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
31	1.215947	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3081, FN=0, Flags=.....C, BI=100, SSID=linksys12
32	1.314223	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2868, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
33	1.416593	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2869, 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=100, SSID=linksys12
35	1.519000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2870, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Flags: 0x00
.... 00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.... 00 = More Fragments: This is the last fragment
.... 00 = Retry: Frame is not being retransmitted
.... 00 = PWR MGT: STA will stay up
.... 00 = More Data: No data buffered
.... 00 = Protected flag: Data is not protected
.... 00 = Order flag: Not strictly ordered
0000 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 0100 = Sequence number: 2868
Frame check sequence: 0x080b1310 [unverified]
[FCS Status: Unverified]

IEEE 802.11 wireless LAN
Fixed parameters (12 bytes)
Timestamp: 17432033186
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0601

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e4 9cX.....
0010 64 00 00 48 10 13 0b 88 80 00 00 00 ff ff ff ff d...H.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 40 b3Q.....@..
0030 82 31 4d 96 28 00 00 00 64 00 01 06 00 0c 33 30 -IM-(-...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 5eBC^.....
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 62BC^..b
00b0 32 2f 00 10 13 0b 88 2/.....

Basic Service Set ID (wlan.bssid), 6 bytes

Packets: 2364 · Displayed: 2364 (100.0%) Profile: Default

Type here to search

Address Links 12:26 PM 4/7/2019

What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?
- (00:16:b6:f7:1d:51)

C:\Users\dgogo\OneDrive\Masters\Computer Networking Course\Lab 7\Lab 7 Wireshark.pcap 2364 total packets, 24 shown

```
No.      Time      Source                Destination            Protocol Length Info
1309 33.146120 128.119.240.19        192.168.1.109          HTTP      393      HTTP/1.1 200 OK (GIF89a)
Frame 1309: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 QoS Data, Flags: .....F.C
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8802
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x02
.... ..10 = DS status: Frame from DS to a STA via AP (To DS: 0 From DS: 1) (0x2)
.... ..0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
..0. .... = Protected flag: Data is not protected
0... .... = Order flag: Not strictly ordered
...000 0000 0010 1000 = Duration: 40 microseconds
Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
.... .... 0000 = Fragment number: 0
1101 0100 0110 .... = Sequence number: 3398
Frame check sequence: 0xe556daa6 [unverified]
[FCS Status: Unverified]
QoS Control: 0x0100
Logical-Link Control
DSAP: SNAP (0xaa)
SSAP: SNAP (0xaa)
Control field: U, func=UI (0x03)
Organization Code: 00:00:00 (Officially Xerox, but
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.240.19, Dst: 192.168.1.109
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 331
Identification: 0xa9bd (43453)
Flags: 0x4000, Don't fragment
Time to live: 49
Protocol: TCP (6)
Header checksum: 0x6c4f [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.240.19
Destination: 192.168.1.109
Transmission Control Protocol, Src Port: 80, Dst Port: 2548, Seq: 1, Ack: 388, Len: 291
Source Port: 80
Destination Port: 2548
[Stream index: 9]
[TCP Segment Len: 291]
Sequence number: 1 (relative sequence number)
[Next sequence number: 292 (relative sequence number)]
Acknowledgment number: 388 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 6432
[Calculated window size: 6432]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x6a25 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
```