Wireshark Lab - 802.11

Jussara Patrícia Rodrigues da Silva

1. Quais são os SSIDs dos dois pontos de acesso que estão emitindo a maioria dos quadros de sinalização neste rastreamento?
Os dois pontos de acesso que estão emitindo a maioria dos quadros de beacon têm um SSID de “30 Munroe St” e de “linksys12”.

2. Quais são os intervalos de tempo entre a transmissão dos quadros de baliza e o ponto de acesso linksys_ses_24086? Do ponto de acesso de 30 Munroe St.? (Dica: esse intervalo de tempo está contido no próprio frame de beacon).
O intervalo de tempo entre as transmissões dos quadros de baliza é de 0,1024300 segundos.

3. Qual (em notação hexadecimal) é o endereço MAC de origem no quadro beacon de 30 Munroe St? Lembre-se da Figura 6.13 no texto de que a origem, o destino e o BSS são três endereços usados em um quadro 802.11. Para uma discussão detalhada da estrutura de quadros 802.11, consulte a seção 7 no documento de padrões IEEE 802.11 (citado acima).
O endereço MAC de origem é 00:16:b6:f7:1d:51.

4. O que (em notação hexadecimal) é o endereço MAC de destino no quadro beacon de 30 Munroe St ??
O endereço MAC de destino é ff:ff:ff:ff:ff:ff.

5. O que (em notação hexadecimal) é o ID MAC BSS no quadro beacon de 30 Munroe St?
O ID do BSS para 30 Munroe é Cisco-LI-f7:1d:51 (00: 16: b6: f7: 1d: 51).

6. Os quadros de sinalização do ponto de acesso 30 Munroe St anunciam que o ponto de acesso pode suportar quatro taxas de dados e oito “taxas de suporte estendidas” adicionais. Quais são essas taxas?

As quatro taxas suportadas são 1(B), 2(B), 5.5(B) E 11(B). As 8 taxas estendidas não suportadas são 6(B), 9, 12(B), 18, 24(B), 36, 48 e 54.

7. Encontre o quadro 802.11 contendo o segmento SYN TCP para esta primeira sessão TCP (que faz download de alice.txt). Quais são os três campos de endereço MAC no quadro 802.11? Qual endereço MAC nesse quadro corresponde ao host sem fio (fornece a representação hexadecimal do endereço MAC do host)? Para o ponto de acesso? Para o roteador de primeiro salto? Qual é o endereço IP do host sem fio que envia esse segmento TCP? Qual é o endereço IP de destino? Esse endereço IP de destino corresponde ao host, ponto de acesso, roteador de primeiro salto ou outro dispositivo conectado à rede? Explique.
Esses endereços MAC são BSSid, endereço de origem e destino. O endereço MAC corresponde ao host sem fio é 00:13:02:d1:b6:4f, o correspondente ao primeiro roteador de salto é 00:16:b6:f4:eb:a8, o correspondente ao host sem fio que envia esse segmento TCP é 00:16: b6:f7:1d:51. O IP correspondente do host sem fio é 192.168.1.109 e o IP de destino é 128.199.245.12 e esse IP corresponde ao host.

8. Encontre o quadro 802.11 contendo o segmento SYNACK para esta sessão TCP. Quais são os três campos de endereço MAC no quadro 802.11? Qual endereço MAC nesse frame corresponde ao host? Para o ponto de acesso? Para o roteador de primeiro salto? O endereço MAC do remetente no quadro corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado nesse datagrama? (Dica: revise a Figura 5.19 no texto se você não tiver certeza de como responder a essa pergunta ou da parte correspondente da pergunta anterior. É particularmente importante que você entenda isso).
Os três campos de endereço MAC no quadro 802.11 são ID do BSS: 00:16:b6:f7:1d:51, destino: 00:13:02:d1:b6:4f e endereço de origem: 00:16:b6:f4:eb:a8. O MAC correspondente ao host é 00:13:02:d1:b6:4f (destino). O MAC correspondente ao primeiro salto é 00:16: b6:f4:eb:a8 (origem). O endereço MAC do remetente no quadro não corresponde ao endereço IP do

dispositivo que enviou o segmento TCP encapsulado nesse datagrama, porque o endereço IP do TCP SYNACK é 128.199.245.12, mas o endereço IP de destino é 192.168.1.109.

9. Quais são as duas ações tomadas (ou seja, quadros são enviados) pelo host no rastreamento logo após t = 49, para terminar a associação com o AP 30 Munroe St que estava inicialmente no local quando a coleta de rastreamento começou? (Dica: uma é uma ação de camada de IP e uma é uma ação de camada de 802.11). Olhando para a especificação 802.11, há outro quadro que você poderia esperar ver, mas não vê aqui?
Um DHCP é enviado para 192.168.1.1 2 e após 0,02s o host envia um quadro de AUTHENTICATION.

10. Examine o arquivo de rastreio e procure por quadros de AUTHENICATION enviados do host para um AP e vice-versa. Quantas mensagens de AUTENTICAÇÃO são enviadas do host sem fio para o AP linksys_ses_24086 (que tem um endereço MAC de Cisco_Li_f5: ba: bb) iniciando em torno de t = 49?
Foram enviadas 17 mensagens de AUTHENTICATION do host sem fio para o AP linksys_ses_24086.

11. O host deseja que a autenticação exija uma chave ou esteja aberta?
O host está solicitando que a associação seja aberta.

12. Você vê uma resposta AUTHENTICATION do linkys_ses_24086 AP no trace?
Não vejo nenhuma resposta.

13. Agora, vamos considerar o que acontece quando o host desiste de tentar associar-se ao AP linksys_ses_24086 e agora tenta associar-se ao AP 30 Munroe St. Procure quadros de AUTHENTICATION enviados do host para e AP e vice-versa. Em que momentos há um quadro de AUTHENTICATION do host para o 30 Munroe St. AP, e quando há uma resposta

AUTHENTICATION enviada daquele AP para o host em resposta? (Observe que você pode usar a expressão de filtro "wlan.fc.subtype == 11e wlan.fc.type == 0 e wlan.addr == IntelCor_d1: b6: 4f" para exibir apenas os quadros de AUTHENTICATION neste traço para esta conexão sem fio hospedeiro).
Em t=63.168087 existe um quadro de AUTHENTICATION enviado de 00:13:02:d1:b6:4f (o host sem fio) para 00:16:b7:f7:1d:51 (o BSS). Em t=63.169071 existe um AUTHENTICATION enviado na direção inversa do BSS para o host sem fio.

14. Um ASSOCIATE REQUEST do host ao AP, e um quadro de ASSOCIATE RESPONSE correspondente do AP ao host, são usados para o host associado a um AP. A que horas há um ASSOCIATE REQUEST do anfitrião para o 30 Munroe St AP? Quando é enviada a ASSOCIATE REPLY correspondente? (Observe que você pode usar a expressão de filtro "wlan.fc.subtype <2 e wlan.fc.type == 0 e wlan.addr == IntelCor_d1: b6: 4f" para exibir apenas os quadros ASSOCIATE REQUEST e ASSOCIATE RESPONSE para este vestígio.)
Em t = 63.169910 existe um Quadro de ASSOCIATE REQUEST enviado de 00:13:02: d1: b6:4f para 00:16:b7:f7:1d:51 (o BSS). Em t = 63,192101 há uma resposta associada enviado na direção inversa do BSS para o host sem fio.

15. Quais taxas de transmissão o host está disposto a usar? O AP? Para responder a essa pergunta, você precisará examinar os campos de parâmetros do quadro de gerenciamento da LAN sem fio 802.11.
As taxas suportadas são: 1, 2, 5,5, 11, 6, 9, 12, 18, 24, 32, 48 e 54 Mbps.

16. Quais são os endereços MAC do remetente, do destinatário e do ID do BSS nesses quadros? Qual é o propósito desses dois tipos de quadros? (Para responder a essa última pergunta, você precisa pesquisar as referências on-line citadas anteriormente neste laboratório).
PROBE REQUEST - Fonte: 00:12:f0:1f:57:13, Destino: ff:ff:ff:ff:ff:ff.
BSSID: ff:ff:ff:ff:ff:ff

PROBE RESPONSE - Fonte: 00:16:b6:f7:1d:51, Destino: 00:16:b6:f7:1d:51.
BSSID: 00:16:b6:f7:1d:51.
A PROBE REQUEST é uma transmissão para procurar um ponto de acesso do host. A PROBE RESPONSE é usada para responder ao host a partir do ponto de acesso