request, auth response (success), client sends association/ reassociation request and AP responds to that with a association/reassociation response (success). After this depending on the security type of the WLAN/SSID, further frames are exchanged. in the below snippet of wireshark you can see the reassociation process followed by EAP/TLS handshake

2243	7.972584	Apple_61:b5:fa	Broadcast	802.11	151	6	Probe Request, SN=121, FN=0, Flags=.....C, SSID=DATA
2244	7.972738	CiscoInc_10:62:0b	Apple_61:b5:fa	802.11	288	12	Probe Response, SN=2125, FN=0, Flags=....R...C, BI=102, SSID=DATA
2284	8.047872	Apple_61:b5:fa	CiscoInc_10:62:0b	802.11	80	12	Authentication, SN=125, FN=0, Flags=.....C
2285	8.047989		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2287	8.067541	CiscoInc_10:62:0b	Apple_61:b5:fa	802.11	59	12	Authentication, SN=4030, FN=0, Flags=.....C
2289	8.067916	Apple_61:b5:fa	CiscoInc_10:62:0b	802.11	205	12	Reassociation Request, SN=126, FN=0, Flags=.....C, SSID=DATA
2290	8.067992		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2291	8.069666	CiscoInc_10:62:0b	Apple_61:b5:fa	802.11	181	12	Reassociation Response, SN=4031, FN=0, Flags=.....C
2293	8.072255	CiscoInc_10:62:0b	Apple_61:b5:fa	EAP	120	7 12	Request, Identity
2295	8.078557	Apple_61:b5:fa	CiscoInc_10:62:0b	802.11	62	12	Action, SN=127, FN=0, Flags=.....C
2296	8.078688		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2297	8.078908	Apple_61:b5:fa	CiscoInc_10:62:0b	EAP	81	0 12	Response, Identity
2298	8.078984		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2299	8.079058	CiscoInc_10:62:0b	Apple_61:b5:fa	802.11	62	12	Action, SN=4032, FN=0, Flags=.....C
2301	8.079299	Apple_61:b5:fa (TA)	CiscoInc_10:62:0b (RA)	802.11	49	12	802.11 Block Ack Req, Flags=.....C
2302	8.079466	CiscoInc_10:62:0b (TA)	Apple_61:b5:fa (RA)	802.11	57	12	802.11 Block Ack, Flags=.....C
2308	8.102922	CiscoInc_10:62:0b	Apple_61:b5:fa	EAP	73	7 12	Request, TLS EAP (EAP-TLS)
2311	8.110274	Apple_61:b5:fa	CiscoInc_10:62:0b	TLSv1	230	0 12	Client Hello
2312	8.110391		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2335	8.121015	CiscoInc_10:62:0b	Apple_61:b5:fa	TLSv1	1079	7 12	Server Hello, Certificate, Certificate Request, Server Hello Done
2337	8.129486	Apple_61:b5:fa	CiscoInc_10:62:0b	EAP	73	0 12	Response, TLS EAP (EAP-TLS)
2338	8.129603		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2340	8.139864	CiscoInc_10:62:0b	Apple_61:b5:fa	TLSv1	1075	7 12	Server Hello, Certificate, Certificate Request, Server Hello Done
2342	8.145614	Apple_61:b5:fa	CiscoInc_10:62:0b	EAP	73	0 12	Response, TLS EAP (EAP-TLS)
2343	8.145697		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2345	8.156076	CiscoInc_10:62:0b	Apple_61:b5:fa	TLSv1	1075	7 12	Server Hello, Certificate, Certificate Request, Server Hello Done
2350	8.199357	Apple_61:b5:fa	CiscoInc_10:62:0b	EAP	73	0 12	Response, TLS EAP (EAP-TLS)
2351	8.199493		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2353	8.209438	CiscoInc_10:62:0b	Apple_61:b5:fa	TLSv1	1075	7 12	Server Hello, Certificate, Certificate Request, Server Hello Done
2373	8.240701	Apple_61:b5:fa	CiscoInc_10:62:0b	EAP	73	0 12	Response, TLS EAP (EAP-TLS)
2374	8.240820		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2391	8.249935	CiscoInc_10:62:0b	Apple_61:b5:fa	TLSv1	151	7 12	Server Hello, Certificate, Certificate Request, Server Hello Done
2412	8.296692	Apple_61:b5:fa	CiscoInc_10:62:0b	TLSv1	1343	0 12	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
2413	8.296806		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2416	8.307264	CiscoInc_10:62:0b	Apple_61:b5:fa	EAP	73	7 12	Request, TLS EAP (EAP-TLS)
2418	8.310614	Apple_61:b5:fa	CiscoInc_10:62:0b	TLSv1	1343	0 12	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
2419	8.310732		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2420	8.320328	CiscoInc_10:62:0b	Apple_61:b5:fa	EAP	73	7 12	Request, TLS EAP (EAP-TLS)
2422	8.323320	Apple_61:b5:fa	CiscoInc_10:62:0b	TLSv1	1343	0 12	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
2423	8.323404		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2424	8.332612	CiscoInc_10:62:0b	Apple_61:b5:fa	EAP	73	7 12	Request, TLS EAP (EAP-TLS)
2426	8.335390	Apple_61:b5:fa	CiscoInc_10:62:0b	TLSv1	793	0 12	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
2427	8.335520		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2444	8.365095	CiscoInc_10:62:0b	Apple_61:b5:fa	TLSv1	132	7 12	Change Cipher Spec, Encrypted Handshake Message
2453	8.407064	Apple_61:b5:fa	CiscoInc_10:62:0b	EAP	73	0 12	Response, TLS EAP (EAP-TLS)
2454	8.407147		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2455	8.431380	CiscoInc_10:62:0b	Apple_61:b5:fa	EAP	71	7 12	Success
2457	8.431602	CiscoInc_10:62:0b	Apple_61:b5:fa	EAPOL	184	7 12	Key (Message 1 of 4)
2459	8.432552	Apple_61:b5:fa	CiscoInc_10:62:0b	EAPOL	202	0 12	Key (Message 2 of 4)
2460	8.432637		Apple_61:b5:fa (RA)	802.11	39	12	Acknowledgement, Flags=.....C
2461	8.433501	CiscoInc_10:62:0b	Apple_61:b5:fa	EAPOL	218	7 12	Key (Message 3 of 4)
2463	8.434442	Apple_61:b5:fa	CiscoInc_10:62:0b	EAPOL	162	0 12	Key (Message 4 of 4)

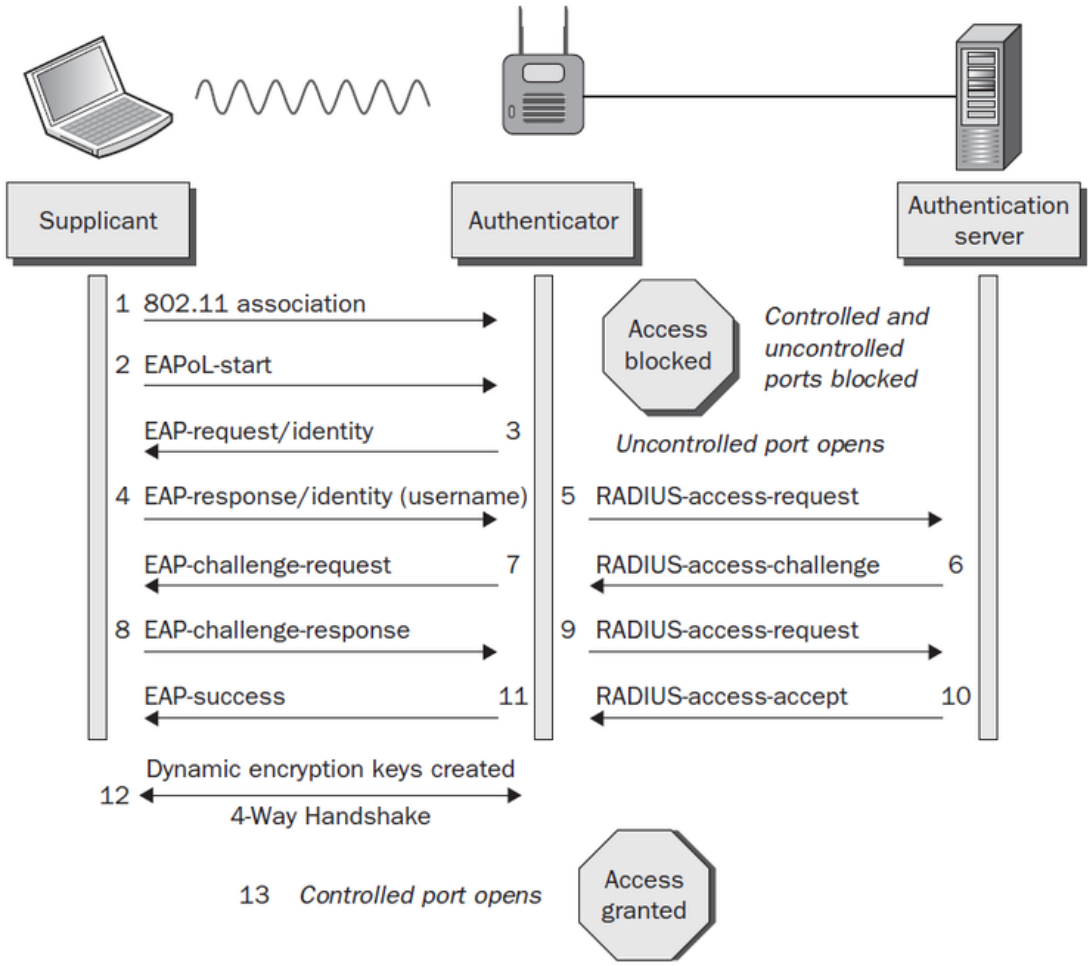
2. Describe the process in detail on how wifi client gets on the wifi network and starts passing traffic

Pretty much the same answer as question 1.

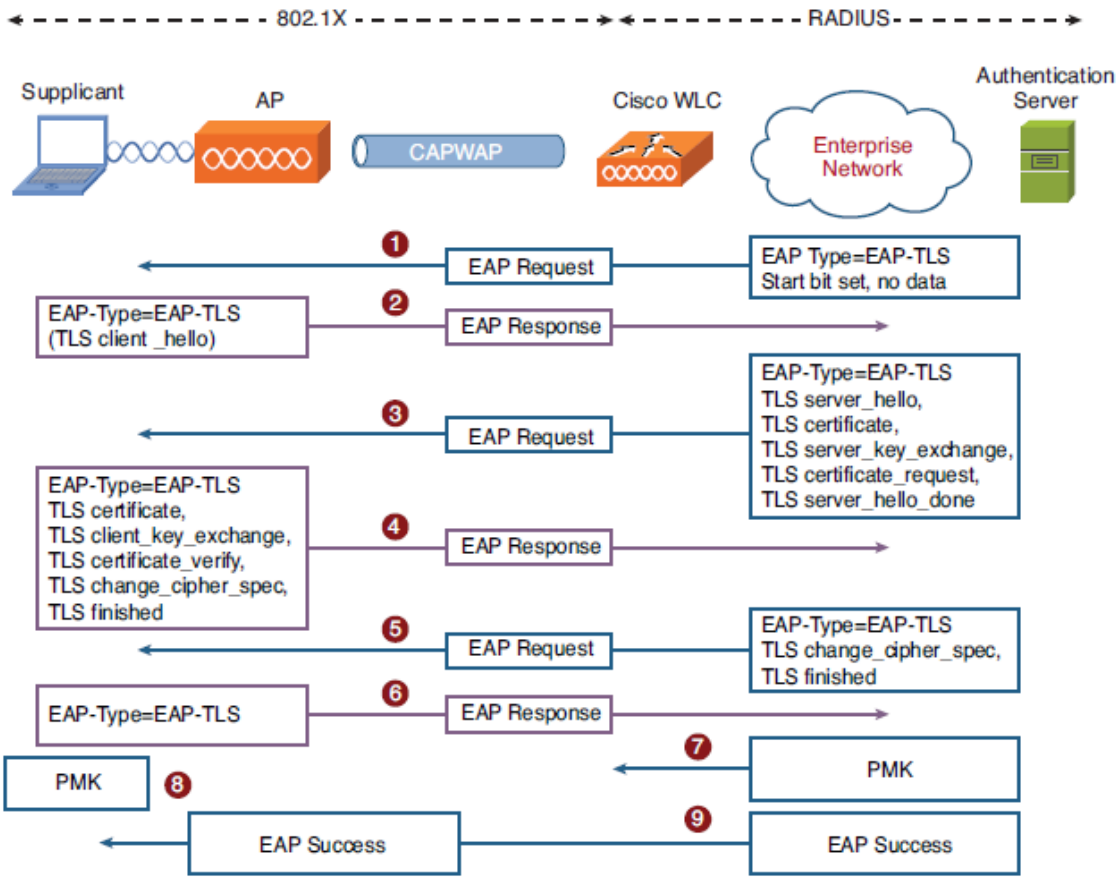
3. Describe the generic EAP process

Talk about the different entities involved like the authenticator, endpoint, authentication server etc.

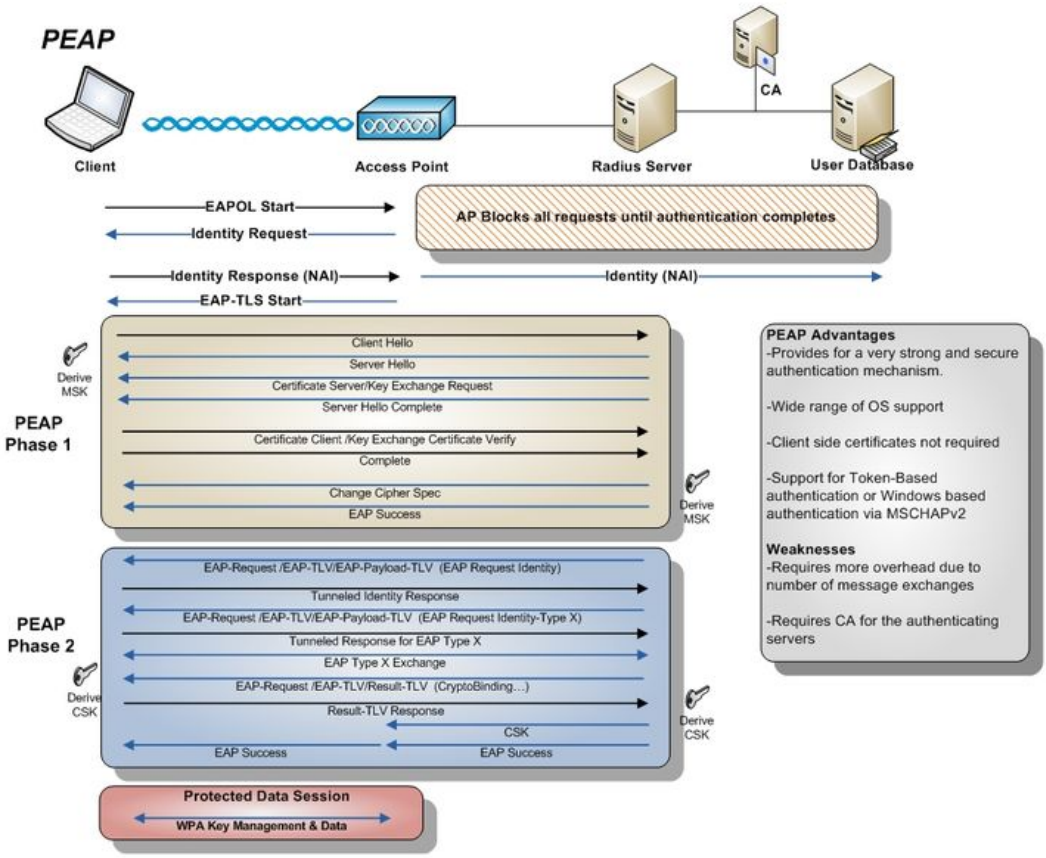
FIGURE 4.24 Generic EAP exchange



4. Explain EAP-TLS process



5. Explain EAP-PEAP



6. Describe in detail what happens when you open the web browser on a client to surf google.com

This article gives a very in-depth breakdown of the process. You just need to know the high level details mainly around DNS and HTTP request

http://igoro.com/archive/what-really-happens-when-you-navigate-to-a-url/ (http://igoro.com/archive/what-really-happens-when-you-navigate-to-a-url/)

7. What is the difference between 'Association frame' and 'Reassociation frame'

https://mrncciew.com/2014/10/28/802-11-mgmt-association-reqresponse/ (https://mrncciew.com/2014/10/28/802-11-mgmt-association-reqresponse/)

https://mrncciew.com/2014/10/28/cwap-reassociation-reqresponse/ (https://mrncciew.com/2014/10/28/cwap-reassociation-reqresponse/) (https://mrncciew.com/2014/10/28/cwap-reassociation-reqresponse/)

8. What is a near - far issues in terms of wifi

Please refer to CWNA Chapter on WLAN troubleshooting

FIGURE 12.10 Mismatched AP and client power

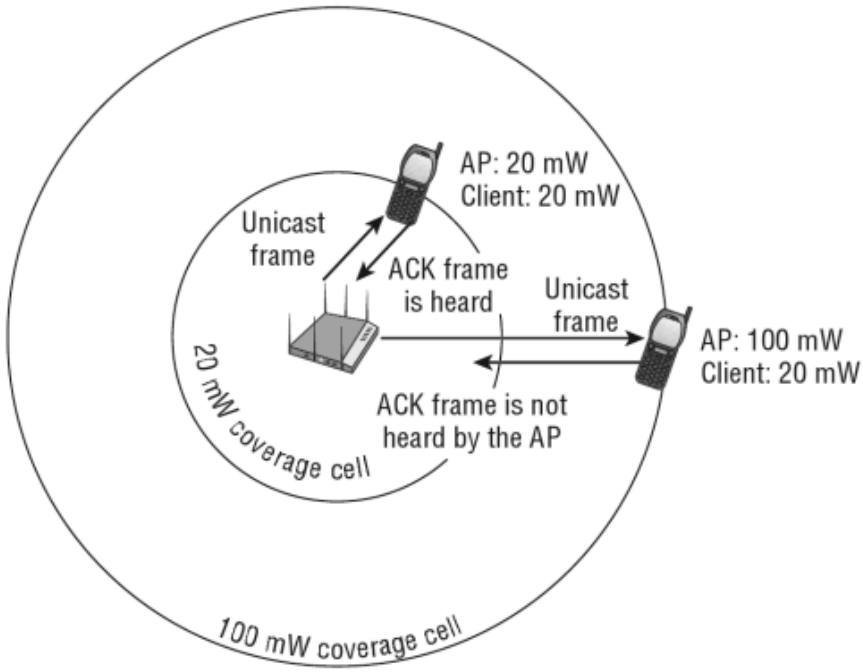
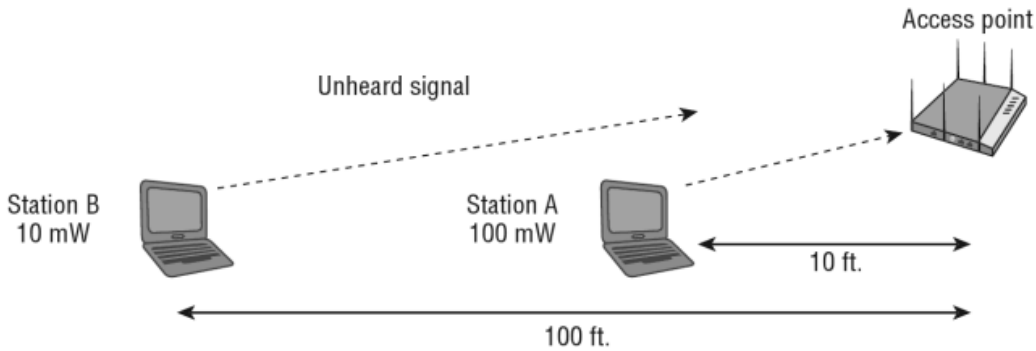


FIGURE 12.11 The near/far problem



9. What is the hidden node/terminal problem?

https://www.youtube.com/watch?v=BLEt10OkE4g (https://www.youtube.com/watch?v=BLEt10OkE4g)

10. How would you troubleshoot low throughput issue on the wifi network

There is no real 'correct' answer for such open ended questions. The interviewer is trying to access your analytical thinking and troubleshooting skills. If the interview is for a customer rep or test engineer, this question would be very important.

Throughput issues can steam from variety of root causes. It is important to ask a few questions and understand what is the problem symptom before you get started. You should look at the data rate at which the client is connecting (802.11n, ac etc), what MCS rate and the clients capability, SNR, RSSI of the client to start off with. A handy tool is WLC / AP debugs logs in conjunction with Over-the-air 802.11 sniffer captures. You can follow the traffic pattern (you won't be able to decode the actual qos data on most occasions) to try and get a sense of any RF issues (if you see too many Retries or

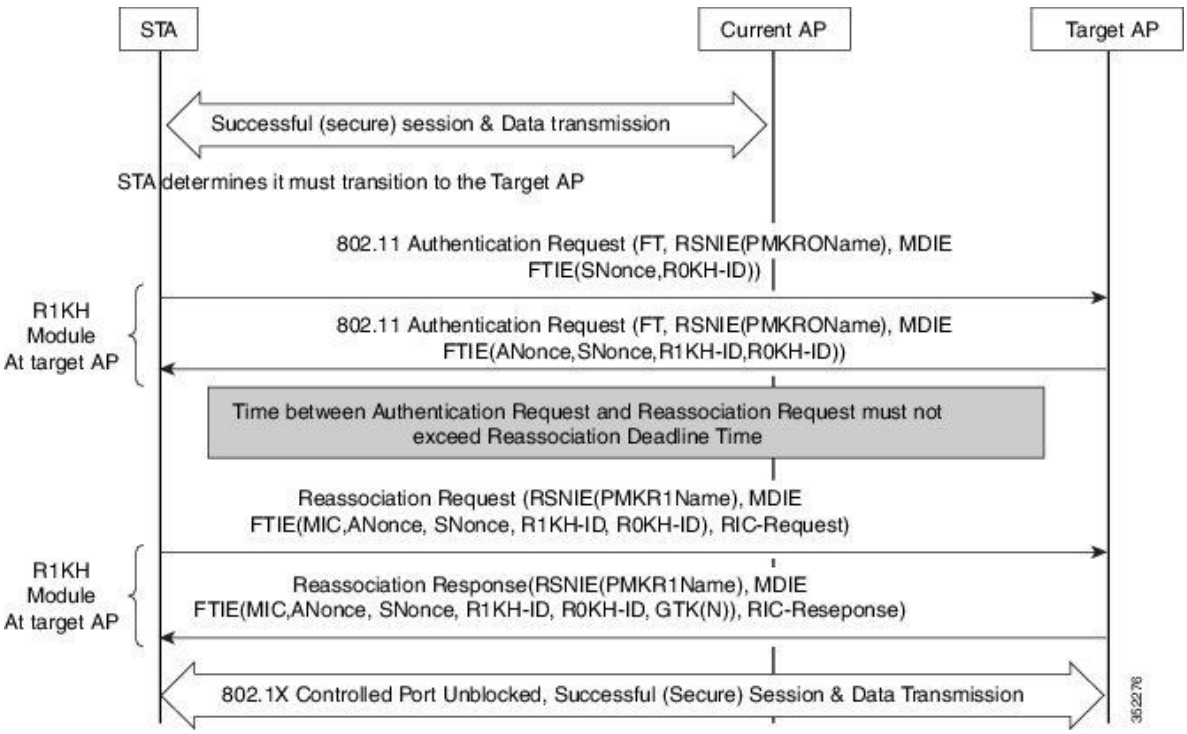
rate downshift). On odd occasion if there is a bug you may land up with incorrect sequencing of the data frames, qos mis configs and potential A-MPDU issues. Next step once you are past the Layer 1 and 2 of the OSI model is to start exploring the layer 3 traffic (decapsulated, preferably at the VLAN level or default gateway). Check for TCP windowing issues or retransmit etc. The problem could be between specific hosts/ servers etc.

11. How would you troubleshoot one way audio issue

Typically one way audio issues stem from power mismatch between the AP and the VoWiFi device. The VoWiFI device has limited transmit power compared to the AP which can cause one way audio issues. The VoWiFi device can hear the AP communication even at relatively far off distances but at cell edge or beyond if the VoWiFi transmits data back, the AP sometimes cannot interpret the data leading to one way audio. This is the simplest form of one way audio issue. You need to determine if the communication is between 2 VoWiFi devices or one VoWiFi and one wired phone. There could be configurations that may block peer to peer communication which may potentially lead to one way audio or no audio between two VoWiFi devices. The way to troubleshoot such issue is normally double check the configurations are ok and adhere voice of wifi best practices and then delve into debugs + over the air captures for further isolating the problem.

12. Briefly explain 802.11r

https://en.wikipedia.org/wiki/IEEE_802.11r-2008 (https://en.wikipedia.org/wiki/IEEE_802.11r-2008)



13. What are the data rates of 802.11b, 802.11g, 802.11a, 11n and 11ac (they can also ask history of 802.11b, g and a). There are too many 802.11n MCS rates so most likely you should not expect a question like that.

802.11(a, b, g) comparison

Standards	802.11g	802.11b	802.11a
Data Rate Support	54, 48, 36, 24, 18, 12, 9, 6,11, 5.5, 2, 1 Mbps	11, 5.5, 2, 1 Mbps	54, 48, 36, 24, 18, 12, 9, 6 Mbps
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps
Frequency Band	2.4 GHz (2.4 GHz to 2.4835 GHz)	2.4 GHz (2.4 GHz to 2.4835 GHz)	5 GHz (5.725 GHz to 5.850 GHz)
Channels	3 non-overlapping channels, up to 13 overlapping	3 non-overlapping channels, up to 13 overlapping	12 non-overlapping channels
Technique	OFDM/CCK (6,9,12,18,24,36,48,54) OFDM (6,9,12,18,24,36,48,54) DQPSK/CCK (22, 33, 11, 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)	DQPSK/CCK (11, 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)	BPSK (6, 9 Mbps) QPSK (12, 18 Mbps) 16-QAM (24, 36 Mbps) 64-QAM (48, 54 Mbps)
Max. Range*	Up to 1,000 ft	Up to 1,000 ft	Up to 500 ft
Backward Compatibility	802.11b	N/A	N/A
Features	Replacement for 802.11b with higher data rate and better security	Most widely deployed today	Ideal for high-density environments

83180 Wireless LANs **802.11g PHY** **Page 17 of 24**

TABLE 1: IEEE 802.11 PHY STANDARDS

Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2012 (expected)	802.11ad	60	2160	SC, OFDM	Beamforming	6.76 Gbits/s
2013 (expected)	802.11ac	5	40, 80, 160	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

802.11n rates: http://mcsindex.com/ (http://mcsindex.com/)

802.11ac MCS rates

http://wirelessonthego.postach.io/post/802-11ac-mcs-rates (http://wirelessonthego.postach.io/post/802-11ac-mcs-rates)

14. Difference between dB, dBm, dBi

http://www.antenna-theory.com/definitions/decibels.php (http://www.antenna-theory.com/definitions/decibels.php)

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-fixed/9218-quick-ref.html (http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-fixed/9218-quick-ref.html)

15. What cell edge and cell overlap would you survey for a voice deployment

-65 to -67 dBm

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73/ch9_Voic.
(http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73/ch9_Voic

16. What data rates are beacons sent out / broadcasted?

Beacons are broadcasted at the mandatory data rates set on the 2.4 and 5GHz radios.

17. How many MCS rates are there for 802.11ac?

There are nine for a specific Spacial stream.
http://wirelessonthego.postach.io/post/802-11ac-mcs-rates
(http://wirelessonthego.postach.io/post/802-11ac-mcs-rates)

18. Modulation techniques -

http://www.ni.com/tutorial/7131/en/ (http://www.ni.com/tutorial/7131/en/)

http://www.wirelessdesignonline.com/doc/modulation-techniques-for-high-speed-wlan-sys-0001 (http://www.wirelessdesignonline.com/doc/modulation-techniques-for-high-speed-wlan-sys-0001)

19. What is antenna beamwidth

https://en.wikipedia.org/wiki/Beamwidth (https://en.wikipedia.org/wiki/Beamwidth)

20. Have you heard of 802.11ah?

https://en.wikipedia.org/wiki/IEEE_802.11ah
(https://en.wikipedia.org/wiki/IEEE_802.11ah)

21. Explain in as much detail as possible when you try and ping a server on the internet

http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_Mays_Ping.pdf
(http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_Mays_Ping.pdf)

Assuming the ping involves a packet being sent over an Ethernet or WiFi network, ARP is used to find the Ethernet hardware address of the device that receives the outbound packet. Typically this will be the router for the LAN the machine originating the ping is on.

The typical process is:

- You enter a command to ping a destination.
- DNS is used to determine the IP address (if needed).
- The routing table is consulted to find the next hop towards that destination.
- ARP is used to find the hardware address of the next hop.
- The IP packet is sent to the next hop, encapsulated in an Ethernet or WiFi frame

22. What is MIMO, SU-MIMO, MU-MIMO, Beamforming etc

These are some of the most common terms you will come across while reading content on 11n and 11ac. The books i have referenced have all you need on these concepts

23. What is the difference between Active scanning and Passive scanning?

Passive scanning: Its the process where the client (STA) listens (on different channels) to the beacons from the AP or Ad Hoc station. The STA continues to listen to the beacons till its hears a beacon with the SSID of the network it wishes to join.

Active scanning: This involves the STA sending a probe request frame. The station sends the probe request frame when it is actively trying to join a specific SSID (network). The probe request frame will either contain the SSID name of the network or a broadcast SSID. If probe request is sent specifying a specific SSID, then only the APs serving the SSID will respond with a probe response frame. If probe request is sent with broadcast SSID then all APs within reach will respond.

24. TCP handshakes, TCP Windowing

You can google it :)

25. 5GHz spectrum channels for WiFi use

http://wirelessonthego.postach.io/post/new-b-regulatory-domain-for-wlan-equipment-for-us (http://wirelessonthego.postach.io/post/new-b-regulatory-domain-for-wlan-equipment-for-us)
(http://wirelessonthego.postach.io/post/new-b-regulatory-domain-for-wlan-equipment-for-us)

26. Common interferers on 2.4GHz

Microwave, 2.4 GHz video camera, 2.4GHz cordless phones, bluetooth devices etc

27. What is the difference between MSDU and MPDU

https://www.youtube.com/watch?v=fYPspcM68h0 (https://www.youtube.com/watch?v=fYPspcM68h0)
(https://www.youtube.com/watch?v=fYPspcM68h0)

https://mrncciew.com/2013/04/11/a-mpdu-a-msdu/
(https://mrncciew.com/2013/04/11/a-mpdu-a-msdu/)
(https://mrncciew.com/2013/04/11/a-mpdu-a-msdu/)

28. What is the difference between MSDU and A-MSDU

https://www.youtube.com/watch?v=fYPspcM68h0 (https://www.youtube.com/watch?v=fYPspcM68h0)

https://mrncciew.com/2013/04/11/a-mpdu-a-msdu/
(https://mrncciew.com/2013/04/11/a-mpdu-a-msdu/)

https://www.cwnp.com/forums/posts?postNum=286912
(https://www.cwnp.com/forums/posts?postNum=286912)
(https://www.cwnp.com/forums/posts?postNum=286912)

29. What is a guard interval

https://en.wikipedia.org/wiki/Guard_interval (https://en.wikipedia.org/wiki/Guard_interval) (https://en.wikipedia.org/wiki/Guard_interval)

https://wifijedi.com/2009/02/11/how-stuff-works-short-guard-interval/ (https://wifijedi.com/2009/02/11/how-stuff-works-short-guard-interval/) (https://wifijedi.com/2009/02/11/how-stuff-works-short-guard-interval/)

30. How many (max) mac addresses are present in a 802.11 header

Four - Sender Address (SA), Transmitter address (TA), Destination address (DA) and Receiver address (RA)

http://community.arubanetworks.com/t5/Technology-Blog/802-11-MAC-Header-Breakdown/ba-p/219264 (http://community.arubanetworks.com/t5/Technology-Blog/802-11-MAC-Header-Breakdown/ba-p/219264) (http://community.arubanetworks.com/t5/Technology-Blog/802-11-MAC-Header-Breakdown/ba-p/219264)

31. Difference between DCF and PCF

http://www.wi-fiplanet.com/tutorials/article.php/1548381/80211-Medium-Access-Methods.htm (http://www.wi-fiplanet.com/tutorials/article.php/1548381/80211-Medium-Access-Methods.htm)

http://www.vocal.com/networking/802-11-distributed-coordination-function-dcf/ (http://www.vocal.com/networking/802-11-distributed-coordination-function-dcf/)

https://en.wikipedia.org/wiki/Point_coordination_function (https://en.wikipedia.org/wiki/Point_coordination_function)

https://en.wikipedia.org/wiki/Distributed_coordination_function (https://en.wikipedia.org/wiki/Distributed_coordination_function) (https://en.wikipedia.org/wiki/Distributed_coordination_function)

32. What are the types of 802.11 frames?

Management, Control, Data frame and reserved

There can be so many more questions from these books below.

Below are some of the books, materials to review/read to better prepare yourself for the interview

- CWTS
- CWNA
- CWSP
- CWAP
- 802.11n Survival Guide O'Reilly
- 802.11ac Survival Guide O'Reilly

For Vendor specific (in this case Cisco since thats all I know :/)